

딥러닝 모델을 활용한 USDT 스테이블코인 이상 탐지

송아현*, 서의성**, 김희열***

Deep Learning-based Anomaly Detection in the USDT Stablecoin

Ahyun Song*, Euseong Seo**, and Heeyoul Kim***

이 논문은 2024년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임
(No. RS-2020-NR049579)

요약

본 논문은 대표적인 스테이블코인인 USDT의 온체인 거래 데이터를 분석하여 딥러닝 모델을 활용해 이상 행위를 탐지하는 방법론을 제안한다. 이더리움 블록체인 상의 ERC-20 기반 USDT 거래 데이터를 수집하고 분석해, 이를 시간 단위로 집계하여 총 6개의 피처(전송량, 거래 수, 송신자 수, 수신자 수, 발행량, 소각량)를 추출하였다. 이후 Anomaly VAE-Transformer 모델을 구성하고, 비지도 학습 방식으로 정상 패턴을 학습한 뒤 재구성 오차 기반 이상 스코어를 계산하였다. 도출된 스코어를 통해 탐지된 이상 구간에 대한 분석을 수행했고, 급격한 발행·소각, 거래 집중 등 다양한 이상 패턴을 효과적으로 탐지하였음을 보였다. 본 논문은 스테이블코인의 거래에 대해 이상 거래를 조기에 탐지할 수 있는 기반을 제공하며, 향후 디파이 생태계의 안정성과 보안성을 강화하는 데 기여할 것으로 기대된다.

Abstract

This paper proposes a deep learning-based methodology for detecting anomalous behavior in the on-chain transaction data of USDT, one of the most widely used stablecoins. We collect and analyze ERC-20-based USDT transaction data on the Ethereum and aggregate it into hourly data to extract six key features. Using this data, we construct an Anomaly VAE-Transformer model, which learns the normal patterns through unsupervised training and calculates anomaly scores based on reconstruction errors. The resulting scores are used to identify and analyze abnormal periods, and we demonstrate effectiveness in detecting various anomalous patterns such as sudden issuance or redemption spikes. This study provides a foundation for the early detection of abnormal activity in stablecoin transactions and is expected to contribute to improving the stability and security of the DeFi ecosystem.

Keywords

stablecoin, anomaly detection, deep learning, blockchain

* 성균관대학교 컴퓨터공학과 박사과정
- ORCID: <https://orcid.org/0009-0006-9192-6694>
** 성균관대학교 컴퓨터공학과 교수
- ORCID: <https://orcid.org/0000-0003-2103-8019>
*** 경기대학교 컴퓨터과학과 교수(교신저자)
- ORCID: <https://orcid.org/0000-0001-6341-580X>

· Received: Jun. 09, 2025, Revised: Jul. 10, 2025, Accepted: Jul. 13, 2025
· Corresponding Author: Heeyoul Kim
Dept. of AI Computer science, kyonggi University, 154-42,
Gwanggyosan-ro, Korea
Tel.: +82-31-249-9607, Email: heeyoul.kim@kgu.ac.kr

I. 서론

최근 블록체인 기반 금융 서비스인 디파이(DeFi)의 급속한 발전과 관심이 증가하면서, 탈중앙화된 형태의 디지털 자산 및 금융 거래가 활발히 이루어지고 있다. 특히, 스테이블코인(Stablecoin)은 가격 변동성이 큰 일반 암호화폐와 달리, 법정화폐에 가치를 연동시켜 변동성을 줄이고 안정성을 제공하는 수단으로 주목받고 있다[1]. 스테이블코인은 암호화폐 생태계에서 거래의 매개 수단, 담보 자산, 유동성 공급자 등 다양한 역할을 수행해 디파이 생태계의 핵심 인프라로 자리매김하고 있다. 그중에서도 USDT[2]는 가장 대표적인 스테이블코인 중 하나로, 시가총액과 거래량 면에서 가장 큰 규모를 보유하고 있다. USDT는 미국 달러화(USD)에 1:1로 가치를 고정(Pegging)시킨다는 점에서 투자자와 사용자들에게 높은 신뢰를 제공하며, 주요 중앙화 거래소(CEX)와 탈중앙화 거래소(DEX), 각종 디파이 서비스에서 폭넓게 사용되고 있다.

그러나, 스테이블코인의 활용성이 높아지면서 보안 사고와 이상 거래에 대한 우려의 목소리가 높아지고 있다. 실제로 USDT는 과거에 자산 담보율 조작 의혹, 회계 투명성의 문제, 급격한 거래량 변동 등 다양한 이슈가 발생하기도 했으며, 이는 블록체인과 디파이 생태계 전반에 큰 위협이 되는 문제가 될 수 있다. 특히, USDT와 같은 스테이블코인은 중앙 발행 기관에 의해 통제되다 보니 블록체인의 핵심 가치인 탈중앙화와 상충하는 구조적 문제를 가지고 있다. 그리고 특정 주소에서 대량으로 USDT를 민팅(Minting)하거나 특정 시점에 대규모의 거래를 발생시키는 등의 이상 거래를 통해 시장 조작, 자금 세탁, 급격한 유동성 유출 등을 발생시키는 위험성을 가지고 있다[3]. 특히, 스테이블코인은 봇에 의한 자동화된 거래, 민감한 가격 유지 메커니즘, 크로스체인 브릿지를 통한 대규모 유동성 이동 등의 구조적 특성을 가지며, 이러한 활동이 의도적으로 조작되거나 급변하는 경우 정상적인 시장 흐름에서 벗어난 이상 징후로 해석될 수 있다. 하지만, 많은 거래들이 자동화되고 대규모로 발생하다 보니, 효과적으로 이상 탐지를 수행하기 매우 어렵다.

본 논문에서는 대표적 스테이블코인인 USDT의 이상 거래 탐지를 문제로 정의하고, 이를 효과적으로 해결할 수 있는 방법론을 제공한다. 문제 해결을 위해, 먼저 블록체인에 기록된 USDT 데이터를 수집하고 분석해 이상 탐지에 적합한 피처를 추출한다. 그리고 딥러닝 모델을 학습시킨 후 평가를 통해 이상 구간을 탐지한다. 이후 탐지한 구간에 대한 분석을 통해 이상 패턴과 발생 원인을 도출한다. 본 논문의 목적은 1) USDT 실거래 데이터를 기반으로 이상 탐지에 적합한 다변량 시계열 피처 추출, 2) 이상 탐지를 위한 딥러닝 모델 설계와 학습, 3) 탐지된 이상 구간에 대한 정성적 분석을 통한 제안 방법론의 실증으로 요약된다. 본 논문은 딥러닝을 활용해 스테이블코인의 이상 탐지를 수행한 최초의 연구이며, 블록체인 기반 자산 시스템과 디파이의 건전성과 안전성 확보에 기여한다는 의의가 있다.

본 논문의 구조는 다음과 같다. 2장에서는 스테이블코인에 대한 분석과 함께 딥러닝 기반 이상 탐지에 관한 연구들을 분석하며, 3장에서는 USDT 데이터의 분석과 딥러닝 모델의 구성, 이상 스코어 계산 방식을 제공한다. 4장에서는 탐지된 이상 구간에 대한 분석을 수행하고, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 블록체인 기반 스테이블코인과 USDT

블록체인 기술은 탈중앙화된 구조와 투명성을 바탕으로 기존의 중앙집중형 구조의 안정성과 신뢰성 문제를 해결할 것으로 기대되고 있으며, 특히 디지털 자산 및 디파이와 같은 금융 서비스의 근간이 되고 있다[4]. 그중에서도 스테이블코인은 기존 암호화폐의 급격한 가격 변동성 문제를 해결하는 대안으로 등장했으며, 실질적인 결제 및 유동성 공급 수단으로 광범위하게 채택되고 있다.

스테이블코인은 일반적으로 담보 구조에 따라 법정화폐 담보형, 암호화폐 담보형, 알고리즘 기반으로 분류된다. 법정화폐 담보형은 발행 기관이 미국 달러화와 같은 법정화폐 자산을 보유하고 이에 상응하는 스테이블코인을 발행하는 구조이다.

대표적 스테이블코인인 USDT가 여기에 속하며, 미국 달러화에 1:1로 가치를 고정하며, 2025년 3월 기준 1500억 달러 가치의 공급량을 제공하고 있다. USDC도 미국 달러에 기반한 담보를 보유한 중앙화된 발행 모델이며, 특히 회계의 투명성과 규제 준수를 강조하고 있다. 암호화폐 담보형은 블록체인 내의 스마트 컨트랙트에 의해 BTC나 ETH와 같은 담보 암호화폐를 예치하고 초과 담보율을 기준으로 스테이블코인을 발행하는 구조이다. DAI는 암호화폐 담보형 스테이블코인으로, 스마트 컨트랙트에 의해 ETH 등의 암호화폐 담보를 예치하는 방식을 사용하고, 특히 다양한 암호화폐와 토큰 간의 스왑과 거래에 활용되고 있다. 알고리즘 기반은 외부 자산에 의존하지 않고 스마트 컨트랙트의 특정 알고리즘을 통해 공급량을 자동 조절함으로써 가격을 일정하게 유지하는 구조를 취한다. TerraUSD는 대표적인 알고리즘 기반 스테이블코인이지만, 2022년 테라 사태로 인한 붕괴로 알고리즘 스테이블코인의 위험 관리와 구조적 취약점에 대한 문제점이 노출되었다.

이 중 USDT는 가장 널리 사용되고 있는 스테이블코인이며, 2014년 출시 이후 빠르게 성장해 2025년 기준으로 전체 스테이블코인 중 가장 높은 시가 총액과 거래량을 보이며 블록체인 기반 디지털 자산 시장에서 사실상의 기축통화 역할을 수행하고 있다. USDT는 테더(Tether limited)라는 발행기관에 의해 운영되며, 이더리움, 트론, 솔라나 등 다양한 블록체인 네트워크에서 유통되고 있다. 특히 이더리움 상에서는 ERC-20 토큰 표준을 따르는 방식으로 구현되어 동작하고 있다. 이는 USDT가 이더리움 상에서 자동화된 토큰 컨트랙트에 의해 동작한다는 의미이며, 투명하게 모든 거래와 유통 흐름을 수집하고 분석, 검증할 수 있다.

2.2 딥러닝 기반 이상 탐지 기법

이상 탐지는 데이터 집합 내에서 정상 패턴과 뚜렷하게 다른 이상치를 식별하는 과정을 의미하고, 제조상의 결함, 시스템의 오작동, 금융 사기 등 다양한 분야에서 활용될 수 있다. 하지만, 이상 패턴

은 매우 드물게 발생하고 예측이 어렵다는 특성을 가지며, 효과적인 이상 탐지를 위한 다양한 연구가 진행되고 있다. 이상은 형태에 따라 크게 세 가지 유형으로 구분된다. 개별 이상은 전체 분포에서 크게 벗어나는 단일 데이터를 의미하며, 조건부 이상은 특정 컨텍스트 상에서의 비정상적인 데이터, 집단 이상은 개별적으로는 정상이나 집합적으로 이상한 패턴을 이루는 경우를 의미한다[5]. 특히 시계열 데이터에서는 세 번째 유형의 이상이 빈번하게 나타난다.

최근 딥러닝 기술이 발전함에 따라, 이상 탐지 분야에서도 다양한 딥러닝 모델을 활용한 기법들이 시도되고 있다. 대표적으로 Pang 등은 딥러닝 기반 이상 탐지를 다음 세 가지로 분류한다[6]: 첫째, 피쳐 추출 기반 방식은 딥러닝을 통해 고차원의 데이터를 저차원의 벡터로 압축한 뒤 전통적인 이상 탐지 기법에 적용하는 방식이다. 둘째, 중단 간 이상 스코어 학습 방식은 딥러닝 모델이 피쳐 추출부터 이상 점수 산출까지 전 과정을 직접 학습하도록 구성되는 방식이다. 셋째, 정상성 표현 학습 방식은 정상 데이터를 효과적으로 표현하는 잠재 공간을 학습하고, 복원 오차를 기반으로 이상을 판단하는 방식이다.

시계열 데이터의 이상 탐지는 이 중에서도 주로 세 번째 방식을 사용하고 있으며, 이는 다시 다음과 같은 세 가지 방식으로 분류된다. 첫째, 재구성(Reconstruction) 기반 방식은 정상 데이터를 기반으로 잠재 공간을 학습한 뒤, 입력값과 복원값의 차이인 재구성 오차를 통해 이상을 식별한다. 대표적인 모델로 AE(Autoencoder)[7], VAE(Variational Autoencoder)[8], Transformer[9] 기반 모델들이 있다. 둘째, 예측(Forecasting) 기반 방식은 과거 데이터를 기반으로 미래값을 예측하고, 예측값과 실제값의 차이를 이용해 이상 여부를 판단한다[10]. 이 방식은 빠른 반응이 필요한 실시간 시스템에 주로 활용되지만, 예측 오류 누적 문제가 있다. 셋째, 유사도(Dissimilarity) 기반 방식은 현재 데이터와 정상 집단 사이의 거리나 유사도를 계산하여 이상 여부를 판단하며[11], 유클리드 거리, 코사인 유사도, 마할라노비스 거리 등이 활용된다.

이 중에서도 재구성 기반 방식은 비선형의 데이터 패턴에 적합하고, 고차원의 시계열 데이터 처리에 적합한 장점이 있으며, 복잡한 이상 유형을 정밀하게 탐지할 수 있다는 장점이 있다.

2.3 블록체인 이상 탐지 연구

블록체인은 모든 거래 내역이 투명하게 기록되므로 외부에서도 거래 흐름을 감시하고 분석할 수 있다는 장점이 있어, 블록체인 데이터를 통해 금융 사기 및 자금 세탁 등의 이상 행위를 탐지하는 시도가 많이 진행되고 있다[12]. 특히, 블록체인 데이터는 시계열적 특성과 불균형적 분포를 가지며 라벨링된 이상 데이터가 매우 적기 때문에, 전통적인 지도학습 방식보다는 비지도 또는 준지도 학습 기반의 이상 탐지 모델들이 선호되고 있다.

기존의 블록체인에 대한 이상 탐지 연구는 주로 사기 행위 탐지에 집중되고 있으며, 의심되는 지갑 주소를 식별하거나[13], 폰지 사기와 같은 사기 거래 분석[14], 스마트 컨트랙트 코드 분석을 통한 사기 탐지[15]에 초점이 맞춰져 왔다. 하지만, 블록체인의 탈중앙화된 구조와 기술적 특성으로 인해 블록체인 이상 탐지 기술은 어려움을 겪고 있으며, 이제 연구가 시작되는 단계라 할 수 있다. 특히, 스테이블코인에 대한 이상 탐지 연구는 거의 이루어지지 않고 있다. 최근에 다층 시간 그래프 구조를 이용한 스테이블코인 이상 거래 분석[16]이 제안되었지만, 세밀한 이상 구간 탐지가 어렵고 사용자 간 거래만 다룬다는 한계를 지닌다.

III. USDT 스테이블코인의 이상 탐지

본 논문에서는 대표적 스테이블코인인 USDT에 대한 이상 탐지를 수행하고 분석된 결과를 제공한다. 연구 과정은 그림 1과 같은 단계로 진행된다. 우선, 이더리움 네트워크 상의 USDT 거래 데이터를 수집하고 분석해 이상 탐지에 적합한 6개의 피처를 추출한다. 이후에 이 데이터를 이용해 딥러닝 모델을 학습시키며, 디파이 서비스를 위한 이상 탐지 모델로 제안되었던 Anomaly VAE-Transformer 모

델[13]을 기반으로 파인튜닝한다. 그리고, 학습된 모델을 통해 USDT 데이터에 대한 이상 탐지를 수행하고 탐지된 이상 패턴에 대한 분석을 수행한다.

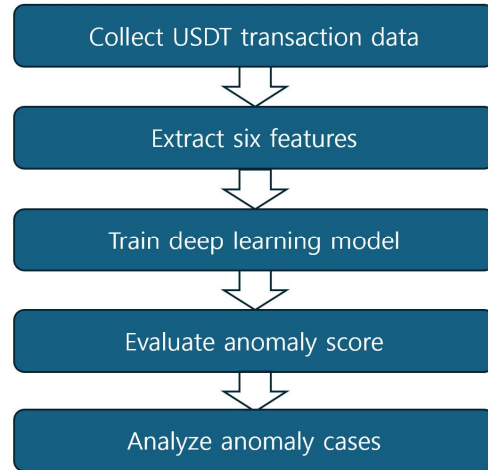


그림 1. USDT 이상탐지 프로세스
Fig. 1. Process of anomaly detection in USDT

3.1 USDT 데이터 수집과 피처 추출

본 논문에서는 이더리움 블록체인 상에서 ERC-20 토큰 표준을 따르는 USDT 거래 데이터를 수집하며, Google Cloud Platform에서 제공하는 BigQuery의 공개 데이터셋을 활용한다. BigQuery는 서버리스 데이터 웨어하우스 서비스로 대용량 데이터를 빠르게 분석하고 시각화하는 기능을 제공한다. BigQuery는 암호화폐에 관련된 다양한 데이터셋을 제공하고 있으며, 이 중에서 이더리움 메인넷 데이터를 포함한 `bigquery-public-data.crypto-ethereum` 데이터셋을 이용한다. 이 데이터셋의 테이블 중 ERC-20 토큰의 온체인 트랜잭션과 이벤트를 구조화한 `token_transfers` 테이블을 이용해 관련 데이터를 필터링해 수집한다.

이더리움 상에서 USDT의 구조는 그림 2와 같다. USDT 스마트 컨트랙트는 ERC-20 토큰을 구현하고 USDT 토큰의 전송과 관리를 담당하며, `treasury`는 자산을 보호하고 달러와의 페깅을 제어하며 토큰의 발행 및 소각을 담당한다. USDT와 관련된 주요 활동 이벤트는 다음과 같이 분류된다: 거래(Transfer)는 USDT 거래를 원하는 사용자 간의 USDT 토큰 이동 활동 이벤트이며, 발행(Issue)은 사용자로부터

달러를 예치받고 해당 수량만큼 신규 USDT를 온체인에 발행하는 활동 이벤트, 회수(Redeem)는 사용자가 보유한 USDT를 반환하고 달러로 상환하는 활동 이벤트이다.

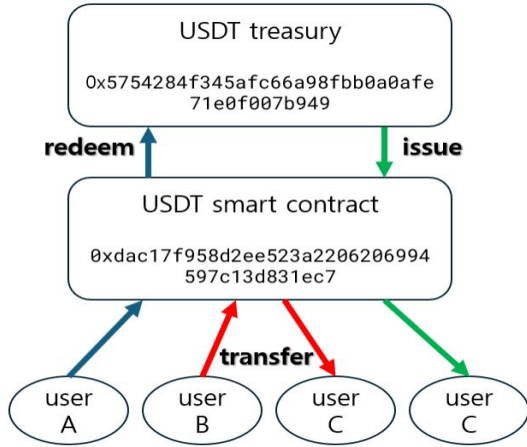


그림 2. 이더리움에서 USDT의 구조와 활동
Fig. 2. Architecture and activities of USDT in Ethereum

우리는 이상 탐지를 위해 2021년 1월 1일부터 2025년 4월 8일까지 기간에 발생한 데이터를 1시간 간격의 시간 단위 시계열 데이터로 재구성하였다. 그리고 그림 3과 같은 쿼리를 구성해 이상 탐지에 적합한 다음의 6가지 피처를 추출하였다. 그림 4는 6가지 피처의 시간에 따른 변동 추세를 보여준다. 전송량은 해당 시간 내 이동한 전체 USDT 전송량의 총합으로 자산 이동의 규모를 반영하는 피처이며, 거래 수는 해당 시간 내 발생한 USDT 전송 트랜잭션의 수이고 시장의 활동성 수준을 반영한다. 송신자 수는 해당 시간 동안 자신의 USDT를 전송한 고유한 송신자 주소의 수이고, 수신자 수는 해당

시간 동안 USDT를 전송받은 고유한 수신자 주소의 수를 나타내는 피처이다. 발행량은 해당 시간 동안 새롭게 treasury로부터 시장에 공급된 USDT의 양을 의미하며, 회수량은 해당 시간 동안 사용자로부터 회수된 USDT의 양이고 treasury로 유입된 금액의 총합을 의미한다.

3.2 딥러닝 모델 학습

본 논문에서는 USDT 거래의 시계열 데이터에 대한 이상 패턴을 효과적으로 탐지하기 위해, 그림 5와 같이 딥러닝 기반의 Anomaly VAE-Transformer 모델을 활용한다. 이 모델은 디파이 서비스의 이상 탐지를 위해 제안되었으며, VAE와 Transformer를 결합한 구조로 각각 비정상 거래 패턴에 대한 저차원 잠재 표현 학습과 장기 시계열 의존성 모델링에 강점을 가진다. VAE는 입력 데이터를 잠재 공간으로 인코딩한 후 이를 다시 복원하는 과정에서 정상 거래의 분포적 특성을 학습하며, 재구성 오류를 기반으로 이상을 식별할 수 있다. Transformer는 self-attention 메커니즘을 통해 시계열 내의 상호작용을 포착할 수 있어, 단기적 급변과 장기적 추세가 혼재된 이상 패턴을 정밀하게 탐지하는 데 유리하다. 따라서, VAE는 로컬 이상에 민감하게 반응하며, Transformer는 시간적 문맥을 고려한 구조적 이상을 포착하게 된다.

모델의 학습을 위해 우리는 전체 데이터 중 2021년 1월 1일~2021년 12월 31일 동안의 시간 단위의 6가지 피처를 추출해 사용한다.

```
SELECT
  TIMESTAMP_TRUNC(block_timestamp, HOUR) AS hour,
  SUM(SAFE_CAST(value AS NUMERIC)) / 1e6 AS redeemed_usdt
FROM
  `bigquery-public-data.crypto_ethereum.token_transfers`
WHERE
  token_address = '0xdac17f958d2ee523a2206206994597c13d831ec7' -- USDT ERC-20
  AND to_address = '0x5754284f345afc66a98fbb0a0afe71e0f007b949' -- Treasury address
GROUP BY
  hour
ORDER BY
  hour DESC;
```

그림 3. 시간당 USDT 회수량 획득을 위한 쿼리
Fig. 3. Query for retrieving the amount of redeemed USDT per hour

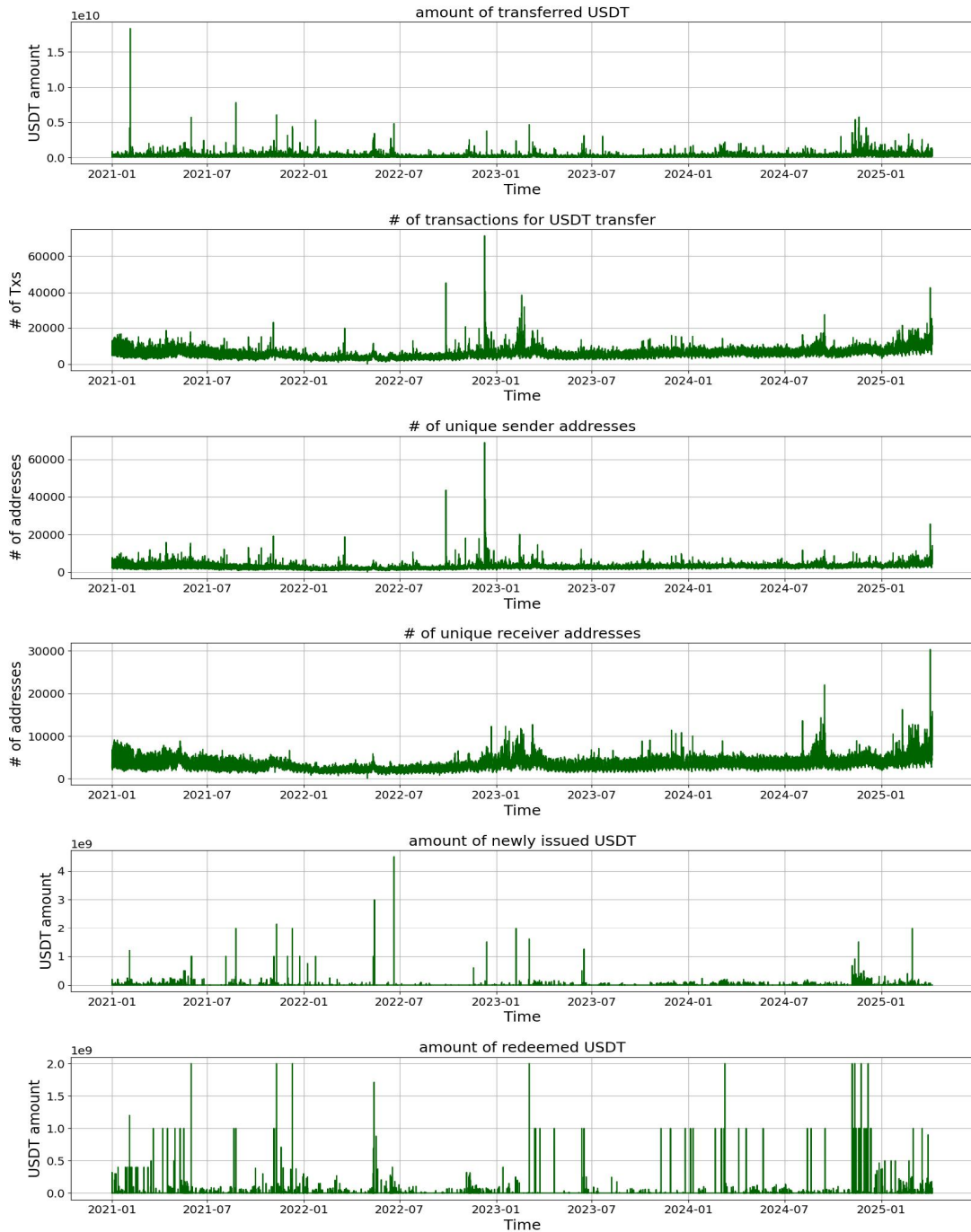


그림 4. USDT의 6가지 피처의 시간에 따른 추세 (2021-2025)
 Fig. 4. Time-series plot of 6 features in USDT (2021-2025)

모델의 학습은 비지도(Unsupervised) 학습 방식을 채택했다. 이는 블록체인 거래 데이터에 대해 정확한 이상 거래 레이블이 존재하지 않으며, 이상 패턴이 매우 희귀하고 다양하게 나타나기 때문이다. 또한, 정상 데이터를 기반으로 학습한 후, 정상 분포에서 벗어나는 패턴을 이상으로 탐지할 수 있어, 사

전 정의되지 않은 새로운 이상에도 효과적으로 대응할 수 있다.

모델의 학습 과정은 다음과 같이 VAE 학습과 Transformer 학습의 두 단계로 진행되며, 표 1에 기술된 하이퍼파라미터를 사용했다.

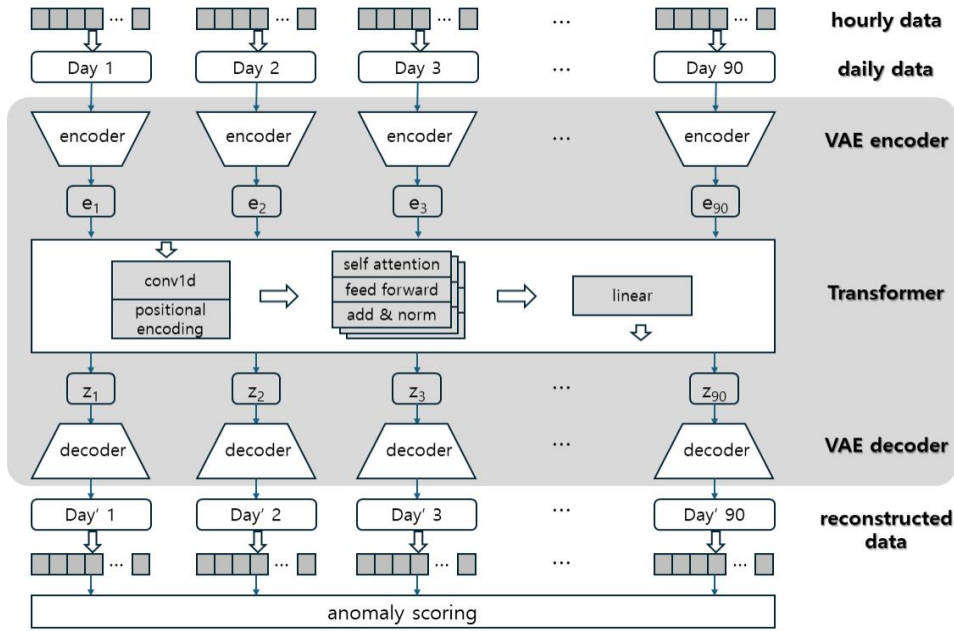


그림 5. Anomaly VAE-Transformer 모델의 구조
 Fig. 5. Architecture of anomaly VAE-Transformer

표 1. 모델 학습에 사용된 하이퍼파라미터

Table 1. Hyperparameters used in model learning

Submodel	Hyperparameter	Value
VAE	Window size	24
	Number of features	6
	Dimension of latent space	64
	Hidden layer size	[128, 64]
	Number of hidden layers	2
Transformer	Sequence length	90
	Dimension of representation	512
	Number of heads	8
	Dimension of feedforward network	512
	Number of encoder layers	3
	Dropout	0.2

3.2.1 VAE 인코더-디코더 학습

먼저 VAE의 인코더-디코더를 통해 입력된 시계열 데이터를 잠재 공간으로 압축하고 다시 복원하는 과정을 학습한다. 시간 단위(Hourly)의 학습 데이터 24개를 합쳐 일 단위(Daily) 데이터를 구성해 입력하고, 인코더를 통해 임베딩하고 이 결과를 디코더에 입력해 재구성된 일 단위 데이터를 생성한다. 이 결과와 원본 데이터 간의 재구성 오차 (Reconstruction error)를 최소화할 수 있도록 ELBO loss를 이용해 VAE를 최적화한다. 이 학습을 통해

모델은 일 단위 정상 데이터의 특성을 압축 표현할 수 있는 잠재 표현을 학습하게 된다.

총 8760개의 데이터로부터 슬라이딩 윈도우 기법을 적용해서 8735개의 일 단위 데이터 윈도우를 구성하였고, 이 윈도우들을 셔플링해서 80%는 학습에, 나머지 20%는 검증에 사용하였다. 그리고 잠재 공간의 차원 수와 히든 레이어 수를 변경해 가며 실험을 수행했고, 이 중에 잠재 공간 차원 수가 64, 히든 레이어 수가 2일 때 가장 우수한 성능을 보였으며 그림 6은 이때의 오차를 보여준다.

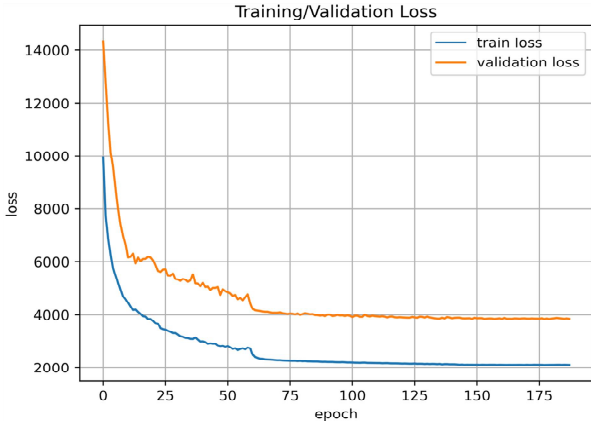


그림 6. VAE 학습 과정에서 오차 변화 (잠재 공간 차원수=64, 히든레이어=[128, 64])

Fig. 6. Loss change in VAE learning process (latent space dimension=64, hidden layer=[128, 64])

3.2.2 변환기(Transformer) 학습

앞서 학습된 VAE의 인코더를 이용해 90일간의 연속된 데이터에 대한 잠재 표현 시퀀스를 구하고, 이를 변환기에 입력해 변환기가 복원 시퀀스를 생성하는 과정을 학습한다. 이때, 복원 시퀀스와 원본 시퀀스의 재구성 오차를 최소화할 수 있도록 변환기를 최적화한다. 이 학습을 통해 모델은 90일간의 일 단위 데이터의 이상 패턴에 대한 민감도를 강화한다.

먼저 슬라이딩 윈도우 기법을 사용해 90일간의 잠재 표현 시퀀스를 담은 윈도우를 구성하고, 이 윈도우들을 셔플링해서 80%는 학습에 사용하고 20%는 검증에 사용하였다. 학습은 MSE(Mean Squared Error) 오차를 최소화하도록 진행되었으며, Adam 최적화 알고리즘을 사용했다.

3.3 이상 스코어 계산

학습된 Anomaly VAE-Transformer는 각 시간 구간 별로 입력된 USDT 거래의 시간 단위 데이터를 기반으로 재구성 데이터를 생성한다. 본 논문에서는 입력 데이터와 재구성 데이터 간의 차이를 기반으로 각 시간 구간의 이상 스코어를 계산한다. 해당 스코어는 각 시간 구간의 거래가 정상적인 거래 흐름으로부터 얼마나 이탈해 있는지를 정량적으로 나타낸다.

이상 탐지의 대상 데이터는 2022년 1월 1일부터 2025년 4월 8일까지 총 28656개의 시간 구간을 이용한다. 먼저 24개씩 시간 단위 데이터를 합쳐 일 단위 데이터를 구성하고, 이를 VAE 인코더에 입력해 일 단위 잠재 표현을 생성한다. 그리고, 슬라이딩 윈도우 방식을 사용해 90일간의 연속된 잠재 표현 시퀀스를 포함하는 윈도우를 구성해 변환기에 입력한다. 이후, 변환기가 생성한 재구성 시퀀스를 일 단위 잠재 표현으로 나누어 VAE 디코더에 입력해 일 단위 재구성 데이터를 획득한다. 그리고 여기에 포함되어있는 24개의 시간 단위 재구성 데이터 각각에 대해 원본 시간 단위 데이터와의 오차를 계산하며, 두 피쳐 벡터간의 유클리드 거리를 이용한다.

슬라이딩 윈도우 방식을 사용하기 때문에, 각 시간 구간은 최대 90개의 윈도우에 포함될 수 있다. 우리는 각각의 윈도우를 통해 계산된 특정 시간 구간의 오차들에 대한 평균을 계산해 이를 해당 시간 구간의 이상 스코어로 사용한다. 이러한 이상 스코어는 재구성 기반으로 계산되기 때문에, 이상 거래가 발생한 구간에서는 모델이 학습한 정상 분포에서 벗어나고 재구성 오차가 커져 높은 이상 스코어를 가지게 된다. 이를 통해 특정 시간 구간의 이상 스코어가 임계치 θ 를 넘는 경우 비정상적인 거래 행위 또는 이벤트가 발생했음을 탐지할 수 있다.

IV. 이상 탐지 결과 및 분석

이상 탐지 연구에서는 종종 정확한 레이블링이 없고 명확하지 않은 데이터를 다루게 되며, 이 경우 F1 score와 같은 전통적인 정량 성능 평가 지표를 사용하기 어렵다. 특히, 스테이블코인에 대해서는 레이블링된 이상 데이터가 존재하지 않아 성능 평가를 수행할 수 없는 상황이다. 본 논문에서는 대신에 딥러닝 모델을 이용해 탐지한 이상 구간들에 대해 사례별 분석을 수행한다.

3장에서 서술한 Anomaly VAE-Transformer를 이용해 각 시간 구간의 이상 스코어를 구했으며, 그림 7은 이상 스코어의 분포를 로그 스케일로 나타낸다. 대부분의 구간은 낮은 이상 스코어를 가지는 반면

에 일부 몇 개의 구간은 비정상적으로 높은 이상 스코어를 가지고 있음을 볼 수 있고, 이 구간이 이상 행위가 발생한 구간이라고 추론할 수 있다.

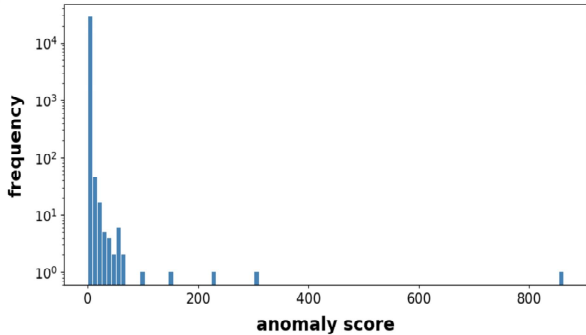


그림 7. 이상 스코어의 로그 스케일 분포
Fig. 7. Log scale distribution of anomaly score

우리는 전체 스코어 중 상위 0.01%의 이상 스코어를 가지는 구간이 이상 구간이 되도록 임계치 θ 를 설정했으며, 그 결과로 탐지된 이상 구간들은 표 2와 같다. 우리는 각 이상 구간에서 발생했던 USDT 거래 내역을 분석하고 6개 피처의 변동을 파악해 구체적 이상 패턴을 도출하고, 당시의 외부 사건들과 연계해 이상 행위의 원인을 추론하였다.

4.1 사례 1: rank #1[2022-06-20 15:00~16:00]

이 구간과 주변 구간들에서 6개 피처의 변동을 살펴보면 그림 8과 같이 갑작스러운 대규모 USDT issue 활동이 발생했음을 알 수 있다. 그리고, 이 구간에 대한 온체인 데이터 트랜잭션을 살펴보니 treasury에서 테더가 관리하는 계정으로 45억 달러의 USDT 전송이 이루어졌다. 이러한 돌발적 활동으로 인해 높은 이상 스코어를 가지게 되어 이상 행위로 탐지된 것으로 파악된다. 실제로 2022년 6월 20일에 USDT를 관리하는 테더는 역사상 최대 규모의

USDT 소각을 단행했고, 이 중 이더리움 네트워크에서 45억 달러를 소각했다. 이 당시 테라 사태 및 Celsius 유동성 위기 등으로 인해 사용자들이 대규모로 USDT를 상환했고, 테더는 이에 대응하여 해당 수량만큼의 USDT 토큰을 소각한 것으로 발표되었다. 위 트랜잭션이 소각을 위해 treasury에서 45억 달러의 USDT를 테더 계정으로 이동시킨 후 소각한 것으로 알려졌다. 이 소각 행위는 기존의 정상적인 패턴에서 벗어나는 갑작스런 활동이었으며, 본 모델이 이상 행위를 성공적으로 탐지했음을 보여준다.

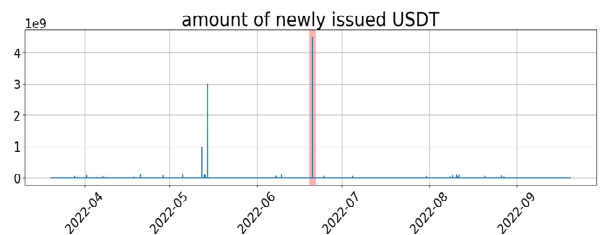


그림 8. (사례 1) 핵심 피처의 시간에 따른 추세
Fig. 8. (Case 1) Time-series plot of important features

4.2 사례 2: rank #2[2022-12-9 16:00~17:00]

이 구간과 주변 구간들에서 6개 피처의 변동을 살펴보면 그림 9와 같이 다수의 송신자들에 의한 거래 트랜잭션들이 급격히 발생했음을 알 수 있다. 이 날, 미국의 암호화폐 거래소인 코인베이스는 최근의 FTX 붕괴 등의 사건으로 인해 USDT의 신뢰성이 하락했으며 고객들에게 USDT를 USDC로 전환하도록 권장하는 발표를 했다. 이로 인해 다수의 일반 사용자들이 자신이 보유하고 있던 USDT를 전환했으며, 그림의 대규모 트랜잭션들이 이를 반영하고 있다고 파악된다. 본 모델이 이러한 다수 사용자들의 갑작스러운 거래 증가를 효과적으로 이상 패턴으로 탐지했음을 알 수 있다.

표 2. 이상 스코어의 내림차순 기준으로 탐지된 이상 구간
Table 2. Detected anomalies in descending order of anomaly score

Score rank	Period	Anomaly score
#1	2022-06-20 15:00 ~ 16:00	862.662327
#2	2022-12-09 16:00 ~ 17:00	309.320498
#3	2022-05-14 12:00 ~ 13:00	231.008841
#4	2023-03-04 10:00 ~ 11:00	155.145179

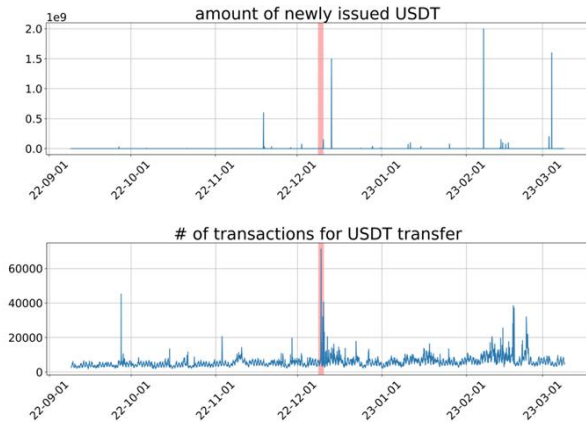


그림 9. (사례 2) 핵심 피처의 시간에 따른 추세
Fig. 9. (Case 2) Time-series plot of important features

4.3 사례 3: rank #3[2022-5-14 12:00~13:00]

그림 10을 보면 5월 12일부터 급작스럽게 USDT의 전송량과 거래 트랜잭션 수가 증가한 것을 볼 수 있으며, 특히 이 구간에서 비정상적인 활동이 두드러지게 확인된다. 이 시기에 테라 사태로 인해 USDT의 디페깅 현상이 발생했으며, 전체 스테이블코인 시장에 대한 불안감이 확산되어 대규모 상환요청이 발생했고 테더는 이 상황을 신속히 처리하는 대응을 수행했다. 아래 그림은 이러한 대규모 상환과 대응 활동이 반영된 것으로 파악된다. 그리고, 본 모델은 갑작스러운 전송량과 거래 증가를 이상 패턴으로 성공적으로 탐지했음을 알 수 있다.

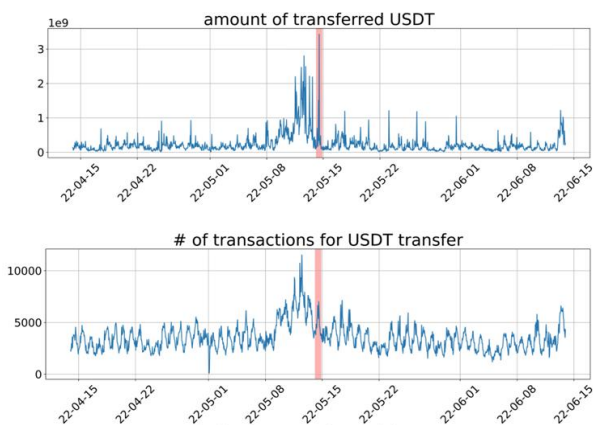


그림 10. (사례 3) 핵심 피처의 시간에 따른 추세
Fig. 10. (Case 3) Time-series plot of important features

4.4 사례 4: rank #4[2023-3-4 10:00~11:00]

그림 11을 보면 이 구간에서 대규모의 issue와 redeem 행위가 발생했음을 알 수 있다. 이 날 USDT의 시가총액이 처음으로 1000억 달러를 돌파했다고 발표되었으며, USDC등 경쟁 스테이블코인에 대한 신뢰성 문제가 불거지며 USDT로 자금이 급격하게 몰린 시기였다. 이로 인해 테더는 급격하게 증가한 유동성을 관리하기 위해 대규모 issue와 redeem을 수행한 것으로 파악된다. 이 사례는 본 모델이 이러한 대규모 유동성 변화에 대해서도 효과적으로 이상 패턴을 탐지했음을 보여준다.

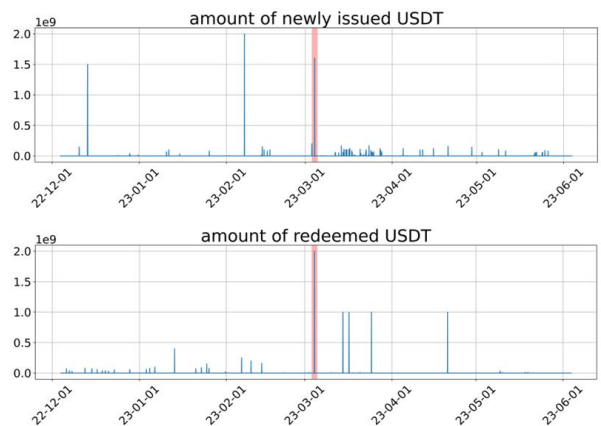


그림 11. (사례 4) 핵심 피처의 시간에 따른 추세
Fig. 11. (Case 4) Time-series plot of important features

4.5 기존 연구와의 비교 및 차별성

스테이블코인의 이상 탐지를 위한 연구들은 드물게 진행되고 있으며, 최근의 연구들은 주로 통계적 이상 식별에 초점이 맞춰져 있다. 예를 들어, [16]은 이더리움 상의 스테이블코인 거래 흐름을 다층 시간 네트워크로 모델링해서 테라 사태 전후의 거래 변화를 분석하였다. 그러나 이 연구는 스테이블코인의 발행과 회수를 고려하지 않고 사용자 간 거래 분석에 중점을 두었으며, 이상 거래를 효과적으로 탐지하는 기능이 부족하다.

반면, 본 논문은 시계열 기반의 딥러닝 접근 방식을 제공하여 USDT 거래 데이터를 시간 단위로 집계하고 재구성 기반의 비지도 학습 모델인 Anomaly VAE-Transformer를 통해 이상 구간을 효과적으로 탐지할 수 있다. 특히, 재구성 오차 기반의 이상 스코어를 통해 갑작스러운 대규모 발행(사례

1), 다수 사용자들의 거래 활동 증가(사례 2), 갑작스러운 거래량 증가(사례 3), 대규모 유동성 변화(사례 4) 등 다양한 형태의 이상 거래를 탐지할 수 있다는 점에서 높은 실용성을 가진다. 또한, 제안 방식은 향후 실시간 이상 탐지 시스템으로의 확장이 가능하다는 점에서 활용성이 높다.

V. 결 론

본 논문에서는 대표적인 스테이블코인인 USDT의 이더리움 기반 온체인 거래 데이터를 활용하여 이상 탐지를 수행하였다. 이를 위해 시간 단위로 데이터를 수집하고 분석해 6가지 주요 피처를 추출하였으며, Anomaly VAE-Transformer 모델을 활용해 학습 과정을 거쳐 이상 스코어를 계산하였다. 그리고 이를 실제 데이터에 적용해 주요 이상 패턴을 탐지했다. 그리고, 탐지된 이상 구간에 대한 분석을 통해 본 연구가 급격한 거래량의 변화, 비정상적인 발행 및 소각 이벤트 등 다양한 이상 패턴을 효과적으로 탐지했음을 보였다.

본 논문의 주요 기여는 다음과 같다. 첫째, 스테이블코인 거래 데이터에서 이상 탐지를 위한 주요 피처를 추출해 재구성하는 방식을 제안하였다. 둘째, 비지도 학습 기반 딥러닝 모델을 구성하고 USDT 거래 흐름 내 이상 구간을 정량적으로 탐지하였다. 셋째, 탐지된 이상 구간에 대한 정성적 분석을 통해 제안 방식의 효과성을 실증하였다.

제안된 방법은 향후 스테이블코인 생태계에서의 위험 관리 및 이상 행위 조기 탐지에 활용될 수 있을 것으로 기대된다. 다만 본 연구는 다음과 같은 한계도 존재한다. 첫째, 본 연구는 이더리움 기반의 USDT 거래 데이터만을 대상으로 하며, 다양한 스테이블코인에 대한 확장 연구가 필요하다. 둘째, 라벨링 없는 비지도 학습 모델이다 보니 임계값 설정이나 이상 구간 분석을 객관화 할 수 있는 추가 연구가 필요하다. 향후에는 이를 보강해 다양한 스테이블코인들이 교환되고 연결되는 탈중앙화 거래소에 대한 이상 탐지를 연구할 계획이다.

References

- [1] D. Li, D. Han, T. Weng, Z. Zheng, H. Li, and K. Li, "On Stablecoin: Ecosystem, architecture, mechanism and applicability as payment method", *Computer Standards & Interfaces*, Vol. 87, pp. 103747, Jan. 2024. <https://doi.org/10.1016/j.csi.2023.103747>.
- [2] Tether, Digital money for a digital age, <https://tether.to/> [accessed: May 16, 2025]
- [3] M. Carvalho, Rubens, H. Inácio, and R. Marques, "Stablecoin: A Story of (In)Stabilities and Co-Movements Written Through Wavelet", *Journal of Risk and Financial Management*, Vol. 18, No. 1, Jan. 2025. <https://doi.org/10.3390/jrfm18010020>.
- [4] H. Choi and H. Kim, "A blockchain-based NFT blood donation certificate management system", *Journal of KIIT*, Vol. 22, No. 9, pp. 133-144, Sep. 2024. <https://doi.org/10.14801/jkiit.2024.22.9.133>.
- [5] K. Choi, J. Yi, C. Park, and S. Yoon, "Deep learning for anomaly detection in time-series data: review, analysis, and guidelines", *IEEE Access*, Vol. 9, pp. 120043-120065, Aug. 2021. <https://doi.org/10.1109/ACCESS.2021.3107975>.
- [6] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep learning for anomaly detection: A review", *ACM computing surveys (CSUR)*, Vol. 54, No. 2, pp. 1-38, Mar. 2021. <https://doi.org/10.1145/3439950>.
- [7] Y. Zhang, J. Wang, Y. Chen, H. Yu, and T. Qin, "Adaptive memory networks with self-supervised learning for unsupervised anomaly detection", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 35, Nno. 12, pp. 12068-12080, Jan. 2022. <https://doi.org/10.1109/TKDE.2021.3139916>.
- [8] S. Lin, R. Clark, R. Birke, S. Schönborn, N. Trigoni, and S. Roberts, "Anomaly detection for time series using vae-lstm hybrid model", *Porc. ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Barcelona, Spain, May 2020. <https://doi.org/10.1109/ICASSP40776.2020.9053558>.
- [9] X. Wang, D. Pi, X. Zhang, H. Liu, and C. Guo,

"Variational transformer-based anomaly detection approach for multivariate time series", *Measurement*, Vol. 191, pp. 110791, Mar. 2022. <https://doi.org/10.1016/j.measurement.2022.110791>.

[10] M. Munir, S. A. Siddiqui, A. Dengel, and S. Ahmed, "DeepAnT: A deep learning approach for unsupervised anomaly detection in time series", *IEEE Access*, Vol. 7, pp. 1991-2005, Dec. 2018. <https://doi.org/10.1109/ACCESS.2018.2886457>

[11] L. Shen, Z. Li, and J. Kwok, "Timeseries anomaly detection using temporal hierarchical one-class network", *Advances in Neural Information Processing Systems*, Vol. 33, pp. 13016-13026, 2020.

[12] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "Ai-powered fraud detection in decentralized finance: A project life cycle perspective", *ACM Computing Surveys*, Vol. 57, No. 4, pp. 1-38, Dec. 2024. <https://doi.org/10.1145/3705296>.

[13] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact", *Future Generation Computer Systems*, Vol. 102, pp. 259-277, Jan. 2020. <https://doi.org/10.1016/j.future.2019.08.014>.

[14] S. Hu, Z. Zhang, B. Luo, S. Lu, B. He, and L. Liu, "Bert4eth: A pre-trained transformer for ethereum fraud detection", *Proc. ACM Web Conference 2023*, Austin TX USA, pp. 2189-2197, Apr. 2023.

[15] Z. Zheng, W. Chen, Z. Zhong, Z. Chen, and Y. Lu, "Securing the ethereum from smart ponzi schemes: Identification using static features", *ACM Transactions on Software Engineering and Methodology*, Vol. 32, No. 5, pp. 1-28, Jul. 2023. <https://doi.org/10.1145/3571847>.

[16] C. Ba, R. Clegg, B. Steer, and M. Zignani, "Investigating shocking events in the ethereum stablecoin ecosystem through temporal multilayer

graph structure", *arXiv preprint*, arXiv:2407.10614, Jul. 2024. <https://doi.org/10.48550/arXiv.2407.10614>.

[17] A. Song, E. Seo, and H. Kim, "Anomaly VAE-Transformer: A Deep Learning Approach for Anomaly Detection in Decentralized Finance", *IEEE Access*, Vol. 11, pp. 98115-98131, Sep. 2023. <https://doi.org/10.1109/ACCESS.2023.3313448>.

저자소개

송 아 현 (Ahyun Song)



2005년 2월 : 한국과학기술원
전산학과(공학석사)
2005년 3월 ~ 현재 : 금융보안원
모바일보안팀 팀장
2022년 3월 ~ 현재 : 성균관대학교
컴퓨터공학과 박사과정
관심분야 : 정보보호, 블록체인

서 의 성 (Euseong Seo)



2002년 2월 : 한국과학기술원
전산학과(공학석사)
2007년 2월 : 한국과학기술원
전산학과(공학박사)
2012년 3월 ~ 현재 : 성균관대학교
소프트웨어학과 교수
관심분야 : 시스템SW, 임베디드
시스템, 클라우드 컴퓨팅

김 희 열 (Heeyoul Kim)



2002년 2월 : 한국과학기술원
전산학과(공학석사)
2007년 2월 : 한국과학기술원
전산학과(공학박사)
2009년 3월 ~ 현재 : 경기대학교
컴퓨터공학부 교수
관심분야 : 정보보호, 블록체인