The Journal of the Convergence on Culture Technology (JCCT)
Vol. 8, No. 1, pp.583-590, January 31, 2022. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2022.8.1.583

JCCT 2022-1-66

분산 암호화폐 거래소 모델 및 이슈 분석

Analysis of Distributed Cryptocurrency Exchange Model and Issues

이태규*

Tae-Gyu Lee*

요 약 암호화폐는 2009년 비트코인 소스 공개와 더불어 지속적으로 기술적 발전과 시장확대가 진행되고 있다. 최근에는 NFT 코인을 비롯해 메타버스 결제 서비스를 중심으로 새로운 응용성이 확장되고 있다. 특히, 중앙암호화폐거래소는 암호화폐 간 또는 기존 법정화폐와 암호화폐 간 중계 거래를 활발히 지원하고 있다. 이러한 중앙거래소에 기초한 암호화폐 거래 시장은 암호화폐의 투기 요인을 부추겨서, 암호화폐의 투기성과 무용론을 강하게 불러 일으켰다. 또한, 중앙암호화폐거래소는 사용자 및 가상자산의 집중화를 유도해서, 블록체인의 탈중화 및 보안성 강화 전략을 저해하고 있다. 따라서 본 연구는 현재 서비스 중인 중앙통제 기반의 중앙암호화폐거래소 현황 및 문제점을 기술하고, 거래소의 분산화 모델로서 분산암호화폐거래소 모델링 전략 및 주요 이슈를 제시한다. 본 연구는 블록체인의 기초한 암호화폐의 익명성, 분산화, 자치성 등을 강화할 수 있다.

주요어 : 암호화폐, 블록체인, 암호화폐거래소, 분산암호화폐거래소

Abstract With the release of the Bitcoin source in 2009, cryptocurrencies are continuously developing and expanding the market. Recently, new applicability is expanding centered on NFT coin and metaverse payment service. In particular, the Central Cryptocurrency Exchange actively supports relay transactions between cryptocurrencies or between traditional fiat currencies and cryptocurrencies. The cryptocurrency trading market based on such a central exchange encouraged speculative factors of cryptocurrencies, strongly arousing speculation and futility of cryptocurrencies. In addition, the central cryptocurrency exchange induces the centralization of users and virtual assets, thereby hindering the decentralization and security enhancement strategies of the block chain. Therefore, this study describes the current status and problems of centrally controlled centralized cryptocurrency exchanges in service, and presents a distributed cryptocurrency exchange modeling strategy and major issues as a decentralization model of the exchange. This research can strengthen the anonymity, decentralization, and autonomy of cryptocurrency based on blockchain.

Key words : Cryptocurrency, Block Chain, Virtual Currency Exchange, Distributed Virtual Currency Exchange

Ⅰ. 서 론

지금까지 블록체인 및 분산원장에 기초한 암호화폐는 사토시 나카모토에 의해 2008년 10월 논문이 발표되고, 2009년 1월 비트코인 소스가 공개되면서 지속적으로 기술적 발전과 시장 확대를 거듭하고 있다 [1]. 특히 최근

*정회원, 평택대학교 ICT융합학부 스마트콘텐츠전공 조교수 (제1저자)
접수일: 2021년 12월 31일, 수정완료일: 2022년 1월 5일
게재확정일: 2022년 1월 8일

Received: December 31, 2021 / Revised: January 5, 2022
Accepted: January 8, 2022
*Corresponding Author: tglee@ptu.ac.kr
Division of ICT Convergence (Smart Contents Major), Pyeongtaek Univ., Korea

에는 NFT 코인 및 메타버스 결제 서비스를 중심으로 새로운 변화를 주도하며 암호화폐의 응용성을 확장하고 있다 [2-4]. 블록체인 기술 기반 암호화폐는 은행 등의 금융거래 중앙관리자를 필요로 하지 않는 개인 간 다양한 금융거래 서비스를 지원한 P2P 거래방식을 지원하여, 세계 금융 및 자산 거래 시장에 변화를 일으키고 있다. 특히, 비트코인 및 이더리움을 비롯한 암호화폐거래소에서 암호화폐의 투자가치 급성장은 가격거품 논란 등으로 사회문제를 일으키고 있다 [5]. 최근 비트코인과 이더리움 뿐만 아니라 대체제로서 신규 알트코인 등에 대한 관심으로 확산되고 있는 실정이다 [6]. 블록체인의 암호 안전성 및 분산처리의 강점에 기초한 무한한 개인 간 익명거래 서비스 확장성 등을 가진 중앙통제가 없는 구조적 및 기능적 강점을 활용하고자 하는 암호화폐의 연구개발 활동도 가속화되고 있다 [7].

그리고 비트코인을 비롯한 암호화폐의 시장가치 실현과 디지털 화폐 경제시스템의 현실화를 위해 중앙암호화폐거래소를 통해서 기존 법정화폐와 암호화폐의 거래 또는 다른 암호화폐 간 환전 및 중계 서비스가 제공되었다. 이러한 중앙거래소를 통한 암화화폐 시장 활성화에 대한 시도는 다양한 암호화폐 거래에 대한 커다란 투자 시장을 형성하였다. 현재 중앙암호화폐거래소는 기존 증권거래소 및 중앙은행 시스템과 유사하여 기존 중앙경제시스템에 익숙한 사용자들에게 편리하게 접근할 수 있는 방안이었다 [8]. 그럼에도 불구하고 중앙거래소 모델은 거래소 운영자 및 정부기관의 과도한 통제로 암호화폐 시장 활성화에 제약을 받고 있으며, 또한 몇몇 악의적인 사용자 및 거래소 운영자의 과도한 프리미엄 및 차익실현을 위해 악용되는 사례도 발생하고 있다. 더 나아가 대부분 암호화폐 이용자의 중앙거래소 위탁에 따른 대규모 암호화폐 해킹 사례도 빈번하게 발생하여 고객에게 커다란 피해를 낳고 있다 [9]. 따라서 암호화폐가 전통적인 경제활동의 중앙통제에서 벗어나 개인 간 또는 커뮤니티 간 주도적인 자유로운 경제활동을 극대화시키자는 새로운 경제시스템 확장에 제약 작용되고 있는 실정이다.

그림 1은 암호화폐 거래소의 프로세스 구조를 보여준다. 단계적 구성으로 첫째, 사용자를 위한 강력한 계정 시스템을 구축하여 규모성을 지원하고 해킹에 대응해야 한다. 둘째, 사용자 암호화폐 지갑을 구축하여 높은 트랜잭션 처리와 고객 신원확인 서비스를 제공한다.

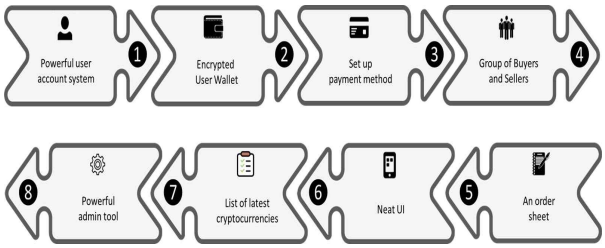

그림 1. 암호화폐 거래 프로세스 구조
Figure 1. Cryptocurrency Exchange Process Architecture

셋째, 지불 처리 서비스를 구축하고, 넷째, 구매자와 판매자를 모집을 활성화 한다. 다섯째, 오더북(암호화폐 거래 주문서) 서비스를 구성하고, 여섯째 직관적인 사용자 인터페이스를 지원한다. 일곱 번째, 최신 암호화폐 리스트를 제공하고, 여덟 번째 강력한 관리자 패널 서비스를 제공하도록 구성한다

중앙암호화폐 거래소의 해킹 위험은 암호화폐 생태계 발전을 막아온 주요 요인 중 하나이다. 2014년 최초의 글로벌 거래소 마운트곡스(Mt.gox)가 해킹을 당해 약 470억엔 가치의 암호화폐를 잃어버린 지 4년이 지났지만 마땅한 대책은 세우지 못한 채 피해 금액만 늘어나고 있다 [10]. 중앙거래소에서 모든 암호화폐 및 가상자산을 저장 및 관리하기 때문에 한 번의 거래소 해킹으로 고객의 막대한 가상자산이 손실을 입게 된다.

본 연구는 현재 서비스 중인 중앙통제 기반의 중앙암호화폐거래소의 분산화(또는 탈중앙화) 모델을 제안하여, 암호화폐의 익명성, 분산화, 자치성을 강화하고자 한다. 제안 모델은 중앙 집중화 거래소의 문제점인 보안 한계성을 극복하는 것 뿐만 아니라 기능 및 성능적으로 개선해야한다.

II. 중앙암호화폐거래소 모델

1. 중앙암호화폐거래소 개요

기존 암호화폐 거래소인 업비트, 빗썸, 바이낸스 등은 중앙 집중화된 거래소(CEX: Centralized Exchange)이다 [11]. 사용자는 거래소를 신뢰하고 자산이나 코인을 맡긴다. 거래소는 모든 거래와 보안 감독 책임을 수행한다. 기존 암호화폐 거래소는 모든 자산을 거래소가 소유한 전자 지갑에 보관한다. 그리고 거래소에서 암호화폐의 거래는 실제 자산이 거래되는 것이 아니라 사용자가 암호화폐를 소유하고 있다는 데이터만 송수신하는 것이다. 이는 마치 동일한 은행에서 실물 화폐가 거래

되는 것이 아니라 서로 다른 고객의 계좌들 사이에 이체 금액 데이터를 교류하는 것과 유사하다. 이 경우 거래소 한 곳에 고객의 많은 가상자산을 보관한다는 점에서 해킹에 위험성이 크고 거래소 내부자가 문제를 일으킬 가능성이 크다는 문제를 안고 있다.

1) 중앙암호화폐거래소의 안전성

대부분의 거래소는 중앙 집중화 거래소에서 거래를 시작하기 전에 고객의 신원을 확인하여 고객 파악(KYC: Know Your Customer)과 자금세탁 방지(AML: Anti Money Laundering) 및 테러 방지 금융(CFT: Counter Terrorism Financing) 검사를 시행한다 [12]. 이러한 중요 절차들은 거래소가 플랫폼 내에서 범죄 활동이 발생하는 것을 예방할 수 있다. 본인 확인이 완료되면, 계좌이체, ACH(Automated Clearing House) 송금, 직불카드 또는 신용카드를 통해 거래소에 원화 및 자금을 입금하거나 비트코인(BTC)나 이더리움(ETH) 등 암호화폐를 예치한다. 구매자는 거래소의 계좌를 통해원화를 입금해서 비트코인을 구매하고, 판매자는 비트코인을 판매해서 원화를 출금할 수 있다.

중앙 집중화 거래소는 거래소 한 곳이 모든 암호화폐를 저장 및 관리하기 때문에 실제 금융 은행과 같다고 볼 수 있다. 이러한 경우 보안에 취약하다는 문제점이 있다. 그러나 현재 중앙 집중화 거래소는 기존 금융 은행보다 규제의 강도가 약하다는 점에서 위험성이 있다. 최근 시행된 특금법에서 실명계좌 확보, 정보보호관리체계(ISMS) 인증 확보, 금융정보분석원(FIU)을 기준으로 신고에 해당하지 않는 국내 암호화폐 거래소들은 운영을 중단하는 규제를 강화하고 있다.

2) 중앙암호화폐거래소의 이슈

중앙거래소의 강점은 기존 증권거래소 및 중앙은행 시스템과 유사성으로 인해 높은 고객 이해도 및 편의성를 제공한다는 것이다. 그리고 전통적인 중앙 시스템 구성과 기술적으로 유사하여 서비스 구현이 용이하다는 것이다.

중앙거래소의 단점들은 다음과 같다. 먼저 중계 트랜잭션 중앙화에 따른 지속적인 시스템 대규모 투자 및 높은 수수료율의 경향을 보인다. 그리고 고객 암호화폐 분실에 따른 위험성이 지속적으로 내재되어 있다. 그리고 중앙 시스템 의존화에 따른 중계거래 독과점 발생이 우려된다. 마지막으로 블록체인 기반 암호화폐의 분산성, 익명성, 독립성 강화와 상반되는 과도한 중앙 집중화 및 고객 의존성이 존재한다.

2. 중앙암호화폐거래소 모델

일반적인 중앙 거래소에서는 고객이 명목화폐(은행 이체 또는 직불/신용 카드) 또는 암호화폐를 입금해야 한다. 암호화폐를 입금할 때는, 고객의 통제권을 포기하고, 해당 암호화폐를 계속해서 거래 또는 출금할 수 있기 때문에 사용성 측면뿐만 아니라, 이를 블록체인에서 사용할 수 없는 기술적 이슈도 가지고 있다.

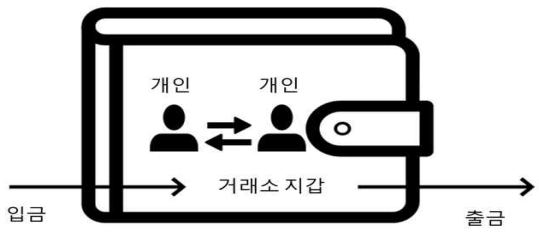

그림 2. 중앙 암호화폐 거래 모델
Figure 2. Centralized Cryptocurrency Transaction Model

그림2와 같이 중앙 암호화폐 거래소는 고객의 계정을 통해서 현금을 입금하고, 자동으로 지갑이 형성되며, 거래소의 위탁거래를 통해 자유롭게 암호화폐를 거래할 수 있다 [11-13]. 이러한 거래소의 사용자는 지갑의 개인 키를 보유하지 않으며, 출금을 진행 시, 거래소에게 고객을 대신하여 트랜잭션에 서명해 줄 것을 위임한다. 트레이딩 시, 트랜잭션은 온체인 상에서 발생하지 않으며, 거래소는 자체 데이터베이스 내에서 자금을 사용자에게 할당한다. 일반적인 트랜잭션 작업 흐름은 매우 효율적인데, 이는 블록체인의 느린 속도로 인한 트레이딩 지연이 발생하지 않기 때문이다.

이러한 거래소 위탁 모델은 고객이 자금을 보관하는 거래소를 신뢰해야하고, 데이터 유출 피해를 최소화할 수 있는 좋은 실적과 예방책을 보유하고 있는 검증된 거래소를 선택하는 것이 최선이다.

3. 중앙암호화폐거래소 현황

1) 해외 현황

표 1은 해외 대표 암호화폐 거래소 8곳의 현황을 보여준다 [13-16]

표 1. 해외 암호화폐 거래소 현황
Table 1. Current status of overseas cryptocurrency exchanges

Exchange	Coins	Fee	Release date	Remark
Binance	419	0.1%	Jul 2017	CHINA
Huobi	193	0.2%	Sep 2013	
FTX	304	0.45%	Feb 2019	
Kucoin	580	0.1%	Aug 2017	
Coinbase	141	2%	Feb 2019	USA
Kraken	102	0.21%	Jul 2011	
Bitstamp	51	0.5%	Aug 2011	EUROPE
BitFlyer	8	0.2%	Jan 2014	JAPAN

Dec 30, 2021 source : Coinmarketcap, CryptoWisser

중국의 거래소는 Binance(바이낸스), Huobi(후오비) 등이 있고 각각 419개, 193개의 코인이 상장되어 있으며 거래 수수료는 0.1%, 0.2%이다.

미국의 거래소는 Coinbase(코인베이스), Kraken(크라켄) 등이 있다. Coinbase는 GDAX를 이용할 수 있고 GDAX간에 발생하는 수수료는 무료로 송금에 용이하다. Kraken은 미국에서 금융 범죄 단속 네트워크(FinCEN)의 규제를 받아 높은 보안성으로 신뢰도가 높은 암호화폐거래소로 불린다.

그리고 유럽 거래소인 Bitstamp(비트스탬프), 일본 거래소인 BitFlyer(비트플라이어)등 이 있다. Bitstamp는 사용자가 계정을 제어할 수 있도록 고객 맞춤 소프트웨어 API를 제공하는 특징을 가지고 있다.

2) 국내 현황

다음 표 2는 국내 대표 암호화폐 거래소 5곳의 현황을 보여준다 [13-16]. 현재 국내 암호화폐거래소는 금융 제도화 및 규제 방안을 통해서 공인 암호화폐거래소를 단계적으로 구축하는 과정이다. 대표 거래소는 2021년 12월 기준, 일 거래액 1억달러 이상을 기록 중인 UPbit, bithumb, coinone, KORBIT, GOPAX 등 이다.

표 2의 UPbit(업비트)는 모바일에 최적화된 다양한 UI를 제공하고 코인 시장 전반에 대한 뉴스, 정보 등을 거래소 안에서 제공한다. 처음 코인거래를 시작하는 입문자들이 가장 많이 사용하고, 거래량이 풍부하고 코인의 종류가 많고 빠르고 안정적인 거래를 하는 것이 장점이다.

Bithumb(빗썸)은 국내 1세대 암호화폐거래소로서 2014년 엑스코인이라는 이름으로 거래 서비스를 시작하여 2015년 빗썸으로 변경됐다. 최근에는 거래 기준 화폐로서 원화가 아닌 비트코인을 사용하여 다른 암호화폐인 이더리움, 리플, 라이트코인, 비트코인 캐시, 이오스 등을 거래할 수 있는 BTC마켓을 개시했다.

표 2. 국내 암호화폐 거래소 현황
Table 2. Current status of domestic cryptocurrency exchanges

Exchange	Coins	Fee	DailyTransaction
Bithumb	188	0.25%	$1.06 billion
UPbit	155	0.25%	$3.37 billion
Coinone	188	0.20%	$0.21 billion
Korbit	77	0.14%	$17.55million
Probit	71	0.09%	$5.27 million

Dec 30, 2021 source : Coinmarketcap, CryptoWisser

III. 분산 암호화폐거래소 모델

본 절은 분산 암호화폐 거래를 지원하는 분산 암호화폐 중계거래소 모델을 제안한다. 먼저 분산 암호화폐 중계거래소의 구조를 기술하고, 다음으로 분산 암호화폐 거래소 프로토타입 설계를 기술한다.

1. 분산 암호화폐거래소 개요

분산 암호화폐거래소는 탈중앙화거래소 (DEX: Decentralized Exchange)로 불리며, 거래 사용자의 자금이나 자산을 거래소가 직접 통제하지 않고 사용자가 직접 자신의 지갑에 암호화폐를 보관하여 관리한다. 이러한 분산 거래소는 실질적으로 스마트계약(smart contract)을 실행하는 시스템이지만 모든 거래를 개시하고 거래의 세부사항을 규정하는 것은 사용자이다. 일반적으로 분산거래소는 소유주가 익명이기 때문에 트랜잭션을 운영하는 사용자가 누구이고 그 목적이 무엇인지 파악할 수 없다. 그러므로 이러한 분산 거래소 방식은 초보자들이 접근하기는 어렵고 사용자의 이해와 자금 및 자산 유동성의 부족으로 거래 속도가 느리다는 문제점을 안고 있다 [16].

분산 암호화폐 거래 시스템의 구성은 지갑주소 및 거래 스크립트 만 공유 하는 방법이 있다. 이 구성은 중소 및 개인 간 암호화폐 거래에 절절한 방법이 될 수 있다.그리고, 분산 하이브리드 암호화폐 거래 시스템은 단말 및 거래소 클라이언트 (앱, 웹 등), 클라우드 거래소 및 분산 거래소, 인터넷 및 거래 중개 미들웨어 등으로 구성할 수 있다.

2. 분산 암호화폐거래소 모델

본 절은 분산 암호화폐 거래 주요 모델을 기술한다.

특히, 세계적인 거래소 트랜잭션의 변화흐름을 이해하고, 분산 암호화폐 거래 모델의 분류을 제시하고자 한다.

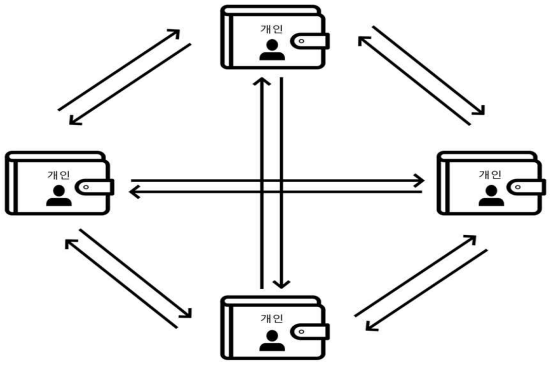

그림 3. 분산 암호화폐 거래 모델
Figure 3. Decentralized Cryptocurrency Transaction Model

그림 3은 분산 암호화폐 거래 모델을 보여준다. 완전 P2P 분산 모델은 중앙서버 제어기 없이 개인 참여노드 간 P2P 암호화폐 송수신 거래를 지원한다. 이러한 모형은 전통적으로 동종의 암호화폐 트랜잭션에서 거래가 용이하다. 그리고 거래소 및 중앙서버에 대한 대규모 컴퓨팅 서비스와 전체 거래 사용자에 대한 그러나 이종 암호화폐 간 다양한 환전 및 거래를 지원하기 위해서는 지갑 소프트웨어의 복잡도 및 크기가 커지기 때문에 거래 사용자에게 관리에 대한 부담감을 가중시킨다. 부분 P2P 분산 모형은 중앙서버 제어기에 일부 또는 일정기간 지갑 위탁하여 중개 또는 환전하는 거래방식을 지원한다.

분산암호화폐거래소는 중앙화된 거래소와 유사한 부분도 있지만, 상당히 다른 부분도 존재한다. 분산 암호화폐 거래소의 일반적인 유형은 온체인(스마트 콘트랙트를 사용)에서 주문이 체결되는 곳이며, 따라서 사용자는 자신의 자금에 대한 통제권을 넘겨주지 않아도 된다. 일부 작업은 크로스체인 분산 거래소에서 진행되었지만, 단일 블록체인(이더리움 또는 바이낸스 체인)상의 자산 거래가 가장 많이 사용되고 있다.

1) 온체인 거래 모델

일부 분산 거래소에서는 모든 것이 온체인(On-chain)에서 진행되므로, 모든 주문(주문 변경 및 취소)이 블록체인에 기록되고, 투명한 접근 모델이 될 수 있다. 주문을 중계하는 제3자를 신뢰하지 않아도 되며, 해당 트랜잭션을 모호하게 만들 수도 없기 때문이다. 이와 동시에 이 모델은 해당 주문 트랜잭션을 블록체인 네트워크상의 기록하기 위해 모든 노드를 호출하며, 최종적으로 수수료(또는 가스비)를 지불하기 때문에 블록체인에 사용자 거래 기록 블록이 추가될 때까지 복잡하고 대기가 발생할 수 있다는 의미이다.

그리고, 프런트 러닝(front running)을 이 모델의 결점이라 할 수 있다. 프런트 러닝은 시장의 내부자가 지연되는 트랜잭션을 인식하고, 트랜잭션이 처리되기 전에 해당 정보를 사용해 거래를 진행할 때 발생한다. 따라서 프런트 러너는 일반 사용자에게 공개되지 않은 정보로부터 이득을 취한다. 물론, 모든 것이 세계적인 장부상에 공개된다면, 보통 말하는 프런트 런의 기회가 없을 것이다. 그럼에도 불구하고, 다른 유형의 공격이 발생할 수 있다. 승인되기 전의 주문을 확인한 특정 마이너가 자신의 주문이 블록체인에 먼저 추가되도록 할 수 있다. 온체인 오더북 모델의 예시로는 스텔라와 비트셰어 DEX가 있다.

2) 오프체인 거래 모델

오프체인(Off-chain) 거래 모델에 기초한 분산 암호화폐거래소는 직거래 측면에서 탈중앙화되어 있지만, 여전히 이전 모델보다 더욱 중앙화 되어 있다. 모든 주문이 실시간으로 블록체인에 기록되지 않으며, 어디선가에서 호스팅을 제공받고 있다. 고객의 선택에 따라, 중앙화된 거래소 주체에게 전적으로 오더북(order book)을 위임할 수 있다. 만약 위탁 거래소가 악의적이라면, 프런트 러닝 또는 주문을 잘못 표시 등과 같이 시장을 조작할 수도 있다.

오프체인 거래 모델은 ERC-20을 위한 이더리움 블록체인상에서 구현된 다른 토큰이 좋은 예시이다. 스마트 계약 및 다른 도구를 사용하여, 거래소 호스트는 복합적인 유동성 풀을 활용할 수 있으며, 사용자 간의 주문을 중계할 수 있다. 해당 주체들이 연결될 경우에만, 온체인 주문이 실행된다.

이러한 접근 방식은 온체인 오더북에 의존하는 것보다 사용성 측면에서 우수하다. 그리고 블록체인을 그리 많이 사용하지 않기 때문에 거래 속도 면에서 동일한 제약이 발생하지 않는다. 그럼에도 블록체인 상에서 거래가 체결되어야 하기 때문에, 오프체인 오더북 모델의 속도는 여전히 중앙 거래소보다 느리다. 오프체인 거래

모델 예시는 바이낸스 DEX, IDEX, 이더델타(EtherDelta) 등이다.

3) 크로스체인 거래 모델

크로스체인(Cross chain)은 서로 다른 블록체인을 연결시켜주는 역할을 수행한다. 예를 들어, 비트코인이나 이더리움 등의 암호화폐는 서로 간의 직접적인 상호 운용이 불가능하다. 따라서, 비트코인을 법정화폐로 교환한 뒤 다시 이더리움을 구매하는 방법이 일반적이다. 그러나, 이러한 거래 과정은 많은 시간과 비용이 소요된다.

이때 암호화폐 교환을 직접 할 수 있도록 지원해 주는 크로스 체인이 활용되면 보다 편리하고 효율적으로 거래가 가능하다. 크로스 체인은 중간자 역할을 하여 두 암호화폐 간의 거래, 교환 등을 원활하게 상호 운용될 수 있도록 지원 역할을 수행한다. 따라서, 서로 다른 암호화폐 간의 교환이 바로 가능해지고 다양한 블록체인 플랫폼 간의 연결이 용이하다.

크로스 체인의 주요 특징은 서로 다른 암호화폐의 교환이 이뤄질 경우 복잡한 단계나 절차 없이 연결이 가능하다. 또한 암호화폐 간의 트랜잭션이 발생할 시, 토큰 간의 교환은 없고 데이터만 전송한다. 마지막으로, 블록체인의 확장성을 높여 다른 블록체인을 연결해 줄 수 있다.

4) 자동화 거래 모델

자동화된 시장메이커모델은 구현 방식에 따라 다르지만, 보통 일련의 스마트 콘트랙트를 연결하고, 사용자의 참여를 위한 보상을 제공한다.

자동화된 시장 메이커 기반 분산 거래소는 사용자 용이성을 극대화하였고, 메타마스크 또는 트러스트 월렛과 같은 지갑을 통합하고 있다. 그러나 다른 유형의 분산 거래소와 마찬가지로, 거래 체결을 위해서는 온체인 트랜잭션이 생성되어야 한다. 응용 예시로, 유니스왑, 카이버 네트워크 등이 있으며, 모두 ERC-20 토큰 거래를 제공한다.

3. 분산암호화폐거래소 설계 방안

본 절은 개인 간 분산 암호화폐 거래를 지원하는 분산 암호화폐 중계거래소 프로토타입을 개발하기 위한 설계 방안을 기술한다. 특히, 주요 시스템 구성요소 및 거래 프로세스를 구현 방안을 제안한다.

본 연구는 분산 암호화폐거래소 모델은 중앙 거래소의 고속성, 확장성, 유연성, 편의성 등을 지원하는 동시에, 참여노드가 주도하는 P2P 거래소의 보안성, 분산화, 스마트계약 및 블록체인화 등을 함께 달성하고자 하이브리드 모델을 제안한다. 이 모델에 관한 기술은 분산 암호화폐 거래 서비스에 관한 전반적인 프로세스의 이해를 제공한다. 암호화폐 거래 사용자의 직접거래 또는 위탁거래를 지원하는 분산 거래소 네트워크를 구성한다. 이는 기존 중앙거래소의 위상 및 역할을 수행할 수 있다. 그리고, P2P 암호화폐 거래 노드로서 다양한 암호화폐 지갑을 보유한 참여노드가 위치한다. 이는 동종 블록체인 기반의 온체인 직거래 서비스를 지원하거나, 이종 블록체인 기반의 오프체인 직거래 서비스를 지원할 수 있다. 그리고 암호화폐 거래의 실시간성을 높이거나 거래상대를 신속히 찾고자 유연성을 강화하는 경우는 분산 거래소 네트워크에 스마트 계약 및 자동화 거래를 통해서 위탁할 수 있다. 분산 거래소 네트워크와 P2P 참여노드는 실시간 암호화폐 매매 리스트를 공유한다.

분산 암호화폐 거래소의 강점은 거래 구조 분산에 따른 거래 수수료를 최소화하고, 디지털 화폐 시스템의 분산화 및 개별화 강화하고, 거래소 중앙화에 따른 단일실패 위험 최소화 및 가상자산 안정화를 강화하는 장점을 가진다. 또한, 거래 고객의 지갑주소 및 개인 정보 등 거래정보 공개 및 노출 최소화에 따른 보안성을 강화한다.

분산 암호화폐 거래소의 약점은 거래구조 복잡도 증가에 따른 구현 난이도 증가하고, 새로운 분산 구조 제안에 따른 시스템 안정화 및 검증 시간이 소요된다. 또한, 기존 타 중앙 암호화폐 중계 거래소와 다른 종류의 중계 연동 인터페이스 지원 문제가 대두되고, 분산 거래정보의 실시간 공유를 위한 시간 지연 및 동기화 이슈에 대한 대안이 요구된다.

Ⅳ. 분산 암호화폐거래소 이슈 분석

본 장은 분산 암호화폐거래소의 다양한 특징 및 이슈들을 기술한다. 몇몇 주요 암호화폐 거래소도 분산화된 시스템을 구축 중인데, 분산 거래소의 이익 창출이 이용자 수수료에 의존하지 않는다면 이용자 입장에서는 더 많은 이점과 혜택을 누릴 수 있다. 이는 거래소

입장에서 이러한 이점을 무기로 더 많은 이용자를 유지할 수 있을 것이다.

1. 암호화폐거래소의 분산화 방안

암호화폐거래소의 분산화 방법은 분산 거래 네트워크의 구성요소로서 서버 유무에 따라 서버 기반과 서버리스로 구분할 수 있다. 그리고 분산화 정도에 따라 암호화폐 거래소의 분산화 전략을 실행할 수 있다. 분산도가 1인 경우는 전체 참여노드가 P2P 네트워크로 구성되고, 완전 분산화 모형으로, 중앙 중개 없이 개인 참여노드 간 직거래 모델이다. 이러한 방법은 중계 서비스 자체를 블록체인 네트워크로 구축하고, 중계 트랜잭션 정보에 대한 모든 정보를 개인 컴퓨터에 저장해야 한다.

완전히 분산된 방식으로 운영되는 거래소가 가장 이상적이다. 하지만 그렇게 되면 거래 속도가 너무 느리다. 보안뿐 아니라 성능도 뛰어나야 한다. 일부 분산 방식으로 운영되는(하이브리드 분산) 거래소는 이용자가 암호화폐를 스스로 보관하다가 거래하고 싶은 양만 중앙거래소에 맡겨 처리하는 방식을 제공할 수 있다.

2. 분산 암호화폐거래소의 장점

분산 암호화폐거래소는 다음과 같은 다양한 장점들을 가질 수 있다.

첫째, 대부분의 기존 거래소는 KYC/AML(고객 알기 제도와 자금 세탁 방지)을 준수한다. 사용자들은 프라이버시를 걱정하거나 접근성을 우려할 수 있다. 그러나, 분산 암호화폐거래소는 허가가 필요없기 때문에, 사용자의 신원을 확인하지 않고, 암호화폐 지갑만 보유하고 있으면 된다는 것이다. 그럼에도 불구하고, 몇몇 중앙 주체가 운영하는 분산 암호화폐 거래소의 경우에 몇 가지 법적 규제 요구 사항이 존재한다. 예를 들어 오더북이 중앙화되어 있는 경우에, 호스트가 관련 규정을 준수해야 한다.

둘째, 분산 암호화폐 거래소의 주된 장점은 사용자의 자금을 보유하지 않는다는 것이다. 따라서 2014 마운트곡스 해킹 사건과 같은 심각한 유출 사태로 인해 사용자의 자금이 위험에 처하거나, 민감한 개인 정보가 유출되지 않을 것이다.

셋째, 중앙 거래소에 상장되지 않은 비상장 토큰들은 수요와 공급이 존재한다면, 분산 암호화폐거래소에서 자유롭게 거래될 수 있다는 것이다.

3. 분산 암호화폐거래소의 이슈

분산 암호화폐거래소는 다음과 같은 몇몇 주요 한계와 이슈들을 기술한다.

첫째, 현실적으로 분산 암호화폐거래소는 아직까지 기존 거래소만큼 사용자 편의성을 보장하지 못한다는 것이다. 중앙화된 플랫폼은 실시간 거래를 제공하며, 이는 블록 시간에 영향을 받지 않는다. 비위탁 암호화폐 지갑에 익숙하지 않은 초보자들에게 중앙 거래소는 훨씬 편리한 인터페이스 경험을 제공할 수 있다. 계정 비밀번호를 잃어버린 경우에도 초기화를 통해서 복구할 수 있다. 그러나 분산 참여노드의 사용자가 시드 문구를 잃어버린 경우에는, 모든 암호화폐 및 가상자산이 사이버 공간에 유실되어 회복할 수 없다는 문제를 안고 있다.

둘째, 분산 암호화폐거래소는 상대적으로 적은 거래량과 낮은 유동성 한계를 지닌다. 현재 중앙거래소의 거래량은 분산거래소의 거래량보다 압도적으로 많다. 더 중요한 것은 중앙거래소는 더 많은 가상자산 유동성을 보유하고 있다는 것이다. 유동성은 적절한 가격에 얼마나 쉽게 자산을 구매 또는 판매할 수 있는가 하는 거래소 지표이다. 유동성이 높은 시장에서는 매수 및 매도의 가격 차이가 거의 없으며, 이는 구매자와 판매자 간에 치열한 경쟁을 통해 적정한 시장이 형성되어 있다는 것을 의미한다. 비유동적인 시장에서는 적정 가격에 자산을 거래하고자 하는 고객들 찾기가 더 어렵다는 것을 의미한다.

셋째, 분산 암호화폐 거래소는 상대적으로 높은 수수료율을 지출한다는 것이다. 분산 거래소에서 언제나 수수료가 비싼 것은 아니지만, 네트워크가 혼잡하거나 온체인 오더북을 사용하는 경우에는 높은 수수료를 지불할 수 있다. 그리고 서버 컴퓨팅 네트워크와 같은 고정 인프라 연동 유무에 따른 투자 비용 정도에 따라 수수료 차이가 발생하고, 수수료율이 달라질 수 있다.

Ⅴ. 결 론

본 연구는 암호화폐거래소의 거래 프로세스인 중앙화, 탈중앙화 가운데 암호화폐거래소의 중앙 집중화 거래 과정을 중점적으로 분석한 후 중앙암호화폐거래소의 높은 거래 수수료 및 취약한 보안성의 문제를 기술했다. 또한 이러한 중앙집중화 암호화폐거래소의 수수료,

보안성, 성능 등의 문제들을 개선하기 위해서 암호화폐 분산 거래소 모델을 제안했다. 이러한 모델은 암호화폐 거래소 사용자들의 과도한 독과점화에 따른 수수료 상승, 보안 취약성, 중앙 집중화에 따른 거래서비스 성능 한계 등을 개선시키는 블록체인의 본질적 분산화 전략 향상을 유도할 것이다.

본 연구의 분산화 모델 분석 및 이슈 대응 방안은 P2P 블록체인 네트워크의 자산 거래 트랜잭션과 조화를 이루고, 사용자 보유 자산의 안전성 및 보안성을 극대화시키는 데 기여할 수 있다.

향후 본 연구에서 제시한 암호화폐 및 암호화폐거래소 이슈들을 개선하기 위한 시스템적 대응방안 및 심층 연구를 수행할 것이다.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” www.bitcoin.org, pp.1-9. 2008

[2] S.Y. Sin, “The core of the metaverse, NFT and virtual economy,” *Emerging Tech & Biz Hana Industry Info*, Vol. 3, Aug. 2021.

[3] G.J. Kim, “Evolution of the real and virtual worlds through metaverse examples,” *Broadcasting and Media* Vol. 26, No. 3 pp. 206-215.

[4] S.W. Song, and D.H. Chung, “Explication and Rational Conceptualization of Metaverse,” *Informatization Policy* Vol. 28, No. 3, pp. 003-022 Sep 2021. DOI: https://doi.org/10.22693/NIAIP.2021.28.3.003

[5] C.Young Song, and Sunghyuck Hong, "One way to solve the problem of presales of Ethereum : how to use public key cryptography," *IJASC*, vol.1, no.2, pp.27-31, 2019. DOI: https://doi.org/10.22662/IJASC.2019.1.2.027

[6] K. C. H. Kim, “The Impact of Blockchain Technology on the Music Industry,” *International journal of advanced smart convergence*, vol. 8, no. 1, pp. 196 - 203, Mar. 2019. DOI: https://doi.org/10.7236/IJASC.2019.8.1.196

[7] J.K. Hong, S.T. Kim, and D.S. Ryu, “Blockchain Watchdog: Real-time Blockchain Surveillance System Connecting Smart Contract Code and Distributed Storage,” *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 20, no. 4, pp. 115 - 121, Aug. 2020. DOI: https://doi.org/10.7236/JIIBC.2020.20.4.115

[8] H.C Kim, “The Effects of e-Service Quality on Satisfaction and Continuance Intention in Cryptocurrency Exchange,” *Journal of the Korea Industrial Information Systems Research*, Vol. 23, No. 6, Dec. 2018. DOI: https://doi.org/10.9723/jksiis.2018.23.6.113

[9] M.I.Lim and H.B.Jang, “A Study on the Risk Reduction Plan of Cryptocurrency Exchange,” *Journal of Platform Technology*, Vol. 8, No,. 4, pp. 29-37, Dec. 2020.

[10]Miko Matsumura, “Evercoin,” http://wiki.hash.kr/index.php/, https://evercoin.com/home

[11]Cryptopedia, “The State of Centralized Exchanges,” 2021. https://www.gemini.com/cryptopedia/centralized-exchanges-crypto

[12]Coinone, “Understanding the cryptocurrency exchange structure and risk management,” 1st *Electronic Finance Forum Regular Meeting*, Bank of Korea, Aug. 30, 2017. http://www.bok.or.kr/portal/bbs/P0002700/view.do?nttId=231522&menuNo=200737&pageIndex=1

[13]Hashnet, “cryptocurrency exchange,” http://wiki.hash.kr/index.php/

[14]“Ranking of domestic cryptocurrency exchanges,” Feb. 2021, https://xfile.tistory.com/81

[15]CoinMarketcap, “Top Cryptocurrency Spot Exchanges,” https://coinmarketcap.com/rankings/exchanges/

[16]CryptoWisser, “Cryptocurrency Exchange List,” https://www.cryptowisser.com/exchanges/?lang=ko

※ 본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 사회맞춤형 산학협력 선도대학(LINC+) 육성사업의 연구결과임.