분산원장기술 기반 가상자산 송금 이용자 신원 확인 서비스 모델

박근덕 서울외국어대학원대학교 AI블록체인연구소 교수, ITU-T SG17 Q10 부라포처

1. 머리말

최근 블록체인 기반 가상자산(암호화폐)을 활용한 국경 간 송금(이전)이 증가하는 추세이다. 그러나 블록체인의 익명성 때문에 가상자산사업자(예: 암호화폐 거래소, 암호화폐 보관 사업자, 암호화폐 전자지갑 사업자 등)는 이용자(송금인 및 수취인)의 신원을 확인할 수 없기 때문에 자금세탁 관련 문제점이 존재한다. 이러한 문제점을 해결하기 위하여 가상자산사업자는 자금세탁방지를 위한 고객확인의무(CDD, Customer Due Diligence) 및 신원 정보 제공 규칙(예: 트래블룰, travel rule)을 준수할 수 있는 서비스 모델이 필요하다. 또한 가상자산사업자는 신원관리사업자가 참여하는 본 서비스 모델을 통하여 이용자의 개인정보를 포함한 신원 정보를 안전하게 확인하고 보관할 수 있다.

본고에서는 자금세탁방지 및 개인정보보호 관련 법 규정의 분석을 통하여 가상자산 관련 자금세탁방지를 위한 이용자 신원 확인 및 신원 정보 제공, 개인정보 파기 및 가명처리 등 요구사항을 식별하고, 가상자산사업자가 이용자(송금인 및 수취인)의 신원 정보를 확인할 수 있는 분산원장기술 기반 이용자 신원 확인 서비스 모델을 제안한다.

2. 가상자산 이용자 신원 정보 처리 관련 법 규정에 근거한 요구사항

가상자산사업자는 가상자산 관련 자금세탁방지를 위한 이용자 신원 확인 및 신원 정보 제공 요구사항, 가상자산 송금 이용자(송금인 및 수취인)의 개인정보 파기 및 가명처리 요구사항 등을 준수하여야 한다.

2.1 가상자산 이용자 신원 확인 및 신원 정보 제공

가상자산사업자는 국제자금세탁방지기구(FATF, Financial Action Task Force)의 지침을 반영하여 개정된 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」(이하 특금법) 및 「특

정 금융거래정보 보고 및 감독규정」(이하 감독규정) 등에 근거하여 가상자산 관련 자금세탁방지를 위한 이용자 신원 확인 및 신원 정보 제공 요구사항을 준수하여야 하고, 제3장에서 제안한 서비스 모델을 통하여 가상자산 송금 시 이용자(송금인 및 수취인)의 신원 정보를 확인 및 제공할 수 있다. 특히, 특금법 제5조의3(전신송금 시 정보제공)은 트래블룰(travel rule)로도 잘 알려져 있고, 특금법 및 감독규정에 근거한 요구사항은 다음과 같다.

- 특금법 제5조의2(금융회사등의 고객 확인의무)
- 특금법 제5조의3(전신송금 시 정보제공)
- 특금법 시행령 제10조의3(일회성 금융거래등의 금액)
- 특금법 시행령 제10조의4(고객의 신원에 관한 사항)
- 특금법 시행령 제10조의8(정보제공대상 전신송금 기준 금액)
- 감독규정 제26조(가상자산의 가격 산정 방식)

2.2 가상자산 이용자의 개인정보 파기 및 가명처리

가상자산사업자는 「개인정보 보호법」(이하 개보법) 등에 근거하여 가상자산 송금 이용자(송금인 및 수취인)의 개인정보 파기 및 가명처리 요구사항을 준수하여야 하고, 제3장에서 제안한 서비스 모델을 통하여 가상자산 이용자의 신원 정보에 포함된 개인정보를 완전 삭제, 가명처리 등의 방법으로 보호할 수 있다. 개보법에 근거한 요구사항은 다음과 같다.

- 개보법 제21조(개인정보의 파기)
- 개보법 제28조의2(가명정보의 처리 등)
- 개보법 제28조의4(가명정보에 대한 안전조치의무 등)
- 개보법 제28조의5(가명정보 처리 시 금지의무 등)
- 개보법 시행령 제16조(개인정보의 파기방법)
- 개보법 시행령 제29조의5(가명정보에 대한 안전성 확보 조치)

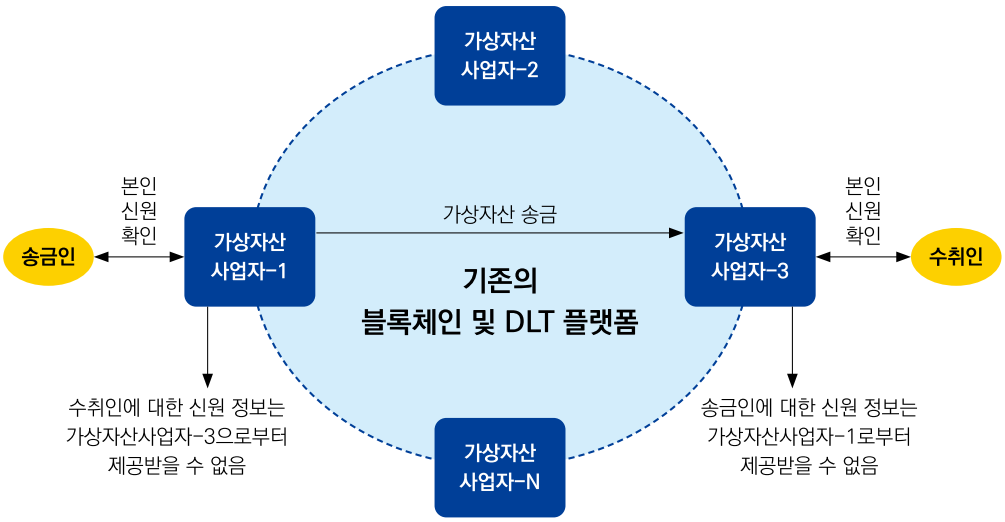
3. 가상자산 송금 이용자 신원 확인 서비스 모델

가상자산 송금 이용자 신원 확인 서비스 모델을 통하여 블록체인 기반 가상자산 송금 시 익명성으로 인한 이용자 신원 확인이 어려운 문제점을 해결할 수 있다.

3.1 가상자산 송금 시 익명성 문제점

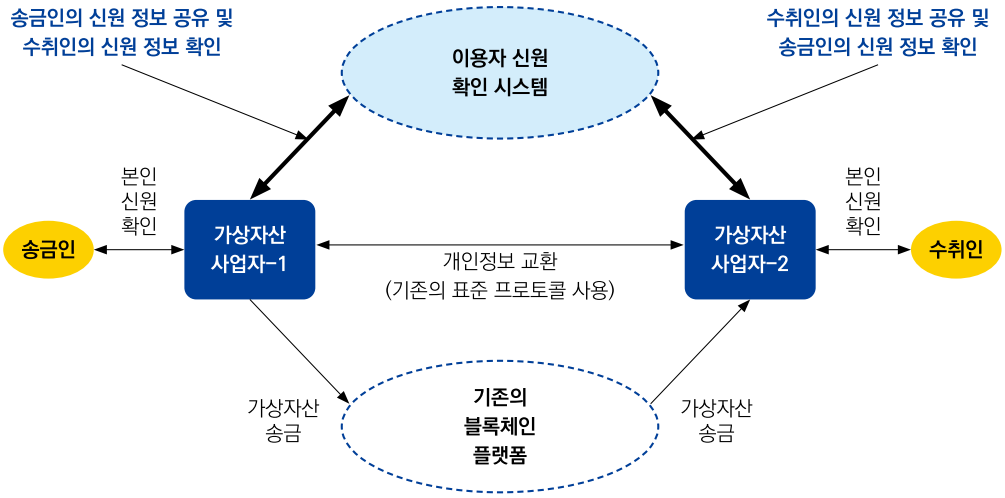
가상자산사업자는 가상자산 송금(이전) 시 자금세탁방지(AML, Anti-Money Laundering)를 위하여 고객확인의무 및 신원 정보 제공(예: 트래블룰)을 준수해야 하지만, 기존의 블록체인 및 분산원장기술(DLT, Distributed Ledger Technology) 플랫폼 환경에서 가상자산을 송금할 때 고객(이용자) 신원정보를 확인할 수 없는 문제가 있다. 이러한 문제는 기존 블록체인 및 DLT 플랫폼의 익명성에 기인한다. 예를 들어 최근 잘 알려져 있고 널리 사용되는 DLT 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)과 이더리움(Ethereum)의 경우, 전자지갑 생성 시 소유자의 신원을 확인하지 않으며, 가상자산 송금 관련 거래 기록을 저장할 때 송금인과 수취인의 신원 정보를 포함하지 않는다. 전자지갑 소유자의 익명성은 가상자산이 자금 세탁 및 테러 자금 조달에 악용되는 문제를 증가시킬 수 있다. 금융 분야에서도 이러한 익명성은 잠재적인 보안 위협으로 식별된다.

[그림 1]에서 기존 블록체인 및 DLT 플랫폼 환경 하에서 송금인이 가상자산을 수취인에게 송금하는 경우 가상자산사업자-1은 송금인의 신원을 확인할 수 있고 가상자산사업자-3은 수취인의 신원을 확인할 수 있다. 그러나 가상자산사업자-1은 가상자산사업자-3으로부터 수취인의 신



출처: 서울외국어대학원대학교 자체 작성

[그림 1] 가상자산 송금 관련 익명성



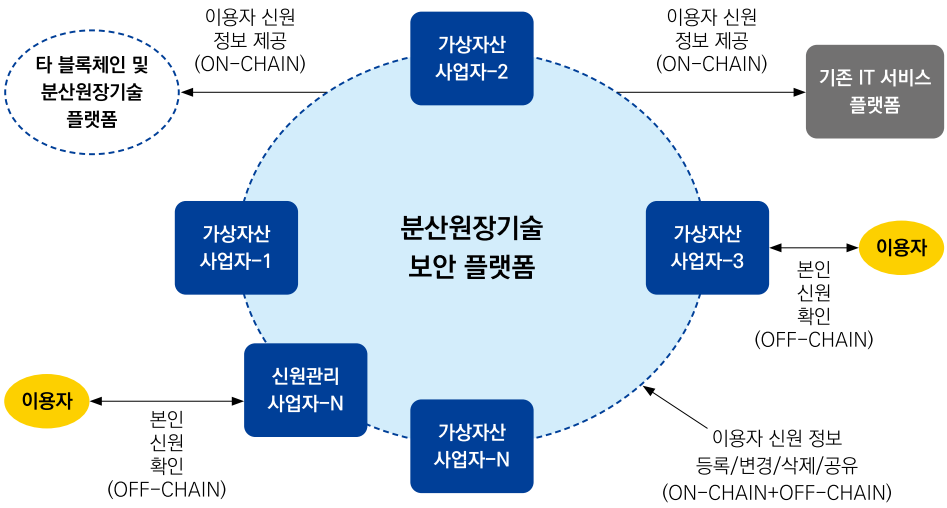
출처: 서울외국어대학원대학교 자체 작성

[그림 2] 이용자 신원 확인 서비스 모델

원 정보를 확인하는 것이 어려우며, 마찬가지로 가상자산사업자-3도 가상자산사업자-1로부터 송금인의 신원 정보를 확인하는 것도 어렵다. 특히 가상자산사업자 간에 이용자(송금인 및 수취인)의 신원 정보를 공유할 수 있는 인프라가 없기 때문에 국경 간 가상자산 송금 시 이용자의 신원을 확인하는 것은 사실상 불가능하다.

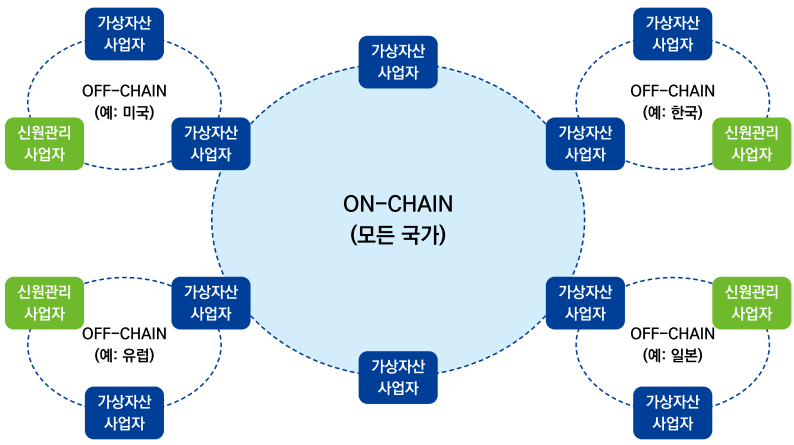
3.2 이용자 신원 확인 방안

본 절에서는 가상자산을 송금하기 전에 가상자산사업자가 송금인과 수취인의 신원을 확인하고 공유할 수 있는 서비스 모델을 제안한다. [그림 2]에서 가상자산사업자-1은 송금인의 신원을 확인한다. 그리고 이용자 신원 확인 시스템을 통하여 송금인의 신원 정보를 다른 가상자산사업자와 안전하게 공유하고 수취인의 신원 정보를



출처: 서울외국어대학원대학교 자체 작성

[그림 3] DLT 보안 플랫폼 기반 이용자 신원 확인 서비스 모델



* OFF-CHAIN : 동일한 사법 관할권에서만 이용자 신원 정보 등록, 변경 및 삭제
* ON-CHAIN : 모든 국가의 가상자산사업자 간의 이용자 신원 정보 공유

출처: 서울외국어대학원대학교 자체 작성

[그림 4] 온체인과 오프체인으로 구성된 DLT 보안 플랫폼

확인할 수 있다. 가상자산사업자-2는 수취인의 신원을 확인한다. 그리고 이용자 신원 확인 시스템을 통하여 수취인의 신원 정보를 다른 가상자산사업자와 안전하게 공유하고 송금인의 신원 정보를 확인할 수 있다. 이용자 신원 확인 시스템은 DLT를 사용하여 가상자산사업자를 연결하고 가상자산을 송금하는 기존의 블록체인 플랫폼(예: 이더리움 등)과 완전히 독립적으로 운영된다. 가상자산사업자-1은 기존의 표준 프로토콜(예: SAML, OpenID Connect, TLS 등)을 사용하여 송금인의 개인정보를 가상자산사업자-2에게 전송한다. 그 역도 마찬가지이다.

3.3 서비스 모델

DLT 기반의 이용자 신원 확인 서비스 모델은 이용자(송금인 및 수취인), 가상자산사업자

(VASP), 신원관리사업자(IDSP), 분산원장기술(DLT) 보안 플랫폼, 기존의 블록체인 및 DLT 플랫폼, 기존의 IT 서비스 플랫폼으로 구성된다. DLT 보안 플랫폼은 보안기능 요구사항을 충족하고 이용자의 신원 정보에 포함된 개인정보를 가명처리한다. 제안 서비스 모델은 VASP와 IDSP가 참여하는 DLT 시스템을 사용하여 VASP 간에 이용자의 최소한의 신원 정보를 안전하게 공유하고 검증할 수 있는 프레임워크를 제공한다. IDSP는 DID(Decentralized Identifier, 탈중앙화 식별자)를 사용하여 이용자를 식별할 수 있다.

[그림 3]에서는 DLT 보안 플랫폼을 기반 이용자 신원 확인 서비스 모델의 주요 구성 요소와 역할을 설명한다. VASP와 IDSP는 DLT 보안 플랫폼의 노드로 참여하며, 보안기능 요구사항을 충족하는 DLT 플랫폼은다음과 같다. DLT 보안 플랫폼은 이용자 신원 정보를 등록, 변경, 삭제 및 공유할 수 있는 온체인 및 오프체인([그림 4] 참조)으로 구성된다. VASP, 기존 블록체인 및 DLT 플랫폼, 기존 IT 서비스 플랫폼은 온체인(ON-CHAIN)에서 이용자 신원 정보를 제공받을 수 있다. 이용자는 VASP 또는 IDSP를 통하여 오프체인(OFF-CHAIN)에 자신의 신원 정보를 제공할 수 있다.

4. 맺음말

많은 국가의 가상자산사업자는 국경 간 가상자산을 송금하기 전에 개인정보를 포함한 방대한 이용자 신원 정보를 상호 공유함에 있어 이용자의 신원 정보가 변조되는 것을 방지하는 것이 매우 중요하다. 본고에서 제안한 서비스 모델은 중앙 집중식 데이터베이스가 아닌 분산원장기술(DLT)을 사용하여 이용자 신원 정보의 무결성을 유지하고, 자금세탁방지 관련 법 규정에서 요구하는 가상자산사업자 간, 가상자산사업자와 기존의 블록체인 및 DLT 서비스 제공자 간, 가상자산사업자와 기존의 IT 서비스 제공자 간의 이용자 신원 확인 서비스에 활용할 수 있다.

향후 본고에서 제안한 분산원장기술 기반 가상자산 송금 이용자 신원 확인 서비스 모델에 필요한 서비스 시나리오, 데이터 규격 등을 개발할 예정이다. 또한 분산원장기술 기반 가상자산 송금 이용자 신원 확인 시스템의 보안 위협을 식별하고 식별된 보안 위협을 완화시킬 수 있는 보안 요구사항을 정의한 신규 표준화 과제를 ITU-T SG17에 제안하여 국제표준으로 개발할 예정이다.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지원에 의하여 수행됨 [과제명: 차세대 보안 표준전문연구실, 과제번호: 2021-0-00112]

주요 용어 풀이

- **ITU-T SG17**: 국제전기통신연합(ITU) 산하의 전기통신표준화부문(T-섹터)에서 '정보보호' 분야의 표준을 개발하는 국제 공적표준화 기구

참고문헌

[1] 금융위원회, "특정 금융거래정보의 보고 및 이용 등에 관한 법률(법률 제18662호)", 2021년 12월

[2] 금융정보분석원, "특정 금융거래정보 보고 및 감독규정(금융정보분석원고시 제2021-1호)", 2021년 3월

[3] 개인정보보호위원회, "개인정보 보호법(법률 제16930호)", 2020년 8월

[4] 개인정보보호위원회, "가명정보 처리 가이드라인", 2022년 4월

[5] TTAK.KO-12.0336, 블록체인 용어정의, 2018년 12월

[6] TTAK.KO-12.0368, 분산원장시스템을 위한 보안기능 요구사항, 2020년 12월

[7] ITU-T X.1400, Terms and definitions for distributed ledger technology, October 2020

[8] Park, Keundug, and Heung-Youl Youm. 2021. "Proposal for Customer Identification Service Model Based on Distributed Ledger Technology to Transfer Virtual Assets" Big Data and Cognitive Computing 5, no. 3: 31. https://doi.org/10.3390/bdcc5030031

[9] 한국경제, "빗썸·코인원·코빗, '트래블룰' 내년 1월 가동…업비트와 연동 가능성도", https://www.hankyung.com/finance/article/202112085029g, 2021년 12월