Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.641

블록체인 거래소 플랫폼을 활용한 RWA 토큰 거래에서의 개인정보보호 개선 방안

이 재 성,[1†] 이 중 희[2‡]
[1,2]고려대학교 (대학원생, 교수)

Enhancing Anonymity Protection in RWA Token Trading Using Blockchain Exchange Platforms

Jaeseong Lee,[1†] Junghee Lee[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

본 논문은 최근 몇 년간 암호화폐 시장에서 가장 두드러진 이슈 중 하나인 실제 자산 토큰, 즉 RWA(Real-World Assets) 토큰의 토큰 거래와 관련된 익명성 보호 문제를 다룬다. 블록체인 기술의 투명성 원칙상 거래자의 익명성을 보장하기 어렵지만, 기존 블록체인 연구에서 대체 가능 토큰(FT)의 프라이버시 보호를 위해 믹서 서비스를 이용하는 경우가 있었으며 대체 불가능 토큰(NFT)의 프라이버시 보호를 위한 선행 연구가 있었다. 그러나 FT와 NFT의 특성을 모두 지닐 수 있으며 실물 자산과 연계된 RWA 토큰은 그 구조상 어느 한 방법만을 사용해서는 익명성 보호라는 목표를 효과적으로 달성하기 어렵다. 본 논문에서는 가상의 토큰 거래 플랫폼인 ARTeX를 제안하고 거래 프로세스를 설명함으로써 RWA 토큰의 익명성 보호를 위한 방안을 분석한다.

ABSTRACT

This paper addresses the issue of anonymity protection in the trading of Real-World Asset (RWA) tokens, a prominent topic in the cryptocurrency market in recent years. The principle of transparency inherent in blockchain technology makes it challenging to ensure the anonymity of traders. Although there have been instances in existing blockchain research where mixer services have been utilized to protect the privacy of Fungible Tokens (FTs), and prior studies have explored the privacy protection for Non-Fungible Tokens (NFTs), RWA tokens, which can embody characteristics of both FTs and NFTs and are tied to physical assets, present a complex challenge in achieving the goal of anonymity protection through any single method. This paper proposes a hypothetical token trading platform, ARTeX, and describes the trading process to analyze measures for protecting the anonymity of RWA token transactions.

Keywords: Anonymity, Blockchain, Real-world-assets token, Privacy Protection

I. 서 론

2008년 신원미상의 인물인 나카모토 사토시(Nakamoto satoshi)가 비트코인을 제안[1]한 이후 수많은 대체 코인이 생성되어 새로운 산업의 성장을 촉진하고 있다. 디지털 자산 시장이 번창함에 따라 이러한 기술의 발전으로 인해 전통적인 물리적 자산과 디지털 자산을 연결하려는 움직임이 나타나고 있다. RWA 토큰은 실물 자산과의 연결을 의미하는 Real-World Assets Token의 약어로 STO

Received(05. 08. 2024), Modified(05. 24. 2024), Accepted(06. 13. 2024)
† 주저자, mandoopapa@korea.ac.kr
‡ 교신저자, j_lee@korea.ac.kr(Corresponding author)

(Security Token Offering)뿐만 아니라 대체 불가능한 토큰(Non-Fungible Token, NFT), SBT(Soul-bound Token)를 포괄하는 개념으로 간주한다[2][3]. 블록체인의 기술적 특성상 거래 이력과 정보가 모든 노드에 투명하게 공개되는데, 이는 RWA 토큰도 마찬가지다. 대표적인 퍼블릭 블록체인인 이더리움의 경우, 이더스캔(Etherscan)과 같은 서드파티 애플리케이션을 통해 특정 토큰 거래 이력과 세부 정보를 쉽게 확인할 수 있다[4]. 이때 토큰의 거래 시 유출될 수 있는 프라이버시에 대한 문제가 제기될 수 있다. 누가 언제, 어떻게, 어떤 가격에 거래했는지 등 토큰과 관련된 많은 세부 정보가 투명하게 공개되어 쉽게 확인할 수 있습니다. 이더스캔을 통해 누구나 평문으로 제시된 거래 당사자들의 지갑 주소를 확인할 수 있으며, 해당 지갑 주소가 보유한 토큰의 상태뿐만 아니라, 거래 이력도 확인할 수 있다. 누가 누구에게 어떤 토큰을 얼마에 양도했는지 쉽게 확인할 수 있다. 자신의 토큰과 관련된 거래 이력을 숨기고 거래자의 익명성을 보호할 수 있는 적절한 장치가 없어 이를 다양한 방식으로 해결하기 위한 노력이 지속되어 왔다. 하지만 현재까지 사용되고 있는 방법인 단순 화면상에 토큰을 노출하지 않는 방법이나 토큰의 상세정보 숨기기, 미끼 계정 활용 기술 등이[5][6]이 익명성 보호에만 초점이 맞춰지고 거래의 안정성을 보장하는데 소홀했다는 점을 고려할 때 실제 서비스 과정을 포함하여 익명성 보호를 포괄하는 방안에 관한 연구가 필요하다. 이에 본 논문에서는 이러한 문제점을 극복하기 위해 기존에 제안된 익명성 보호 방법들을 살펴보고, 각 방법에서 발생하는 문제점을 분석한 후 익명성 보호를 위해 가상의 토큰 거래 플랫폼인 ARTeX(Anonymity Real-world assets Token exchange)를 제안함으로써 목적에 다가가는 연구를 시도한다.

II. RWA 토큰의 정의

RWA 토큰은 2023년 무렵부터 대중에 널리 알려지게 되었지만, RWA 토큰에 관한 연구는 2017년부터 진행된 바 있다[7]. 현실 세계의 자산을 거래한다는 의미의 Real-World Assets 토큰은 현실에 존재하는 모든 유형 및 무형 자산의 토큰화를 의미[7]하며, 본 논문에서 정의한 RWA 토큰은 이 정의를 차용한다. NFT가 단순히 교환 불가능한 토큰을 포괄하는 개념이라면, RWA는 현실 세계와 연결된 자산을 포함하여 토큰화할 수 있는 모든 것을 포괄하는 한 단계 넓은 개념으로 볼 수 있다. 한편, RWA 토큰 표준화를 위해 제안된 이더리움의 ERC3643 프로토콜은 RWA 토큰의 개념을 실물 자산, 증권, 암호화폐, 로열티 프로그램 [8]의 네 가지로 정의하기도 했는데, 이 역시 NFT보다 더 포괄적인 개념으로 RWA 토큰을 정의한 것이다. 종합하면 RWA 토큰은 현실 세계의 자산과 연계되어 발행할 수 있고, 이 과정에서 FT와 NFT 등의 형태에 제한 없이 자유롭게 발행할 수 있는 포괄적 개념의 토큰이다.

III. 익명성 보호(Anonymity Protection)

3.1 익명성과 프라이버시 보호

가상의 플랫폼인 ARTeX를 통해 거래 당사자의 개인정보를 보호하는 프로세스를 소개하기에 앞서, 익명성과 프라이버시 보호라는 용어를 정의한다. 두 용어가 혼용되기도 하는데, Bradbury의 구분[9]에 따르면, 프라이버시 보호는 정보 자체를 숨기는 것이고, 익명성 보호는 정보의 소유자를 숨기는 것에 더 가깝다. 본 고에서 제안하는 ARTeX는 토큰 정보 자체가 아닌 거래에 관련된 개인정보의 익명성을 보장하는 것을 목표로 참여자의 프라이버시를 강화하고 개인정보 보호를 달성하고자 한다. 이는 실제 자산의 판매자와 구매자를 분리하고, 블록체인과 분리된 별도의 보안 채널을 통해 토큰을 안전하게 전달하는 방법으로 이루어진다.

3.2 RWA 토큰 거래에 익명성 보호가 필요한 이유

일반 토큰과 RWA 토큰의 가장 큰 차이점은 RWA 토큰의 기반이 실제 세계의 자산이라는 점에 있다. 따라서, RWA 토큰 거래 시 익명성 보호의 필요성은 개인 정보 보호와 더불어 실물 자산의 안정성을 유지하고 의도적인 시장 조작을 방지하는 데에도 목적이 있다. 즉, 토큰 거래 시 구매자와 판매자의 정보, 거래 금액 등을 블록체인에 기록하지 않음으로써 익명성을 보호해야할 필요성이 있다. 다만, 거래 대상이 되는 토큰 자체를 익명화하게 되면 거래가 올바르게 이루어지기 어렵기 때문에 구매자가 구매하는 토큰에 대한 정확한 정보를 가질 수 있도록 해야 한다[10].

IV. 관련 연구

4.1 단순히 화면상에 노출하지 않는 방법

중앙집중형 거래소에서는 RWA 토큰에 대한 모든 정보가 공개되지만 거래소의 웹페이지에는 판매자와 구매자의 신원이 표면상 드러나지 않도록 감추는 웹 환경에서 익명성을 보장하기 위한 가장 일반적인 방법이다. 그러나 앞서 언급한 바와 같이 블록체인상의 토큰은 거래된 토큰의 거래 정보를 쉽게 볼 수 있는 서비스가 있으며, 거래된 토큰의 정보를 확인하는 것만으로도 판매자와 구매자의 정보를 확인할 수 있다.

4.2 토큰 상세정보 숨기기

일반적인 방법의 단점을 극복하기 위해 중앙집중화된 거래소에서 판매자와 구매자의 거래 계좌를 숨기는 방법도 제안되었다. 이지스에서는 거래 금액 및 대상 토큰에 대한 정보를 암호화하는 방법(이 경우 NFT에 한함)을 제안했다[5]. 다만, RWA 토큰 거래에 있어서 이러한 방식을 사용하는 것은 위험하다. RWA 토큰은 실물 자산을 기반으로 하므로, RWA 토큰 거래를 위해서는 적어도 토큰에 대한 상세한 정보를 공개할 필요가 있으며, 이를 기반으로 어떤 자산을 기반으로 하는지 명확하게 정의할 필요가 있다. 이는 구매자에게 필요한 정보를 제공해야 한다는 점에 해당한다.

4.3 미끼 계정(Decoy accounts) 활용

미끼 계정은 중앙집중화된 거래소가 관리하는 계정으로 일반적인 사용자 계정과 같이 보이나 해당 미끼 계정의 개인키는 거래소가 관리하며 NFT 등의 거래에서 암호화폐 결제를 분리하여 NFT 거래 과정에서 구매자와 판매자를 연결하기 어렵게 할 목적으로 사용된다[10]. NFT를 거래할 때 구매자는 미끼 계정에 구매 비용을 지불하고 거래소는 구매자가 다른 미끼 계정에서 구매한 금액과 동일한 금액을 판매자로 이체해 구매자와 판매자, 이체된 NFT 간의 연결 고리를 찾는 것이 어려워진다는 것이다. 하지만 이러한 미끼 계정을 통한 결제 방식은 드러난 미끼 계정 정보를 추적하는 방식을 통해 제3자가 거래 금액과 정보를 추적할 수 있다.

V. ARTeX 소개

5.1 ARTeX 개요

본 고는 RWA 토큰 거래의 익명성을 달성하기 위해 ARTeX라는 가상의 플랫폼을 가정하고 거래 과정을 따라가며 익명성을 강화하는 방안을 제안한다. ARTeX는 RWA 토큰을 판매자의 자유의사에 따라 상장을 통해 RWA 토큰을 거래할 수 있는 플랫폼을 제공한다고 가정한다.

5.1.1 전통적인 RWA 토큰 거래 상황

Fig. 1.은 일반적인 시장에서 RWA 토큰을 거래하는 모습을 나타낸다. 먼저 판매자는 시장에서 판매하고자 하는 토큰의 정보를 나열하여 잠재적 구매자에게 노출한다. 구매자는 나열된 토큰을 보고 구매를 결정하고, 적정 금액을 입찰하게 된다. 판매자는 상황에 따라 적정 가격으로 판매 계약을 설정하거나, 일정 기간 최고 입찰가를 받은 후 낙찰받은 가격으로 토큰을 판매할 수도 있다.

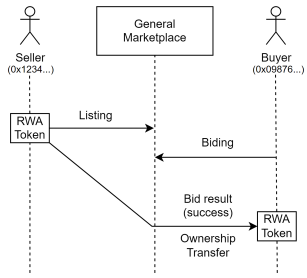

Fig. 1. The case of trading RWA tokens in general

5.1.2 ARTeX에서의 RWA 토큰 거래

ARTeX는 여기서 더 나아가 판매자와 구매자의 익명성 보호에 초점을 맞추고 있다. 판매자와 구매자를 한곳에 모아 거래하는 플랫폼의 역할을 하며 거래의 특성상 본인의 신원을 드러내고 싶지 않으면서도 어떤 토큰을 구매해야 하는지에 대한 명확한 정보를 얻을 수 있도록 돕는다. ARTeX는 토큰 거래 시장에 대한 신뢰를 제고하기 위해 기존 시장에서의 거래와는 다른 프로세스를 도입한다. 판매자는 판매 등록을 위해 RWA 토큰을 ARTeX에 보낸다. 전송된

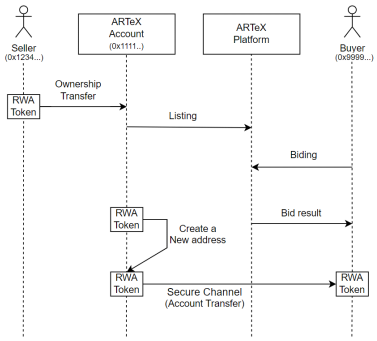

Fig. 2. The case of trading RWA tokens on ARTeX

RWA 토큰은 ARTeX 플랫폼에 상장되고 구매자는 RWA 토큰을 확인하고 구매를 위한 입찰 과정에 참여할 수 있다. Fig. 2.에는 개별 지갑 주소가 표시되어 있어 상장 과정과 구매자에게 보내는 패키징 과정의 차이를 명확하게 보여준다. 그러나 실제로는 이러한 지갑 주소가 공개적으로 노출되지 않아 누구도 확인할 수 없다.

5.1.3 거래 전 회원등록 및 KYC

거래에 앞서 판매자와 구매자 모두 ARTeX에 등록해야 한다. ARTeX는 판매 및 구매 시 정산에 필요한 KYC(Know Your Customer, 고객확인제도) 정보를 수집하여 보관한다. KYC 정보에는 여권, 정부 발행 ID 또는 운전면허증, 주민등록번호 등이 포함될 수 있으며, 등록된 회원이 거래 당사자임을 증명할 수 있는 서류도 필요할 수 있다. KYC 정보는 사기, 자금세탁 및 기타 불법행위를 방지하기 위해 필요하며, 불법적인 목적으로 발행된 토큰이 식별되는 경우 수사 협조를 위해 필요하다[11]. 판매자 및 구매자의 신원과 관련된 정보는 대중에 공개되지 않을 뿐만 아니라, 거래 당사자 간에도 공유되지 않는 것은 자명하다.

ARTeX 웹페이지를 통해 ID, 비밀번호, 현재 사용중인 이메일을 작성하여 제출하면 사용자는 잠정 회원가입을 완료하게 되며, 사용자는 해당 ID와 비밀번호로 로그인하여 ARTeX를 열람할 수 있으나 아직 거래는 할 수 없다. 여기서 사용자가 KYC 정보를 입력한 필드에 따라 KYC 정보를 입력하여 제출한 후, 검토가 완료되면 RWA 토큰을 거래할 수 있는 정회원으로 등록된다. 다음은 거래를 위한 준비 과정인 ARTeX 회원가입에 필요한 정보를 종합적으로 정리한 것으로, ARTeX는 이 정보를 안전하게 보관하며 거래 당사자 간 또는 외부와 공유하지 않는다[14]. ARTeX에서는 일반적인 전자상거래 서비스와 마찬가지로 토큰의 판매, 구매, 결제 등의 절차가 반드시 짧은 기간 내 연속적으로 발생하지 않을 수 있다. 따라서 로그인 과정에서 쿠키나 세션 ID 등 ARTeX 회원의 자격 증명을 확인할 수 있는 다양한 웹 서비스 기술이 필요할 것이다.

5.2 ARTeX 거래 프로세스

ARTeX에서의 거래 전 과정은 Fig. 3.과 같으며, 총 5단계로 구성된다.

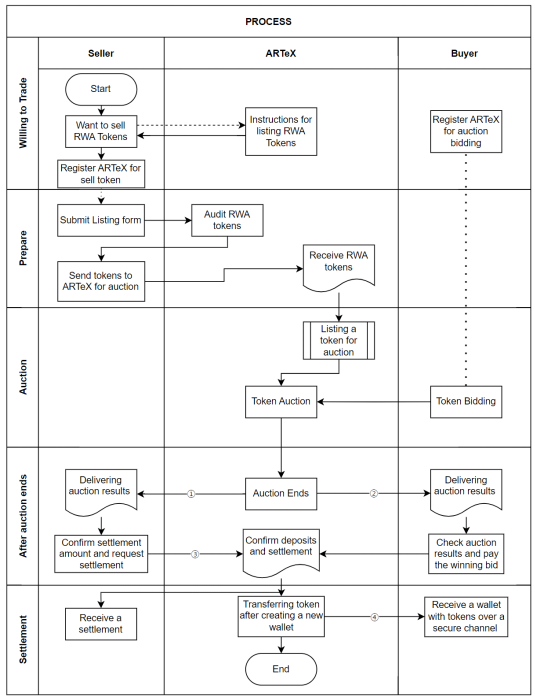

Fig. 3. ARTeX Trading process

5.2.1 토큰 소유자의 토큰 판매 준비 단계

토큰 보유자가 자신의 토큰을 판매하고자 하는 단계이다. 이 단계에서는 토큰 이동이 발생하지 않는다. 자신의 RWA 토큰을 ARTeX 시장에 상장하는 방법을 확인하고 가이드에 따라 토큰 판매를 결정한다. 이 단계에서 RWA 토큰의 ARTeX 상장을 위해

어떤 정보를 공개해야 하는지 가이드를 확인하고 ARTeX에 등록한다. 계정을 생성한 판매자는 RWA 토큰 판매를 위해 경매 등록에 필요한 정보를 입력하고 토큰 판매를 준비한다.

5.2.2 RWA 토큰 경매 준비 단계

판매자는 RWA 토큰을 ARTeX에 양도하여 판매한다. 토큰 양도가 확인되면 ARTeX는 토큰을 경매 등록하기 전 검토에 들어간다. 검토에는 토큰이 제대로 발행되었는지, 위법성은 없는지 등을 확인하는 작업이 포함된다. 토큰이 제대로 발행되었는지, 문제가 없는지 등이 확인되면 토큰은 ARTeX의 양식에 맞춰 ARTeX 웹사이트에 상장되고 경매를 위한 모든 준비를 마친다.

5.2.3 RWA 토큰 경매 진행 단계

등록된 RWA 토큰을 구매하고자 하는 사용자는 ARTeX를 통해 토큰 정보를 꼼꼼하게 점검하고 경매에 응찰한다. 경매가 최종적으로 마무리되면 토큰 판매자와 낙찰자에게 경매 결과가 전달된다. 최종 낙찰자와 별도로 별도의 공지 없이 토큰 경매가 종료되었음을 알린다. 구매를 희망하는 사용자는 ARTeX 내에서 사용할 수 있는 ID_B 계정을 직접 만들어 입찰에 참여한다. ID_{B_1}가 1ETH를 제안하면 ID_{B_2}는 1.1ETH처럼 조금 더 높은 입찰가를 제시해 상위 입찰자가 되는 방식으로 경매가 진행된다. Laffont의 게임 이론[13]에 따르면 경매는 실시간 공개 경매형, 영문 경매, 네덜란드 경매, 비공개 진행 경매형 등으로 구분되는데, ARTeX에서 어떤 방식을 채택할지는 실제 서비스에서 중요한 시스템 및 마케팅 요소가 될 수 있지만 본 논문의 요지인 익명성과는 무관하므로 임의적인 방식으로 안전하게 경매가 진행되었을 것으로 가정한다. 다만 경매 참여자에게 입찰가격 정보를 공개하지 않는 것이 경매에서 공정한 가격으로 거래를 보장한다는 연구[14]에 따라 기술적 환경이 가능하더라도 경매 참여자에게 입찰가격 정보를 공개하지 않는 방향으로 경매를 진행하는 것이 바람직할 것이다.

5.2.4 RWA 토큰 경매 종료 단계

일정 기간 후 경매가 종결되는 단계이다. ① 경매가 종료되면 ARTeX는 판매자에게 경매가 종료되었다는 사실과 함께 최종 낙찰금액을 알린다. ② 최종 낙찰자에게 거래 성사를 알리고, 낙찰금액과 지급 방법을 선택할 수 있도록 한다. 구매자는 하나의 지갑에서 ARTeX의 지갑 주소로 낙찰금액을 한꺼번에 이체할 수도 있고, 여러 지갑 주소에서 분할납부할 수도 있다. 옵션에 따라 원하는 만큼 ARTeX 지갑 주소를 확인할 수 있다. ③ 토큰 판매자는 최종 낙찰을 확인하고 ARTeX에 정산을 요청한다. 판매자는 경매할 정산금에 동의했음을 전달함과 동시에 정산금을 받을 지갑 주소를 ARTeX에 제공한다. 이때 판매자는 토큰을 소유하고 있던 지갑 주소 T_{sell_1}로 정산금을 받을 수 있고, 다른 옵션으로 자신이 소유한 다른 지갑 주소 P_{sell_2}로 정산금을 받을 수 있다. 일반적으로 후자의 경우가 익명성 보호에 유리하다. 판매자가 다른 지갑 주소로 정산금을 받으면 판매된 RWA 토큰의 이력을 확인할 때 ARTeX에 토큰을 전달하기 위해 얼마나 정산했는지 확인하는 것은 매우 어려워진다.

토큰 구매자는 경매에서 최종 입찰 금액을 ARTeX에 전달한다. 이를 정산받을 지갑 주소가 P_{A_1}라고 한다면, 토큰 판매자로부터 받은 지갑 P_{sell_2}과는 다른 지갑 주소다. 하나의 지갑 주소에서 전액을 이체하거나 분할 지급할 수 있다. 예를 들어, 100 ETH가 최종 낙찰가가 되어 이를 지급하는 경우 $P_{buy_1}(100ETH) \rightarrow P_{A_2}$ 로 한 번에 지급하거나 전체 금액을 분할해 각기 다른 지갑 주소로 나눠서 $P_{buy_1}(50ETH) + P_{buy_2}(30ETH) + P_{buy_3}(20ETH) \rightarrow P_{A_2}$의 방식으로 100 ETH를 지급할 수 있다. 마찬가지로 ARTeX로 송금받는 지갑 주소가 반드시 P_{A_2} 중 하나일 필요는 없으며 $P_{buy_1}(90ETH) \rightarrow P_{A_2}$ 및 $P_{buy_2}(10ETH) \rightarrow P_{A_3}$처럼 총액은 동일하나 각기 다른 지갑으로 전송하는 것도 가능할 것이다. ARTeX에 전체 낙찰금액에 맞게 전달된다면 최종 정산에는 문제가 없을 것이다. 결제금액이 적절하게 입금된 것이 확인되면 ARTeX는 토큰 구매자에게 전달할 별도의 지갑을 생성하고, 판매 완료된 RWA 토큰을 해당 지갑으로 전달한다.

5.2.5 RWA 토큰 거래 후 정산 단계

토큰의 판매자는 정산금을 받고자 하는 지갑 주소

P_{sell_1} 또는 P_{sell_2}로 판매 정산금을 받으면 판매 절차가 완료된다. ④ RWA 토큰이 포함된 새로운 지갑 T_{A_n}는 보안 채널을 통해 개인 키와 함께 구매자에게 전달되며 구매 절차도 완료된다. ARTeX는 플랫폼 페이지를 통해 토큰의 거래가 완료되었음을 알린다.

5.3 토큰이 포함된 지갑을 전달하기 위한 보안 채널

NFT 거래소 등 기존 블록체인 기반 거래 사업에서는 별도의 보안 채널을 통해 전달하는 방식이 일반적으로 사용되지 않는다. 다만 RWA 토큰의 익명성을 보호하기 위해, 보안 채널의 사용을 고려하여 ARTeX 모델에 적용한다. ARTeX는 완료된 거래에 대해 판매자로부터 토큰을 전달받아 새로운 지갑 주소를 생성한 후 별도의 보안 채널을 통해 구매자에게 전달한다. 이 방식을 사용하면 구매자는 지갑 주소 노출 없이 원하는 RWA 토큰을 안전하게 거래할 수 있고 거래를 완료할 수 있다. 구매자는 구매 후 필요에 따라 토큰을 개인 지갑으로 자유롭게 이전할 수 있으며, 거래된 토큰의 불법성이 의심되어 수사가 필요한 경우 수사관에게 수사 협조 요청이 오면 보안 채널을 통해 구매자에게 전달되는 지갑 주소를 가지고 있기에 ARTeX는 관련 정보를 제공할 수 있다. 이후 추적은 온체인 상에 기록된 단계까지 가능할 것이다. ARTeX는 법적 절차에 따라 제공할 수 있으며, 보안 채널을 통해 통신 결과를 제공하지 않더라도 수사기관이 토큰의 정확한 정보를 알고 있으면 추적 가능하다. 보안 채널 자체의 안전성은 모든 중앙집중형 전자상거래 서비스가 겪고 있는 보안 문제이므로 본 고에서는 별도로 다루지 않기로 한다.

VI. 분 석

ARTeX의 거래 과정을 따른다면 RWA 토큰 판매자와 구매자 간의 연계성이 어떻게 단절되어 익명성을 달성할 수 있는지 분석한다.

일반적인 P2P 거래에서는 Fig. 4.와 같이 거래 당사자가 일정 금액을 지급하고 이에 상응하는 토큰을 전달한다. 블록체인을 기반으로 한 RWA 토큰의 거래에서는 단순한 P2P 거래는 토큰의 거래 금액과 당사자 등의 기록이 그대로 블록체인에 온체인 데이터로 남게 된다. 블록체인 네트워크에 남은 기록은 누구나 확인할 수 있으므로 거래의 익명성이 보호되

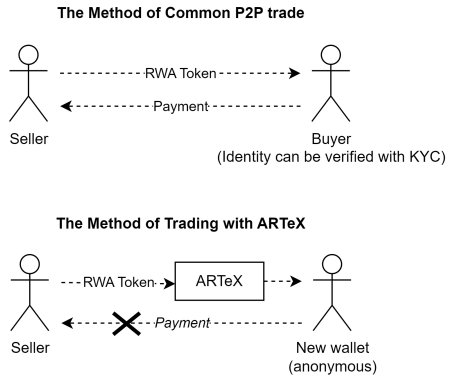

Fig. 4. Difference between Common P2P Trade and ARTeX Trade

지 않지만, ARTeX를 통해 이루어지는 거래에서는 실제로 RWA 토큰이 거래소에는 전달되지만, 누구에게 전달됐는지, 판매라면 얼마를 정산받았는지도 블록체인상에 기록되지 않는다. 따라서 제3자는 토큰 정보만으로는 거래로 보기도 어려울 수 있다. 기존 토큰 보유자의 지갑 주소를 확인하는 것만으로는 토큰의 이전만 확인되기 때문이다. 단순 토큰의 이동은 거래보다 기부나 단순 증여, 혹은 사기에 의한 피해일 가능성을 배제할 수 없다. 즉 토큰이 이전되었지만, 거래의 익명성은 그대로 유지되는데 이는 거래 당사자 간의 연결 고리를 차단하기 때문에 가능하다.

Table 1.에서 볼 수 있듯, 기존의 연구에서는 거래(Transaction)를 웹페이지 내에서 바로 확인할 수는 없더라도 블록체인에 기록으로 남아있는 경우 추적이 가능하며, 미끼 계정 사용 연구와 같이 블록체인 네트워크상에 기록이 부분적으로만 남기도록 하

Table 1. Comparing ARTeX's Process with Previous Work

Trait / Methods	Tx is available directly on screen	Tx recorded on the blockchain	Traceability
Simply, not exposed on screen	X	O	O
Hide the details of the token	X	O	O
Using Decoy Accounts	O	△	O
ARTeX Process	X	X	X

더라도 미끼 계정임이 인식되는 순간 추적이 가능하다. 앞서 살펴본 바와 같이 미끼 계정은 일회용 계정이 아니기에 시스템 관리자가 계속해서 사용하게 되므로 해당 계정 주소를 라벨링[15]해 추적할 수 있다.

6.1 토큰 판매자와 구매자 간의 연결 고리 끊기

익명성을 유지하는 가장 중요한 요소는 토큰 판매자와 구매자 간의 관계를 효과적으로 흐리게 만드는 것이다. 동시에 개인정보 보호를 위한 중추적인 전략은 거래 링크를 차단하는 것인데, 이는 외부 관점에서 보면 거래를 눈에 띄지 않게 만든다. 기존 거래에서 RWA 토큰은 공급업체의 지갑 주소 T_{sell}에서 구매자의 지갑 주소 T_{buy}로 전달된다. 또한, 거래 대금도 P_{buy}에서 P_{sell}로 전달된다. 이 거래 기록은 블록체인에 보관된다. 위에서 설명한 대로 당사자가 직접 거래하면 누구나 거래 내용, 즉 관련 토큰, 거래 시기, 거래 금액, 구매자의 신원을 쉽게 확인할 수 있다. 이 정보는 토큰의 거래를 확인하기만 하면 얻을 수 있다. 시간이 지남에 따라 더 많은 거래가 발생하더라도 이러한 기록은 블록체인에 영구적으로 저장되므로 과거 기록을 검토하는 것은 여전히 간단하다. 시간이 지남에 따라 데이터 변경과 삭제가 점점 더 어려워지는 블록체인의 본질은 거래 링크가 초기에 분리되지 않으면 익명성을 보장하기 어렵다는 점을 더욱 가중한다. 토큰의 거래 형태는 ARTeX 프로세스를 거쳐 $T_{sell_1} \rightarrow T_{A_1} \rightarrow T_{A_n}$순으로 전달된다. 거래 금액의 전달은 다양한 형태를 취할 수 있다.

(1) 구매자는 총입찰금액을 한 번에 지불하고, 판매자는 토큰을 보유하고 있던 지갑 P에서 정산받는다.

$$P_{buy_1} \rightarrow P_{A_2} \rightarrow P_{sell_1}$$

(2) 구매자는 총입찰금액을 한 번에 지불하고 판매자는 토큰을 보유한 지갑이 아닌 다른 지갑에서 정산금을 받는다.

$$P_{buy_1} \rightarrow P_{A_2} \rightarrow P_{sell_2}$$

(3) 구매자는 입찰금액을 여러 개의 지갑으로 나누어 지급하고, 판매자는 토큰을 보유하고 있던 지갑에서 다음과 같은 정산을 받는다.

$$P_{buy_1} + P_{buy_2} + P_{buy_3} \rightarrow P_{A_2} \rightarrow P_{sell_1}$$

(4) 구매자는 입찰금액을 여러 개의 지갑으로 나누어 대금을 지불하고, 판매자는 토큰을 보유한 지갑이 아닌 다른 지갑으로 대금을 받는다.

$$P_{buy_1} + P_{buy_2} + P_{buy_3} \rightarrow P_{A_2} \rightarrow P_{sell_2}$$

(5) 판매자는 의도에 따라 정산금을 여러 개의 지갑 주소로 나눠 받을 수 있다.

$$P_{buy_1} + P_{buy_2} + P_{buy_3} \rightarrow P_{A_2} \rightarrow P_{sell_2} + P_{sell_3} + P_{sell_4}$$

(6) 입찰금액을 여러 개의 지갑 주소로 나누어 지급하는 방법도 가능하다.

$$P_{buy_1} + P_{buy_2} + P_{buy_3} \rightarrow P_{A_2} + P_{A_3} + P_{A_4} \rightarrow P_{sell_2} + P_{sell_3} + P_{sell_4}$$

지갑 주소와 사용 방법이 (1)에서 (6)으로 발전함에 따라 복잡성이 증가하고, 그에 따라 익명성도 강화된다. (1)과 같이 토큰 판매 지갑으로 직접 정산금을 받는 경우, 일반적인 P2P 거래와 같이 블록체인에 기록이 남는다. 반면, (6)과 같이 거래에 사용되는 지갑의 수를 늘리면 정산금액이 분할되어 정확한 금액을 예측하기 어려워지며, 거래 당사자를 식별하기도 어렵다. 본 논문에서 언급한 기존 연구들은 다수의 지갑을 활용하여 거래를 분산하는 방안을 제시하지 않기 때문에, 거래 자체가 추적되면 그에 따라 거래 당사자의 정보와 거래 금액 등의 기록이 드러나게 된다.

6.2 RWA 토큰 거래를 위해 믹서 서비스를 이용하지 않는 이유

대체 가능 토큰의 경우, 믹서 서비스를 이용하여 거래 이력을 추적하기 어렵게 만들 수 있다. 하지만 RWA 토큰은 발행자의 필요에 따라 대체 불가능한 형태로 발행될 수 있기 때문에 믹서 서비스를 이용하여 목적을 달성할 가능성은 현저히 낮다. 또한 믹서 서비스의 경우, 불법성 논란 역시 있다. 바이낸스는 2019년 유명 믹서 서비스 코인조인(CoinJoin)을 통합한 프라이버시 보호 비트코인 지갑인 와사비(Wasabi)로의 인출을 차단하며 자금세탁 관련 자금이 유입된 정황이 있다고 발표했다[16]. 본 고에서 논의한 바와 같이 RWA 토큰 거래의 익명성을 보호하고자 함이 단순히 거래 기록을 숨겨 불법성에 활용

하기 위함이 아니므로 믹서 서비스를 사용하지 않는 것이 바람직할 것이다.

VII. 결 론

RWA 토큰 거래에서 가상의 플랫폼인 ARTeX로 살펴본 일련의 거래 프로세스는 블록체인에 자신의 개인정보를 명시적으로 밝히지 않고 토큰을 거래하기를 원하는 거래 당사자 모두 안심하고 거래할 수 있도록 돕는다. 본 논문은 단순한 서비스 제안이 아닌 현실 세계에서 구축된 체계화된 거래 프로세스가 웹 3 환경에 어떻게 적용될 수 있는지를 제시하려 노력했다. 여기에 포함된 일부 개인정보보호를 위한 개념들과 프로세스는 향후 연구를 통해 그 형태를 더욱 명확하게 개선해 실질적인 서비스 구현을 가능하게 하는 기반이 될 것이다. 다만 현재로서는 판매자와 구매자의 정보를 완전히 단절시키는 프로토콜은 제안하기 어렵다. 기술적으로도 그러하지만, 앞서 언급한 바와 같이 불법 토큰, 해킹, 사기 등으로 토큰 거래의 완전한 정보 단절은 개인 간 거래뿐만 아니라 정부 당국의 조사에도 부정적인 영향을 미칠 것이기 때문이다. 사안에 따라 안전성과 적법성을 충족할 방법이 제안된다면 판매자와 구매자의 연결 고리를 완벽히 분리할 수 있는 프로세스를 제안해볼 수 있을 것이다.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, Mar. 2008.

[2] T. Lambert, D. Liebau, and P. Roosenboom, "Security token offerings," *Small Business Economics*, pp. 1–27, Sep. 2021.

[3] T. J. Chaffer and J. Goldston, "On the existential basis of self-sovereign identity and soulbound tokens: An examination of the self" in the age of web3," *Journal of Strategic Innovation and Sustainability*, vol. 17, no. 3, pp. 1–9, Dec. 2022.

[4] G. A. Oliva, "Mining the ethereum blockchain platform: best practices and pitfalls (msr 2022 tutorial)," in *Proceedings of the 19th International Conference on Mining Software Repositories*, pp. 201–202, May. 2022.

[5] H. S. Galal and A. M. Youssef, "Aegis: Privacy-preserving market for non-fungible tokens," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 1, pp. 92–102, Sep. 2022.

[6] Z. Chen and K. Omote, "Toward achieving anonymous nft trading," *IEEE Access*, vol. 10, pp. 130166–130176, Dec. 2022.

[7] B. Notheisen, J. B. Cholewa, and A. P. Shanmugam, "Trading real-world assets on blockchain: an application of trust-free transaction systems in the market for lemons," *Business & Information Systems Engineering*, vol. 59, pp. 425–440, Oct. 2017.

[8] G. C. Krishna and P. J. IR, "Exploring the ethereum blockchain: An introduction to blockchain technology," in *Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies*, pp. 261–290, IGI Global, Sep. 2023.

[9] D. Bradbury, "Anonymity and privacy: a guide for the perplexed," *Network Security*, vol. 10, pp. 10–14, Oct. 2014.

[10] E. Moyakine, "Online anonymity in the modern digital age: Quest for a legal right," *Journal of Information Rights, Policy and Practice*, vol. 1, no. 1, Oct. 2016.

[11] D. George, A. Wani, and A. Bhatia, "A blockchain based solution to know your customer (kyc) dilemma," in 2019 *IEEE International Conference on Advanced Networks and Telecommunications Systems* (ANTS),

pp. 1 - 6, IEEE, Dec. 2019.
〔12〕 A. Conklin, G. Dietrich, and D. Walz, "Password-based authentication: a system perspective," in 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, pp. 10 - pp, IEEE, Jan. 2004.
〔13〕 J.-J. Laffont, "Game theory and empirical economics: The case of auction data," *European Economic Review,* vol. 41, no. 1, pp. 1 - 35, Jan. 1997.
〔14〕 W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *The Journal of finance*, vol. 16, no. 1, pp. 8 - 37, Mar. 1961.
〔15〕 Gayialis, Sotiris and Kechagias, Evripidis and Konstantakopoulos, Grigorios D. and Papadopoulos, Georgios and Tatsiopoulos, Ilias: "An approach for creating a blockchain platform for labeling and tracing wines and spirits. In: Advances in Production Management Systems. Artificial Intelligence for Sustainable and Resilient Production Systems." Proceedings, Part IV. pp. 81 - 89. Aug. 2021
〔16〕 Danny Nelson, "Binance blockade of wasabi wallet could point to a crypto crack-up," CoinDesk, 13 Sep. 2021.

〈저자소개〉

이 재 성 (Jaeseong Lee) 정회원
2015년 2월: 영남대학교 경영학전공 학사
2021년~2022년: 퓨처센스, 블록체인 개발자
2022년 9월~현재: 고려대학교 금융보안학과 석사과정
〈관심분야〉 블록체인, 프라이버시 보호, 정보보호

이 중 희 (Junghee Lee) 종신회원
2000년 2월: 서울대학교 컴퓨터공학과 공학학사
2003년 2월: 서울대학교 컴퓨터공학과 공학석사
2003년~2008년: 삼성전자, 연구원
2013년 2월: 조지아공과대학교 전자공학과 공학박사
2014년~2019년: University of Texas at San Antonio 교수
2019년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 하드웨어 보안