정 보 보 호 학 회 지
제 34 권 제1호, 2024. 2

블록체인 탈중앙화 거래소 DEX의 취약점과 MEV 공격 기법 분석

최 낙 훈*, 김 희 열**

요 약

블록체인 기술의 발전과 중앙집중형 금융서비스의 취약성과 불신에 대한 우려가 커지면서 탈중앙화 금융(DeFi)과 탈중앙화 거래소(DEX)가 유망한 대안으로 떠올랐다. 본 논문에서는 특히 Uniswap에 초점을 맞춰 DeFi 내의 과제와 문제를 살펴본다. 우리는 DeFi 및 DEX의 현재 상태에 대한 배경 지식을 제공하여 MEV(Maximal Extractable Value) 공격에 대한 취약성을 강조한다. 우리의 접근 방식에는 MEV 공격 패턴을 식별하고 분석하기 위한 Uniswap에 구조 분석이 포함된다. 이 연구는 DEX 보안을 강화하고 MEV 위험을 완화하기 위한 귀중한 지침을 제공하여 DeFi 생태계의 이해관계자에게 필수적인 리소스 역할을 한다.

Ⅰ. 서 론

블록체인 기술의 발전과 함께 대두되는 탈중앙화 금융(DeFi)과 탈중앙화 거래소(DEX)는 중앙화된 관한과 서버, 관리자 없이 여러 종류의 암호화폐를 거래할 수 있는 플랫폼을 제공하는 방법으로 금융 기술의 혁신적인 전환점을 대표한다. 블록체인 기술 발전에 따라 그 부산물인 암호화폐와 ERC-20, ERC-721 등의 표준에 따라 생성된 토큰화 자산이 사용되고 있다. 이에 따라 금융 시장은 암호화폐의 거래를 위한 중앙집중화된 거래소(CEX)를 서비스하고 있다. 하지만, 잇따른 거래소 해킹과 자산 탈취, 중앙화된 거래소의 판단에 대한 신뢰성 부족 등 다양한 문제가 발생하고 있다. 블록체인 연구자들은 이러한 중앙화된 서비스에서 발생하는 문제와 탈중앙화라는 블록체인의 기조를 강화하기 위한 금융 기술인 DeFi와 DEX를 제안하였다. DeFi는 전통적인 중앙 집중형 금융 체계를 대체하는 블록체인 기반의 금융 서비스를 제공하며, DEX는 이러한 새로운 금융 생태계에서 사용자들에게 암호화 자산의 직접적인 자산 교환의 기회를 제공한다. 탈중앙화된 금융은 블록체인 스마트 컨트랙트(smart contract)를 통해 P2P거래를 촉진하고, 거래의 투명성과 보안을 강화하는 동시에 중앙 집중식 거래소에서 발생하는 관리자의 악의적 행위 및 권한 탈취 등의 위험을 배제한다. 이는 금융 거래의 투명성과 접근성을 극적으로 개선하고 있다[1]. DeFi와 DEX는 전세계적으로 금융 서비스의 이용 가능성을 확장하고 있으며, 이는 전통적인 금융 시스템에 대한 중요한 도전으로 여겨진다[2].

DeFi와 DEX는 블록체인의 새로운 기술 혁신 속에서 많은 관심을 받고 있으나, 이와 동시에 다양한 보안 위협에 직면해 있다. 스마트 컨트랙트의 취약점, 시장 조작, 프론트 러닝(Front-running)과 같은 다양한 공격 기법들이 이 분야의 주요 위협으로 부각되고 있다[3][4]. 중대한 위협 중 하나인 MEV(Maximal Extractable Value) bot의 등장은 분산 금융의 취약점을 통해 이익을 취득하며, 사용자의 거래 체결에 대한 수수료와 교환비 손해를 초래하고 있다. 블록체인 자체의 보안취약점 혹은 DEX의 취약점을 공략하는 MEV의 다양한 시도가 발견되고 있으며, 거래 무결성과 공정성을 훼손하고 있다. 탈중앙화된 금융 서비스에 대한 보안 문제와 공격은 사용자의 자산을 직접적인 위험에 노출시키며, 블록체인 플랫폼과 서비스에 대한 신뢰성을 훼손하며, 전체 시장의 안정성에 영향을 미치고 있다[5]. 공정하고 신뢰 되는 금융환경을 위

본 연구는 2024년 경기대학교 대학원 연구원장학생 장학금 지원에 의하여 수행되었음.
* 경기대학교 컴퓨터과학과 정보보호연구실 (대학원생, nakhoon.choi@kyonggi.ac.kr)
** 경기대학교 AI컴퓨터공학부 (교수, heeyoul.kim@kyonggi.ac.kr)

해 분산 금융의 보안취약점과 공격 방법에 대한 철저한 분석과 이해는 필수적이다. 이러한 분석은 DeFi와 DEX의 지속 가능한 성장과 발전을 위한 중요한 기반을 제공할 것이다.

본 논문은 블록체인 금융서비스인 DeFi와 DEX 시스템의 취약점과 이에 기반하는 다양한 공격 기법을 확인한다. 이를 통해 시장 동향과 사용자 행동, 보안 문제를 파악함으로써, 이 분야의 보안 강화와 효율적인 시장 운영 방안을 모색한다. DEX에서 발생하는 프론트 러닝 기법을 기반으로 하는 MEV-bot의 공격 방식과 DEX 차익거래 등의 여러 공격을 분석한다. DEX거래에서 차익거래 봇과 프론트러닝 기반 MEV-bot은 전체 거래량의 일평균 10억달러 중 4.8억 달러에 이르며, 일평균 전체 볼륨의 45%를 차지한다. 우리는 이러한 공격 기법을 소개하고 공격량 측정을 통해 MEV 공격자의 심각성을 재조명한다. 이러한 분석과 연구는 DeFi와 DEX의 안정성과 투명성을 향상시키는데 기여할 뿐만 아니라, 이 분야의 학문적 연구와 산업적 실천에 중요한 참고 자료가 될 것이다.

본 논문은 2장에서 블록체인과 탈중앙화 금융 및 탈중앙화 거래소에 대해 전반적으로 설명하며, 3장에서블록체인과 탈중앙화 거래소에 존재하는 취약점과 그 취약점을 기반으로 하는 공격유형을 분석한다. 마지막으로 4장에서 결론을 서술하며 논문을 마무리한다.

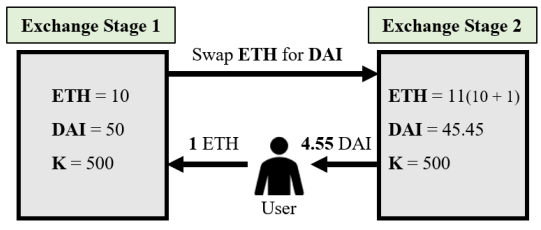
Ⅱ. 블록체인과 DeFi & DEX

2.1. 블록체인(Blockchain)

블록체인과 탈중앙화 금융은 현대 금융 기술의 핵심요소로, 전통적인 금융 시스템의 한계를 극복하고자 하는 혁신적인 접근 방식을 제공한다. 블록체인은 정보의 분산 저장과 암호화된 거래 기록을 통해 데이터의 무결성과 보안성을 보장한다. 각 거래는 블록으로 알려진 데이터 단위에 기록되며, 이 블록들은 체인으로 연결되어 변조가 어려운 특성을 가진다. 각 블록은 이전 블록의 해시와 연결되어 블록체인의 모든 거래가 시간 순서대로 연결되어 있음을 보장한다. 블록체인의 각 블록을 체인으로 연결하는 네트워크상의 작업을 합의라 부르며, 블록체인의 구조와 특성에 따라 PoW, PoS, DPoS 등의 다양한 합의 알고리즘이 존재한다[6]. 이러한 합의를 통해 선출된 블록생성자에 의해 생성된 블록은 네트워크의 모든 참여자에게 전송된다. 네트워크 참여자는 거래의 유효성을 확인하고 기록하는 방식으로 네트워크상의 모든 참여자에게 투명하게 공개된 네트워크를 유지한다. 이 과정은 중앙 집중식 기관이나 중개자 없이도 신뢰할 수 있는 거래 환경을 조성한다. 블록 생성 보상으로 생성되는 암호화폐와 스마트 컨트랙트를 통해 생성되는 ERC-20, ERC-721와 같은 토큰형 암호화폐는 오더북 기반 거래소 서비스를 통해 거래된다. 하지만, 거래소 자체의 빈번한 해킹으로 인한 자산 피해와 중앙 거래소 판단에 의한 암호화폐 등록 등 관리자에게 의존하는 문제점이 있다. 이를 위해 스마트 컨트랙트를 통해 탈중앙화된 거래소를 만들기 위한 시도로 DEX가 등장하였다.

2.2. 탈중앙화 금융(Decentralized Finance)과 탈중앙화 거래소(Decentralized Exchange)

탈중앙화 금융은 블록체인을 기반으로 하는 금융 서비스를 탈중앙화된 환경에서 관리자없이 제공한다. 전통적인 금융 서비스가 은행이나 거래소 기업을 통해 이루어지는 것과 달리, DeFi는 스마트 컨트랙트를 통해 금융 거래를 자동화하고, 사용자가 직접 거래에 참여할 수 있게 한다. 이더리움에서의 초기 DEX 프로젝트인 EtherDelta는 오더북 기반을 기반으로 구매자와 판매자를 연결하고, 입찰 가격과 최저가격의 매칭을 지원하는 방식을 제안했다. 하지만, 오더북 기반의 DEX는 거래 체결에 대한 너무 많은 가스 수수료가 필요했으며, 매수 및 매도 거래를 미리 등록하기 때문에 거래를 생성하서나 취소하는데 큰 부담이 존재했다. 또한, 유동성 부족으로 인해 사용성과 확장성에 대한 문제가 발생하였다. 오더북 기반 거래소는 블록체인 환경에 부적합하였으며, 이를 해결하기 위해 AMM(Automated Market Maker) 기반 탈중앙화 거래소가 제안되었다[7]. AMM은 누구나 유동성을 거래소



〔그림 1〕 CPMM 기반의 DEX의 토큰 교환(Swap) 예시.

에 제공할 수 있으며, 유동성을 바탕으로 알고리즘으로 결정된 가격으로 사용자 간 거래를 지원한다.

2023년 전체 DEX의 거래량은 $889 billion에 이르며, 전체거래자는 4,320만여명에 이른다. 우리는 DEX 분석을 위해 가장 큰 거래볼륨과 사용자 수를 가지는 Uniswap에 대한 분석을 수행한다. Uniswap은 오픈소스 DeFi 프로젝트로, 스시스왑(SushiSwap)과 같은 거래소는 Uniswap 오픈소스를 기반으로 유사한 구조로 구성되었다. Uniswap은 AMM기반의 거래소로, 가격결정 알고리즘, 유동성 공급자, 토큰 페어로 구성된다. Uniswap은 AMM 모델 중 CPMM(Constant Product Market Maker) 모델을 사용한다. CPMM은 상수 곱셈 공식인 식 (1)을 통해 가격을 결정하며, X와 Y는 각 토큰(x, y)의 수량을 뜻하며, K는 수량의 곱을 뜻한다.

$$X^{*}\ Y = K \tag{1}$$

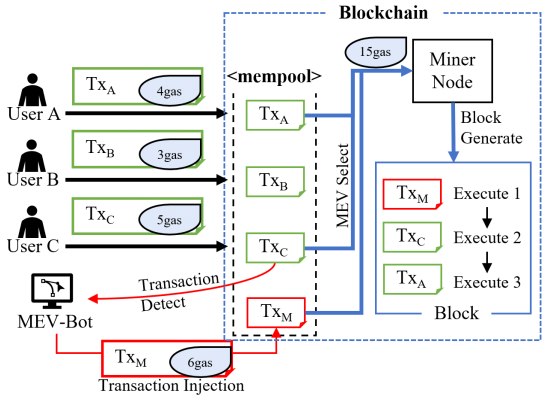
CPMM은 유동성 내에서 모든 거래 수행 후 변경된 X와 Y의 곱이 항상 일정하게 K로 유지되는 알고리즘이다. 토큰 페어풀에서 X를 Y로 교환할 때 X의 양은 줄어들고 Y의 양이 늘어나며, 그에 따라 x의 가격은 하락하고, y의 가격은 상승하며 K는 일정하게 유지된다. 그림 1은 CPMM 기반의 거래 예시를 보인다. 사용자는 거래 이전의 ETH대비 DAI의 가격을 1:5으로 인지하였지만, CPMM에 의해 유의미한 차이가 발생하는 일시적 가격 변동(Slippage)[8]이 발생하였다. 이러한 slippage는 거래소에 제공된 유동성의 양이 많을수록(K가 클수록) 거래 실행 시 발생하는 가격 변동량이 하락한다. 이러한 AMM의 특성에 따라 거래소는 유동성 확대를 위해 유동성 제공자에게 거래에 따른 수수료를 제공한다. 하지만, Uniswap은 블록체인에서 서비스되는 금융 거래소로, 블록체인을 사용함에 따라 발생하는 여러가지 문제점과 거래소 구조 및 프로젝트 구조에 따른 취약점이 존재한다. 우리는 이러한 블록체인 플랫폼과 DEX의 구조적 취약점과 여러가지 공격 유형에 대한 분석을 수행한다.

Ⅲ. 탈중앙화 거래소의 취약점과 공격유형 분석

DEX 사용자의 자산을 노리는 공격의 유형은 다양하다. 블록체인 커뮤니티와 연구자들 사이에는 DEX의 구조적 취약점을 통해 차익거래, 프론트러닝과 같은 방식으로 이익을 탈취하는 것이 공격인지 정당한 수익활동인지에 대한 논쟁이 이루어지고 있다[9]. 하지만, 우리는 이러한 행위에서 발생하는 이익이 다른 사용자의 자산을 탈취하는 과정으로 발생하는 것임으로 공격으로 규정하고 이를 분석하고자 한다. 이와 같은 '공격'은 일반 사용자의 구매과정에 개입하여 사용자가 더 높은 가격에 거래를 수행하도록 하여 이익을 발생시킨다. DEX 공격 행위는 DEX의 신뢰성을 뒷받침하는 블록체인의 투명성을 악용하여 불공정한 거래를 발생시키는 행위이며, DEX를 넘어 블록체인 플랫폼 환경에 대한 신뢰성을 파괴하는 행위이다. MEV-bot은 DEX에서 발생하는 일정 규모 이상의 모든 거래에 대해 이러한 공격을 수행하고 있으며, 사용자의 손실을 강제하고 있다[10]. 이 섹션에서는 DEX의 구조적 취약점과 이에 따라 발생하는 공격 유형을 분석한다.

3.1. 블록체인의 구조적 취약점과 공격유형

블록체인을 기반으로 하는 DEX는 블록체인의 구조적 특성을 동일하게 가지고 있다. 블록체인의 블록생성 메커니즘의 큰 특징은 MEV(Miner Extractable Value)이다. 블록체인 사용자의 트랜잭션은 바로 처리되는 것이 아닌 블록생성자 후보의 트랜잭션 대기공간인 mempool에서 보류되어 있다가, 선출된 블록생성자에 의해 선택되어 특정 블록에 삽입된 후 블록으로 가공되어 블록체인에 합류한다. 라운드에서 선출된 블록생성자(Ethereum Validator)는 mempool에서 계류중인 트랜잭션 중 가장 높은 수수료(gas)를 지불하는 트랜잭션들을 우선 선택하여 블록으로 가공하고자 한다. 채굴자는 MEV-bot과 마찬가지로 최대의 이익을 추구한다. 하지만, 대부분의 MEV를 차익거래 봇과 같은 MEV-bot이 취함에 따라 현재는 MEV를 Maximal Extractable Value이라 칭하고 있다. 그림 2는 블록체인에서 채굴자의 블록생성 메커니즘에 따른 트랜잭션 선택을 보인다. 그림 2의 MEV(Miner Extractable Value) 트랜잭션 선택에 따라 블록생성자는 mempool에서 가장 높은 수수료를 지불하는 트랜잭션을 블록에 추가하는 걸 확인할 수 있다. 채굴대기중인 임시 공개 트랜잭션 목록인 mempool은 블록체인 투명성에 의해 공개되어 있으며, 노드 어플리케이션을 통해 엑세스 가능하다. 프론트러닝 방식의 공격은 이에 착안하여 공개된 트랜잭션 대기 목록인 mempool의 트랜잭션 내용을 확인하여 기존 트랜잭션보다 먼저 처리되는 트



〔그림 2〕 블록체인 블록 생성자(Miner)의 MEV(Miner Extractable Value)거래 선택 및 선행 공격 (Front-running).

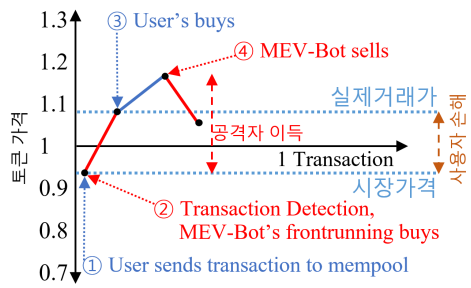
랜잭션을 네트워크에 전송할 수 있다. 이러한 방식은 2019년 Flash boys 2.0[11]에서 처음 제시되었다. 공격자는 mempool로 전송된 트랜잭션을 지속적으로 모니터링하며, 특정 조건을 만족하는 거래가 탐지될 경우 해당 거래의 결과를 미리 시뮬레이션하고, 이익이 생성될 조건의 조작된 거래를 먼저 실행하여 이익을 발생시킨다. 블록 생성 메커니즘에서 MEV 트랜잭션 선택에 의해 트랜잭션의 처리 순서는 네트워크에 트랜잭션이 실제 전송된 시간과 다를 수 있다. 하지만 DEX에서 토큰스왑, 유동성 제공과 같은 행위는 선후행위와 시간정보에 따라 시장가치에 변동성이 생긴다. 사용자는 이러한 요소로 인해 의도했던 거래와 다른 실제 거래수행으로 인한 손해가 발생한다.

Sandwith 공격은 DEX의 AMM모델을 대상으로 하는 프론트러닝 공격의 한 형태로, DEX 생태계에서 가장 많이 발생하는 프론트러닝 기반 공격이다. 식별된 샌드위치 공격의 볼륨은 2023년 1년동안 212억 달러에 이르며, 평균 공격 볼륨은 4만달러 정도이며, 2022년 1월부터 현재까지의 기간에서는 1,392억달러에 이른다. 일평균 샌드위치 봇의 트랜잭션 4,000여개이며 풀에서의 트랜잭션의 약 8%을 차지한다. 또한, 샌드위치 봇이 지불하는 수수료(gas)는 월평균 2,100ETH에 이르며, 트랜잭션에서 일반 사용자의 수수료보다 약 30% 많은 수수료를 지불한다. sandwich 공격은 직관적으로 설명하자면, 특정 조건에서 구매 거래가 실행된 예정일 때 MEV-bot은 동일한 토큰을 먼저 구매하고 거래가 실행된 직후 판매하여 그 차익만큼 수익을 창출한다. 그림 3은 sandwich 공격의 일례를 표현한 그림이다. sandwich 공격의 순서와 과정을 자세히 설명하면 아래와 같다:

1. DEX를 이용하는 일반 사용자는 자산 스왑을 위한 트랜잭션을 제출하고, 해당 트랜잭션은 블록체인 mempool에 기록된다;
2. 공격자는 블록체인 mempool을 모니터링하고 유동성 풀의 가격을 크게 변화시킬 것으로 예상되는 대규모 보류 트랜잭션을 탐지한다. 또한, 탐지에 따라 공격자는 사용자의 거래가 처리되기 전에 동일한 토큰에 대한 구매 주문을 더 높은 수수료(gas)로 제출하여 AMM에 따른 토큰 가격을 인위적으로 인상한다;
3. 사용자는 의도한 가격보다 높은 가격으로 토큰을 구매하게 되며, 거래 처리이후 거래 규모에 따라 토큰 가격은 더욱 상승한다;
4. 공격자는 피해자의 거래 직후 이전단계에 구매한 토큰을 인상된 가격으로 판매하여 그 차익만큼의 이익을 실현한다.

그림 3에서 MEV-bot의 붉은색 글씨로 표현되었으며, 편의상 직관적으로 확인할 수 있게 표시하였다. Bot의 수익을 더 확실하게 표시한다면 식 (1)의 CPMM에 따라 bot의 토큰 구매단계에서 실제 사용된 금액과 판매단계에서 실제 판매된 가격으로 표시된다. 차익거래 봇과 달리 sandwich 공격은 단일 트랜잭션에서 발생할 수 없는 구조이지만, Universal Router, Flashbot과 같은 중계 서비스를 통해 복수 개의 공격 트랜잭션이 구매-판매의 공격 로직이 긴밀하게 수행될 수 있도록 한다.

샌드위치 공격의 경우 프론트러닝 방식의 공격과 함께 백러닝 공격이 함께 수행된다. 백러닝 공격은 프론트러닝과 반대로 mempool에서 확인된 피해자의 트랜잭션의 바로 뒤나 그 이후에 처리될 수 있도록 목표

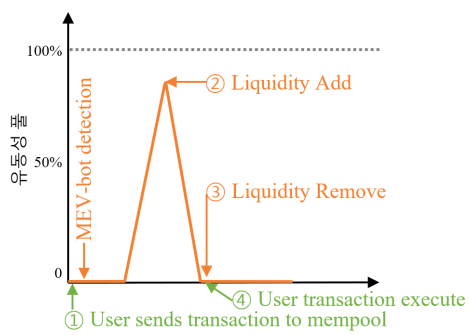


〔그림 3〕 Sandwich공격의 실행 과정 및 수익 창출 과정.

하는 공격방식이다. 이를 위해 MEV-bot은 대상 트랜잭션의 수수료와 거의 동일하거나 아주 약간 낮은 수수료로 트랜잭션을 생성한다. 공격자는 거래 규모가 큰 트랜잭션을 탐지했을 때 해당 거래 체결과 동시에 일시적으로 발생하는 높은 슬리피지에 따른 시세 차익을 위해 반대 주문을 제출한다.

3.2. 탈중앙화 거래소의 구조적 취약점과 공격유형

앞선 챕터에서는 블록체인의 블록 생성 과정에서의 MEV 특성에 의한 구조적인 공격 취약점에 대해 서술하였다. 이 챕터에서는 DEX가 가지는 구조적인 취약점과 DEX가 도입한 서비스에 의해 발생하는 취약점과 공격에 대해 확인한다. AMM을 기반으로 하는 탈중앙화 거래소는 대부분 유동성 제공자에 의한 유동성 풀로 운영된다. 이러한 유동성을 기반으로 하는 대표적인 공격기법은 Just-In-Time liquidity 공격(이하 'JIT'라 통칭함)이다. JIT 공격은 프론트러닝과 백러닝을 모두 포함하여 LP(Liquidity Pool) sandwich 공격이라 칭하기도 하지만, 본 논문에서는 JIT로 칭한다. JIT공격자에 의해 일시적으로 제공되는 유동성 평균 1,700만달러이며, 평균 피해자의 스왑 볼륨은 14만달러이다. JIT 공격자는 상위 25개의 계정에서 USDC3 풀의 유동성 거래량의 7,600억 달러중 7,400억 달러를 차지하였다. 상위 5개 계정으로 범위를 축소했을 때에도 3,000억달러의 유동성 차지율을 보였다. JIT 공격자는 소수지만 매우 큰 자산으로 시장을 형성한다. JIT는 일반적인 Sandwich 공격과 달리 유동성을 추가 및 제거하는 방식의 공격을 수행한다. 직관적으로 봤을 때 JIT는 사용자의 거래 탐지 후 그 앞뒤에 유동성을 추가하였다가 제거한다. 이를 좀 더 자세히 관측하면 그림 4와 같다. 그림 4는 단일 트랜잭션에서 유동성의 변화를 가정한다.

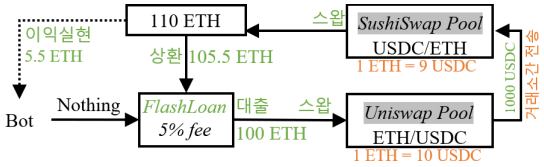


〔그림 4〕 Just-In-Time Liquidity의 실행 프로세스.

JIT를 간단한 예시와 함께 설명하자면, JIT 실행자가 유동성 공급자로서 대규모 스왑거래를 관측한다. 이때 공격자는 프론트러닝 방법을 통해 유동성 풀에 약 90% 공급량을 차지하도록 대규모 유동성을 공급한다. 대규모 스왑거래를 수행되면 해당 거래의 수수료는 JIT 실행자에게 지급되며, 거래 직후 유동성을 인출한다. JIT 공격은 특정 가능한 정도의 수의 bot만이 네트워크에 존재한다. Uniswap V3에서 추가된 집중 유동성에 의해 용이해진 공격 유형이지만, 공격자가 사용자의 거래보다 평균 269배의 자산을 동원해야 하는 특징이 있으며, 낮은 수익성을 보인다[12].

DEX에서 발생하는 MEV-bot의 활동에는 다양한 분산 거래소 간의 가격 차이를 활용하는 차익거래 전략이 있다. 분산 거래소 간 가격 차이는 주로 자산의 유동성이 낮거나, 시장 정보가 느리게 업데이트되는 경우 발생한다. 차익거래 봇은 실시간으로 여러 거래소의 가격을 모니터링하며, 한 거래소에서 저렴한 가격으로 자산을 구매하고, 다른 거래소에서 높은 가격으로 판매함으로써 이익을 실현한다. 이는 시장의 효율성을 높이고 거래소간 가격 균형을 맞추기위한 방안으로 기여한다고 여겨질 수 있다. 결국 사용자와 유동성 제공자의 손해를 발생시키고 이익을 생성하는 것으로 공격의 한 유형으로 정의될 수 있다. 차익거래 봇은 전체기간에서 약 32%의 MEV-bot 활동 볼륨을 차지하며, 일평균 12000여개의 트랜잭션을 생성한다. 차익거래 봇은 자신의 자산을 통해 차익거래를 수행할 수 있지만, Uniswap V2에서 도입된 Flashloan[13]을 통해 더 많은 공격 사례가 발견되고 있다. 그림 5는 플래시론을 통한 차익거래 수행 과정을 보인다.

플래시론은 풀에서 원하는 만큼의 토큰을 빌린 뒤 이를 이용하여 원하는 작업에 사용한 뒤 해당 금액과 이자를 한 트랜잭션 내에서 상환하는 대출방식이다. 플래시론은 일반 금융에서의 대출과 달리 담보와 신용이 필요없으며, 대출 실행 트랜잭션 실행전에 트랜잭션 시뮬레이션을 통해 한 트랜잭션 내에서 상환과 수수료 납부만 가능하다면 무제한으로 대출이 가능하다. 그림 5에서 플래시론을 이용한 차익거래는 거래소간 가격 격차를 통해 수수료 납부를 포함한 이득 최소값을 달성하는 거래에 대해 차익거래를 수행하게 된다. 플래시론을 이용한 차익거래뿐 아니라 유동성 풀의 가격을 조작하는 시작 조작, 프로토콜 해킹 등의 여러 공



〔그림 5〕 DEX flashloan 기반 차익거래 실행 프로세스.

격 사례가 존재한다. 플래시론과 플래시스왑은 최근 지속적으로 발생한 디파이 해킹 사례의 주요 수단으로 많이 언급되며 부정적인 여론이 형성되었다. 하지만, 유니스왑 팀을 비롯한 디파이 커뮤니티는 이러한 기능을 악용하여 공격에 사용한 것이 문제일 뿐 기능 자체에는 문제가 없다는 입장이다.

여러 MEV-bot은 대규모 거래가 탐지되는 시기에 가장 큰 활동과 이익을 생성한다. 유니스왑 팀과 커뮤니티는 이러한 MEV-bot의 활동이 정당한 경제활동이라고 주장하지만, 블록체인 기술의 신뢰성과 탈중앙화 금융 및 거래소의 공정 거래에 대해 신뢰성을 위해 MEV-bot의 활동을 제재될 필요성이 있다. 사용자 탈중앙화 시장에서-거래에 있어 자산 탈취의 위험성과 무분별한 bot의 활동은 시장 진입에 대한 진입 장벽이며, 기술 발전의 걸림돌이 될 것이다. DEX 거래를 위한 안전하고 공정한 거래 기술이 연구될 필요성이 있으며, 탈중앙화된 환경에서도 일반 사용자를 보호하기 위한 방안이 시급하다.

Ⅳ. 결 론

본 논문은 탈중앙화 거래소, 특히 Uniswap에 초점을 맞추어 Maximal Extractable Value (MEV) 공격이라는 탈중앙화 금융(DeFi) 분야의 중대한 위험을 강조한다. 이 연구는 DeFi 생태계의 복잡한 구조와 MEV-bot과 같은 정교한 위협에 대한 취약성을 드러낸다. 이러한 공격은 거래의 정확성뿐만 아니라 시장 역학과 전체적인 DeFi 시스템에 대한 신뢰에도 큰 영향을 미친다. 이러한 공격 분석을 통해 본 논문은 DeFi에서 지속적인 경제와 적응형 보안 전략의 필요성을 강조한다. 우리는 MEV 공격을 사전에 감지하고 대응하기 위해 더욱 역동적인 보안 프로토콜과 고급 모니터링 시스템의 구축을 지지한다. 또한, 탈중앙화 환경에서 공정한 거래를 위한 거래 기술을 개발을 촉구한다. 이 연구는 이러한 위협의 진화하는 본질과 탈중앙화 공간 내에서 더욱 강건한 금융 구조의 개발에 대한 추가 연구의 길을 열어준다. 결론적으로, DeFi와 DEX는 금융 서비스를 혁신적으로 변화시키고 있지만, 그들의 보안은 여전히 중요한 문제이다. 이 연구는 이러한 플랫폼의 안전성과 신뢰성을 강화하기 위한 연구의 필요성을 강조한다.

참 고 문 헌

[1] Schär, Fabian. “Decentralized finance: On blockchain-and smart contract-based financial markets.” *FRB of St. Louis Review*, 2021.

[2] A. D. Popescu, “Understanding FinTech and Decentralized Finance (DeFi) for Financial Inclusion,” *FinTech Development for Financial Inclusiveness, IGI Global*, pp. 1-13, 2022.

[3] WU, Siwei, et al. “Defiranger: Detecting price manipulation attacks on defi applications.” *arXiv preprint arXiv:2104.15068*, 2021.

[4] HEIMBACH, Lioba; WATTENHOFER, Roger. “Sok: Preventing transaction reordering manipulations in decentralized finance.” *arXiv preprint arXiv:2203.11520*, 2022.

[5] ZHOU, Liyi, et al. “High-frequency trading on decentralized on-chain exchanges.” *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, p. 428-445, 2021.

[6] Krishnamurthi, Rajalakshmi, and Tuhina Shree. “A Brief Analysis of Blockchain Algorithms and Its Challenges.” *Architectures and frameworks for developing and applying blockchain technology*, 69-85, 2019.

[7] “Introducing Uniswap v3.” Accessed: Jan. 31, 2024. [Online]. Available: https://blog.uniswap.org/uniswap-v3

[8] WU, Mike; MCTIGHE, Will. “Constant power root market makers.” *arXiv preprint arXiv:2205.07452*, 2022.

[9] WANG, Ye, et al. “Cyclic arbitrage in decentralized exchanges.” *Companion Proceedings of the Web Conference 2022.* p. 12-19, 2022.

[10] J. Fábregas, “Tracking Ethereum blockchain crypto attackers: Measuring sandwich attacks,”

Tarlogic Security. Accessed: Dec. 01, 2023. [Online]. Available: https://www.tarlogic.com/blog/ethereum-blockchain-sandwich-attacks/

[11] DAIAN, Philip, et al. "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges." *arXiv preprint arXiv:1904.05234*, 2019.

[12] XIONG, Xihan, et al. "Demystifying Just-in-Time (JIT) Liquidity Attacks on Uniswap V3." *Cryptology ePrint Archive*, 2023.

[13] "Flashloans." Accessed: Jan. 31, 2024. [Online]. Available: https://flashloans.com/

〈저자소개〉

최 낙 훈 (Nakhoon Choi)

2020년 : 경기대학교 컴퓨터과학과 (이학사)
2022년 : 경기대학교 컴퓨터과학과 (이학석사)
2022년~현재 : 경기대학교 컴퓨터과학과 박사과정

<관심분야> 블록체인, 인공지능, 정보보호

김 희 열 (Heeyoul Kim)

2000년 : 한국과학기술원 전산학과 (공학사)
2002년 : 한국과학기술원 전산학과 (공학석사)
2007년 : 한국과학기술원 전산학과 (공학박사)
2009년~현재 : 경기대학교 AI컴퓨터공학부 교수

<관심분야> 정보보호, 블록체인