chapter 2

가상 자산 송금을 위한 분산원장기술 기반 이용자 신원 확인 서비스 모델

박근덕 ‖ 서울외국어대학원대학교 교수

I. 서론

최근 블록체인(Blockchain) 기반 가상 자산을 사용한 해외 송금이 매년 증가하고 있는 추세이다. 글로벌 법정 화폐 송금 시장규모는 2017년 기준 1.9조 달러이고, 한국에서의 해외 송금액 규모는 2018년 기준 134억 달러 규모로 추산된다[9],[10]. 블록체인 및 분산원장기술(Distributed Ledger Technology: DLT)의 발전에 따라 가상 자산 송금 시장이 빠른 송금 시간, 저렴한 수수료 등을 강점으로 법정 화폐 송금 시장을 대체할 수 있을 것으로 예상된다. 각 국가별 수수료율이 다르지만 2017년 200달러 기준 해외 송금 평균 수수료율은 7.14%(약 14달러)이고, 가상 자산 송금의 경우 이보다 저렴한 수수료율을 적용할 수 있어 이용자의 부담을 줄일 수 있을 것이다[11].

그러나 블록체인의 익명성에 기인하여 가상 자산 사업자는 송금인 및 수취인의 신원을 확인할 수 없기 때문에 자금세탁 관련 문제점이 존재한다. 또한, 국제자금세탁방지기구(The Financial Action Task Force: FATF)는 2019년 6월에 발표한 가상 자산 관련 자금세탁방지 지침을 통해 가상 자산 사업자에게 자금세탁방지 의무를 부여하였고, 이에 따라 국내에서는 FATF 지침을 반영하여 2020년 3월에 개정된 「특정 금융거래정보의

* 본 내용은 박근덕 교수(☎ 02-2182-6017, jacepark926@gmail.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

보고 및 이용 등에 관한 법률」(일명: 특금법)을 통해 국제 기준을 이행한다. 본 고에서는 가상 자산 사업자가 고객확인의무(Customer Due Diligence: CDD)를 준수하여 자금 세탁 방지를 이행할 수 있도록 송금인 및 수취인의 신원을 확인할 수 있는 DLT 기반 이용자 신원 확인 서비스 모델을 제안하고자 한다.

II. 가상 자산 송금 시 신원 확인 방안

본 장에서는 기존의 블록체인 및 DLT 플랫폼 환경에서의 가상 자산 송금과 이용자(송금인 및 수취인) 신원 확인 방안에 대해 설명한다.

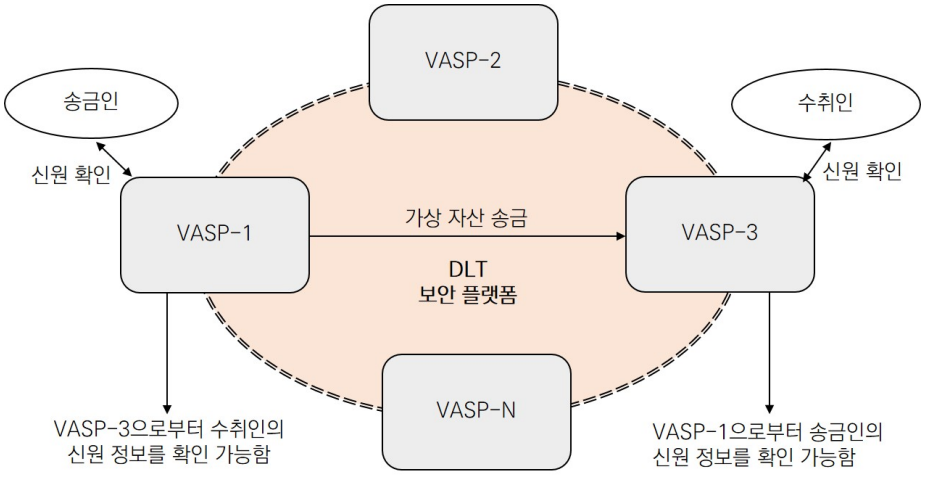
1. 가상 자산 송금

기존의 블록체인 및 DLT 플랫폼 환경에서 가상 자산 송금은 송금인이 보유한 가상 자산의 소유권을 수취인에게 이전하는 것을 의미한다. 이를 거래(Transaction)라고 한다. 예를 들어, 이더리움(Ethereum)에서 가상 자산을 송금하는 경우, 송금인과 수취인 간의 거래에 필요한 정보는 송금인의 전자지갑 주소, 수취인의 전자지갑 주소 및 이더(Ether) 금액 등이다[17]. 그러나 송금인과 수취인의 신원 정보는 확인할 방법이 없다. 이러한 이용자(송금인 및 수취인)의 익명성은 가상 자산을 통한 자금 세탁 및 테러 자금 조달에 악용되고 있는 실정이다.

2. 이용자 신원 확인 방안

가상 자산 사업자(Virtual Asset Service Provider: VASP)는 고객(이용자)의 신원을 확인하지만 VASP 간에 이용자의 신원 정보를 공유하는 것은 매우 어렵다. 다시 말해서, 가상 자산을 송금할 때, 송금인 측의 VASP는 상대방 VASP의 수취인에 대한 신원 정보를 확인할 수 없으며 그 반대도 마찬가지이다.

본 고에서는 가상 자산 사업자가 국내 또는 국경 간 가상 자산을 송금할 때 송금인과 수취인의 신원을 확인하고 공유할 수 있는 서비스 모델을 제안한다. [그림 1]과 같이 VASP-1은 송금인의 신원을 확인하고 DLT 보안 플랫폼을 사용하여 송금인의 신원 정보



〈자료〉 서울외국어대학원대학교 자체 작성

[그림 1] 이용자 신원 확인 서비스 모델

를 다른 VASP와 안전하게 공유한다. VASP-3은 수취인의 신원을 확인하고 DLT 보안 플랫폼을 사용하여 수취인의 신원 정보를 다른 VASP와 안전하게 공유한다. 따라서 VASP는 DLT 보안 플랫폼을 통해 공유된 송금인 및 수취인의 신원 정보를 확인할 수 있다. 여기서 신원 정보는 전자지갑 소유자 일치 여부, 전자지갑 불법 사용 여부 등을 포함한다. 가상 자산을 송금하는 기존의 블록체인(예; 이더리움, 리플넷 등)과 송금인 및 수취인의 신원 정보를 보관 및 공유하는 DLT 보안 플랫폼은 각각 독립적으로 운영된다.

III. 가상 자산 이용자 신원 확인 문제점 및 요구사항

본 장에서는 자금세탁방지 및 개인정보 보호와 관련된 국내외 규제, 기존 블록체인 및 DLT 플랫폼에서의 이용자 신원 확인 문제를 설명한다.

1. 자금세탁방지를 위한 고객확인의무

국제자금세탁방지기구인 FATF는 2020년 4월 현재 37개 회원국과 전 세계 모든 지역에서 가장 중요한 금융 센터를 대표하는 2개의 지역 조직으로 구성되어 있다[12].

지난 2019년 6월에 FATF는 “가상 자산 및 가상 자산 사업자에 대한 지침(GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS)”을 제정하였고, “자금세탁 및 테러자금 확산 방지에 관한 국제 표준(INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION)”이라는 권고안(Recommendation)을 개정하였다. FATF 지침 내 “권고 15-신기술(Recommendation 15-New Technologies)” 및 “주석서 15(Interpretative Note to Recommendation 15(INR. 15))”는 가상 자산 사업자에게 중요한 내용이다. 특히, “주석서 15”의 제7조 (a)항 및 (b)항은 VASP에 적용되는 고객확인의무(CDD)를 명시하고 있다[1].

2020년 3월에 FATF에서 제정된 “디지털 신원에 대한 지침(Guidance on Digital Identity)” 제3장 고객확인의무에 대한 FATF 표준(SECTION III: FATF STANDARDS ON CUSTOMER DUE DILIGENCE) 제79조에 근거하여 VASP는 이용자의 문서/물리적 형태의 신원 정보뿐만 아니라 디지털 형태의 신원 정보를 사용하여 고객확인의무를 수행할 수 있다[4].

FATF 권고안 내 “주석서 16(Interpretative Note to Recommendation 16(INR. 16))”은 국경 간 송금에 수반되는 신원 정보(예; 송금인 및 수취인 이름, 송금인과 수취인의 계좌번호 등)를 명시하고 있다[2].

상기에서 언급한 FATF 지침 및 권고에 근거한 규제 사항을 요약하면 다음과 같다.

- 규제의 목적은 가상 자산 사업자에게 자금세탁방지 의무를 부과함
- 규제 대상은 가상 자산을 교환, 양도(송금), 보관, 발행 또는 판매하는 개인 또는 법인인 가상 자산 사업자
- 가상 자산 사업자는 금융 당국으로부터 사업 허가를 받아야 함
- 국가는 가상 자산 사업자의 자금세탁방지 준수 여부를 관리·감독해야 함
- 가상 자산 사업자는 가상 자산 양도(송금) 시 송금인 및 수취인의 신원 정보를 확보하여야 함

FATF가 발표한 “가상 자산 및 관련 사업자에 대한 공개 성명서(Public Statement on Virtual Assets and Related Providers)”에 따르면, 가상 자산이 범죄 및 테러에 악용되는 위협이 심각한 수준이므로 FATF는 모든 국가가 가상 자산 활동 및 사업자와 관련하여

FATF 권고안을 이행하기 위한 즉각적인 조치를 취할 것을 요구하고 있고, FATF는 국가 및 사업자의 새로운 요구 사항에 대한 이행을 모니터링하고 2020년 6월부터 12개월 동안 이행점검을 수행한다고 밝히고 있다[3].

이에 따라 국내에서는 2020년 3월에 FATF 지침 및 권고안을 대부분 반영한 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」(일명: 특금법)을 개정하여 가상 자산 사업자의 자금세탁방지 준수 여부를 관리·감독할 수 있는 근거를 마련하였다[5].

2. 개인정보 보호

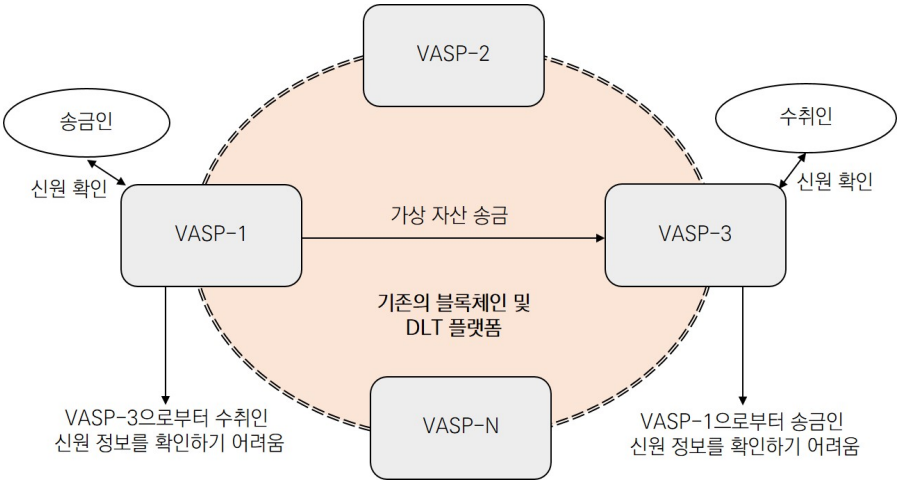
유럽연합(EU)의 “일반 데이터 보호 규정(General Data Protection Regulation: GDPR)”은 “해설전문 제156조”, “제4조 정의 제(5)항”, “제17조 삭제권(잊힐 권리)” 등에 개인정보의 가명화 및 삭제권(잊힐 권리)을 명시하고 있다[14].

국내에서는 EU GDPR 적정성 평가를 위해 2020년 2월에 개정된 「개인정보 보호법」에서는 “제2조(정의) 제1의2항”, “제21조(개인정보의 파기)”, “제28조(가명정보의 처리 등)” 등에 개인정보의 파기 및 가명정보의 처리를 명시하고 있다[15].

3. 이용자 신원 확인의 문제점

제III장 제1절에서 언급했듯이 VASP는 자금세탁방지를 위해 고객확인의무를 준수하여야 한다. 그러나 기존의 블록체인 및 DLT 플랫폼의 익명성 때문에 가상 자산을 송금 시 이용자(송금인 및 수취인)의 신원을 확인할 수 없는 문제가 있다. 예를 들면, 이미 널리 사용되고 있는 DLT 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)과 이더리움 등을 활용하여 전자지갑을 만들 때 소유자의 신원을 확인하지 않으며, 가상 자산의 양도(송금) 거래 기록을 저장할 때 송금인 및 수취인의 신원을 확인하지 않는다[6],[7]. 전자지갑 소유자의 익명성으로 인해 가상 자산이 자금 세탁 및 테러 자금 조달에 악용되는 사례가 증가하고 있고[16], 금융 부문에서 익명성은 잠재적인 보안 위협으로도 식별된다[8].

[그림 2]와 같이 송금인이 기존 블록체인 및 DLT 플랫폼(예; 이더리움, 리플넷 등)을 통해 가상 자산을 수취인에게 송금하기에 앞서 VASP-1은 송금인의 신원을 확인할 수 있고 VASP-3은 수취인의 신원을 확인할 수 있다. 그러나 기존의 가상 자산을 송금하는



〈자료〉 서울외국어대학원대학교 자체 작성

[그림 2] 가상 자산 송금 시 이용자 익명성

블록체인 및 DLT 플랫폼(예; 이더리움, 리플넷 등)의 익명성으로 인해 VASP-1이 VASP-3으로부터 수취인의 신원 정보를 확인하는 것은 어렵고, 또한 VASP-3이 VASP-1로부터 송금인의 신원 정보를 확인하는 것도 어렵다.

VASP 간에 이용자 신원 정보를 공유할 수 있는 글로벌 인프라가 없기 때문에 국경 간 가상 자산 송금 시 VASP가 송금인 및 수취인의 신원을 확인하는 것은 사실상 불가능하다. 이러한 문제를 해결하기 위해 최근 쿨빗엑스(CoolbitX)사에서는 시그나 브릿지(Signa Bridge)[18]를 통해 이용자의 신원 정보를 VASP 간에 공유하는 서비스를 제공하고 있다. 시그나 브릿지는 중앙화된 서버 기반의 단순 메시징 서비스이지만, 본 고에서 제안한 서비스 모델은 분산원장기술을 기반으로 하고 있기 때문에 개인정보보호 측면에서 차별적 우위성이 있다.

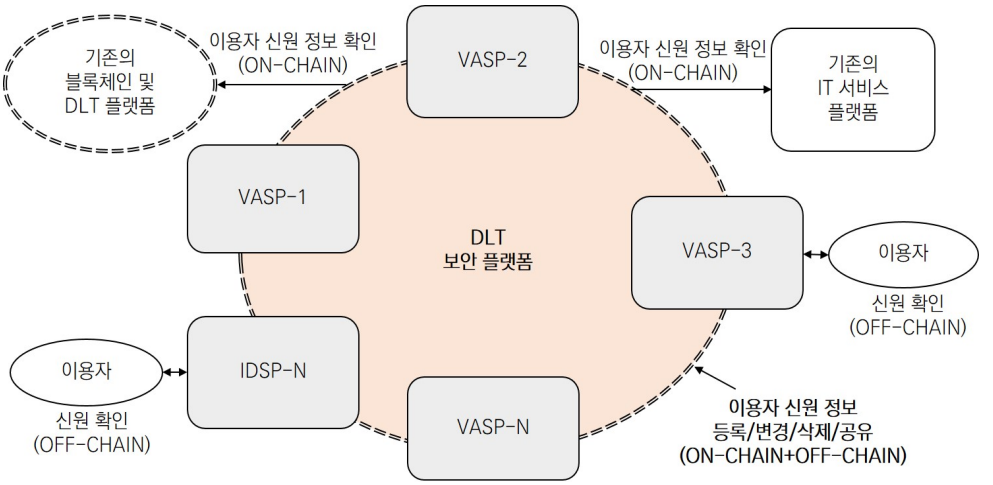
IV. 이용자 신원 확인 서비스 모델 제안

본 장에서는 제III장 제3절에서 언급된 이용자 신원 확인 문제를 해결하기 위해 가상 자산 송금을 위한 DLT 기반 이용자 신원 확인 서비스 모델을 제안한다.

1. 개요

DLT 기반 이용자 신원 확인 서비스 모델은 이용자(송금인 및 수취인), 가상 자산 사업자(VASP), 신원 사업자(IDSP), DLT 보안 플랫폼, 기존 블록체인 및 DLT 플랫폼, 기존 IT 서비스 플랫폼 등으로 구성된다.

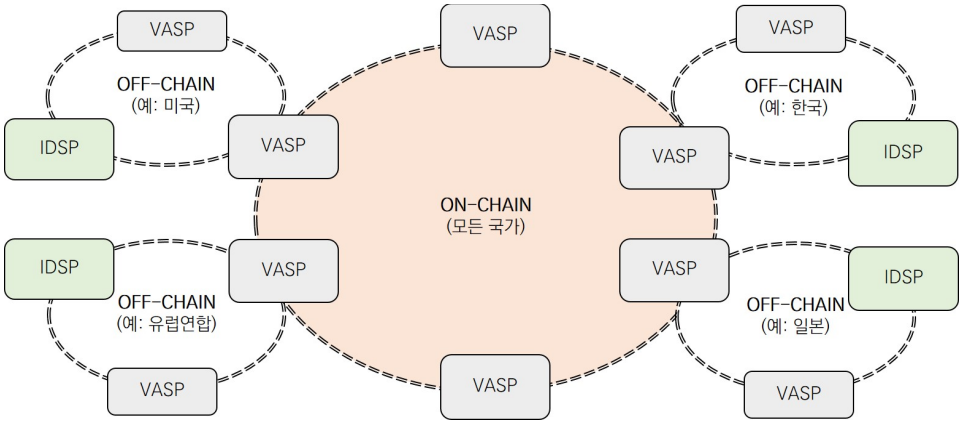
[그림 3]과 같이 DLT 보안 플랫폼은 이용자(송금인 및 수취인) 신원 정보를 등록, 변경, 삭제 및 공유할 수 있는 온-체인(ON-CHAIN)[13] 및 오프-체인(OFF-CHAIN)[13]으로 구성된 허가형(Permissioned) 및 폐쇄형(Private) 분산원장시스템(Distributed ledger system)[13]이다. VASP, 기존 블록체인 및 DLT 플랫폼, 기존 IT 서비스 플랫폼은 온-체인을 통해 이용자 신원 정보를 확인할 수 있다. 이용자는 VASP 또는 IDSP를 통해 오프-체인에 자신의 신원 정보를 제공할 수 있다.



* IDSP: Identity Service Provider(신원 사업자)
* VASP: Virtrual Asset Service Provider(가상 자산 사업자)
〈자료〉 서울외국어대학원대학교 자체 작성

[그림 3] DLT 기반 이용자 신원 확인 서비스 모델

[그림 4]와 같이 IDSP는 오프-체인에 참여하고 VASP는 온-체인에 참여하지만, IDSP 역할을 하는 VASP는 오프-체인에 참여할 수 있다. 본 서비스 모델에서는 오프-체인을 사용하여 동일한 사법 관할권 내에서만 비식별화(de-identification) 처리된 이용자 신원 정보를 등록, 변경 및 삭제하고, 온-체인을 사용하여 모든 국가에서 VASP 간에 비식별화



* IDSP: Identity Service Provider(신원 사업자)
* VASP: Virtual Asset Service Provider(가상 자산 사업자)
* OFF-CHAIN: 동일한 사법 관할권 내에서 신원 사업자를 통해 이용자 신원 정보를 등록, 변경, 삭제함
* ON-CHAIN: 모든 국가에서 가상 자산 사업자 간에 이용자 신원 정보를 공유함
〈자료〉 서울외국어대학원대학교 자체 작성

[그림 4] ON-CHAIN과 OFF-CHAIN

처리된 이용자 신원 정보를 공유한다.

본 서비스 모델의 주요 구성 요소인 DLT 보안 플랫폼은 다음과 같은 보안기능 요구사항을 충족해야 한다.

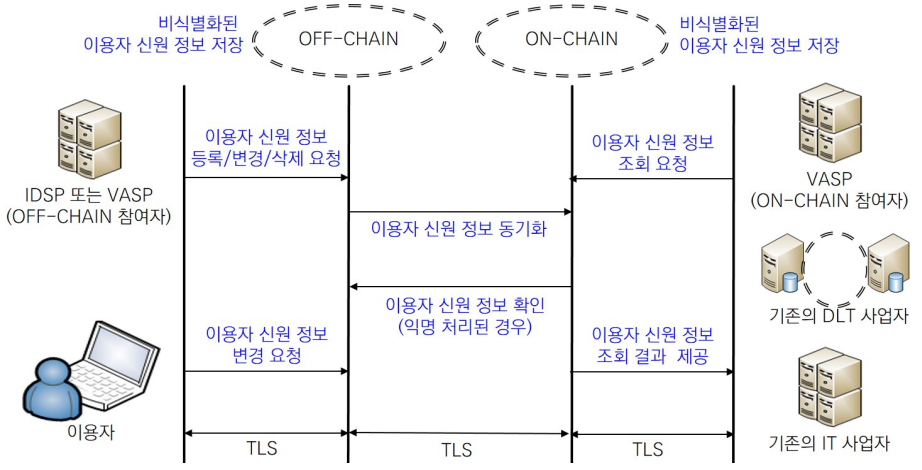
- 식별 및 인증: 분산원장기술시스템은 본인 확인 절차에 따라 이용자 또는 애플리케이션을 식별하고 인증하는 수단을 제공할 필요가 있다. 또한, 거래의 중요도에 따라 강화된 인증 수단(예; 일회용 패스워드, 인증서 등)을 적용한다[8].
- 보안 감사: 분산원장기술시스템은 이용자의 행위 이력을 기록하고 안전하게 보관하여 보안사고 발생에 대한 책임을 추적할 수 있는 수단을 제공할 필요가 있다[8].
- 통신 보호: 분산원장기술시스템은 분산 원장 네트워크에 참여하는 노드 간의 중요 정보 전송 시 안전한 통신 수단을 제공한다. 또한, 분산원장기술시스템과 외부 시스템 간의 중요 정보 전송 시 안전한 통신 수단을 제공할 필요가 있다[8].
- 암호 통제: 분산원장기술시스템은 이용자 간의 거래 시 전자서명, 중요 정보 전송 또는 저장 시 데이터 암호화 등을 위한 암호키를 안전하게 처리(생성, 이용, 보관, 파기 등)할 수 있는 수단을 제공할 필요가 있다[8].
- 접근 통제: 분산원장기술시스템은 비인가자가 중요 정보자산(분산 원장, 스마트 계약,

분산 원장 네트워크 등)에 무단으로 접근하는 것을 통제할 수 있는 수단을 제공할 필요가 있다[8].

- 개인정보 보호: 분산원장기술시스템은 이용자의 개인정보가 유출 및 노출되지 않도록 안전하게 처리(수집, 이용, 보관, 파기 등)할 수 있는 수단을 제공할 필요가 있다[8].
- 데이터 보호: 분산원장기술시스템은 이용자의 거래 데이터, 분산 원장 데이터(개인정보 포함) 등 중요 정보가 유출 또는 위·변조되지 않도록 안전하게 전송 또는 저장하는 수단을 제공할 필요가 있다[8].
- 자원 가용성: 분산원장기술시스템은 분산 원장 네트워크에 참여하는 노드의 시스템 자원(CPU, 메모리, 네트워크, 스토리지 등) 부족, 분산원장기술시스템을 운영하는 소프트웨어 오류 등에 대응하여 시스템 가용성을 극대화할 수 있는 수단을 제공할 필요가 있다[8].

2. 서비스 시나리오 및 데이터 흐름

본 절에서는 VASP 또는 IDSP와 오프-체인의 관계, 이용자와 오프-체인의 관계를 설명한다. 또한, VASP와 온-체인의 관계, 기존의 DLT 사업자 또는 IT 사업자와 온-체인의 관계, 온-체인과 오프-체인의 관계에 대해서도 설명한다.



* TLS: Transport Layer Security
〈자료〉 서울외국어대학원대학교 자체 작성

[그림 5] 서비스 시나리오 및 데이터 흐름

[그림 5]와 같이 오프-체인의 참여자인 IDSP 및 VASP는 오프-체인에서 이용자 신원 정보를 등록, 변경 및 삭제한다. 이용자는 오프-체인을 통해 자신의 신원 정보(예; 전자지갑 주소 등)를 변경한다. 오프-체인 및 온-체인은 비식별화 처리된 이용자 신원 정보를 저장한다. 오프-체인은 이용자 신원 정보를 온-체인과 동기화한다. 이용자 신원 정보가 익명화(Anonymization) 처리된 경우 온-체인은 해당 신원 정보를 오프-체인에서 추가로 확인할 필요가 있다. 온-체인의 참여자인 VASP는 온-체인에서 이용자 신원 정보를 확인한다. 기존의 DLT 사업자와 IT 사업자는 온-체인을 통해 이용자 신원 정보를 확인한다. VASP는 송금인 및 수취인의 신원 정보를 확인한 결과, 각각 '유효'한 경우에만 가상자산을 송금해야 한다. 여기서 '유효'는 '송금 거래 가능'을 의미한다.

[표 1]과 같이 본 서비스 모델에서 이용자 신원 확인을 위한 데이터는 이용자 번호, 국가 코드, 성명, 인증서, 전자지갑 주소, 가상 자산 사업자명, 신원 사업자명, 유효성 등으로 구성된다.

[표 1] 데이터 규격

항목	비식별화 처리 여부	값	설명
D-0	-	이용자 번호	- 이용자에게 부여된 유일한 번호 - D-1~D-3에 대한 해쉬 값
D-1	비식별화	국가 코드	- 이용자의 국가 코드 - 예: 한국(KR), 미국(US) 등
D-2	비식별화	성명	- 이용자(개인 또는 법인)의 성명
D-3	비식별화	인증서	- 이용자 신원을 증명할 수 있는 인증서 - 예: X.509 규격, 공개키 등
D-4	비식별화	전자지갑 주소	- 이용자 소유의 가상 자산을 송금할 전자지갑 주소
D-5	-	가상 자산 사업자명	- 이용자의 전자지갑을 관리하고 있는 가상 자산 사업자 명칭 또는 식별자
D-6	-	신원 사업자명	- 이용자의 신원을 확인한 신원 사업자 명칭 또는 식별자 - 가상 자산 사업자가 신원 사업자일 수도 있음
D-7	-	유효성	- 이용자 신원의 유효성 - 예; Valid(송금 거래 가능), Invalid(송금 거래 불가), N/A (확인할 수 없음, 송금 거래 불가) 등 - Invalid 예시: 전자지갑 소유자가 불일치, 전자지갑이 불법 거래에 사용 등
D-8	-	예약	- 예약
D-9	-	예약	- 예약

〈자료〉 서울외국어대학원대학교 자체 작성

3. 기대 효과

가상 자산을 사용한 국내 또는 국경 간 송금 시, 본 서비스 모델은 VASP에게 다음과 같은 이점을 제공한다.

- VASP는 본 서비스 모델을 통해 이용자 신원 정보를 등록하고 확인함으로써 FATF 지침 및 국내 법규에 명시된 자금세탁방지에 필요한 고객확인의무를 준수할 수 있다.
- VASP는 본 서비스 모델을 통해 이용자의 개인 정보를 비식별화 처리함으로써 EU GDPR, 국내 개인정보 보호법 등 개인정보보호 관련 법규를 준수할 수 있다.
- VASP는 본 서비스 모델을 통해 송금인 및 수취인의 신원 확인 문제를 해결할 수 있다.

V. 결론

가상 자산을 활용한 송금, 특히 국경 간 송금 규모가 최근에 증가하고 있고, 이에 따라 규제 당국은 가상 자산 관련 자금 세탁 문제를 심각하게 우려하고 있다. 그 이유는 기존의 블록체인 및 분산원장기술의 익명성으로 인해 가상 자산을 활용한 송금 시 송금인과 수취인의 신원을 확인하는 것이 현실적으로 불가능하기 때문이다. 이러한 문제를 해결하기 위해 국제자금세탁방지기구(FATF)는 2019년 6월에 가상 자산 관련 자금세탁방지 지침을 제정하여 가상 자산 사업자에게 고객확인의무를 부과하였고, FATF의 회원국인 우리나라는 이러한 FATF 지침을 반영하여 2020년 3월에 개정된 특금법을 통해 국내의 가상 자산 사업자를 규제할 수 있게 되었다.

본 고에서는 이러한 이용자 신원 확인 문제를 기술적으로 해결하고 가상 자산 관련 자금 세탁 방지를 위해 DLT 기반의 이용자 신원 확인 서비스 모델을 제안하였다. 본 서비스 모델은 이용자(송금인 및 수취인), 가상 자산 사업자, 신원 사업자, DLT 보안 플랫폼 등으로 구성된다. DLT 보안 플랫폼은 식별 및 인증, 보안 감사, 통신 보호, 암호 통제, 접근 통제, 프라이버시 보호, 데이터 보호, 자원 가용성 등과 같은 보안기능 요구사항을 만족한다. 또한, 온-체인과 오프-체인으로 구성된 DLT 보안 플랫폼은 이용자의 개인 정보를 비식별화 처리하여 EU GDPR, 한국의 개인정보 보호법 등 법적 요구사항을 만족한다.

본 서비스 모델은 온-체인 및 오프-체인을 활용하여 이용자의 신원 정보를 VASP 간에 안전하게 공유하여 자금세탁 방지를 위한 이용자 신원 확인 문제를 해결할 수 있다. 본 서비스 모델은 2020년 3월에 TTA PG502에서 정보통신단체표준 과제로 채택되었고, 향후 ITU-T SG17에서 국제 표준으로 개발될 예정이다.

[참고문헌]

[1] The Financial Action Task Force(FATF), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," 2019. 6.

[2] The Financial Action Task Force(FATF), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," 2019. 6.

[3] The Financial Action Task Force(FATF), "Public Statement on Virtual Assets and Related Providers," 2019. 6.

[4] The Financial Action Task Force(FATF), "Guidance on Digital Identity," 2020. 3.

[5] 금융위원회, 법무부, "「특정 금융거래정보의 보고 및 이용 등에 관한 법률」," FIU기획행정실, 국제형사과, 2020. 3.

[6] 하이퍼레저 패브릭 커뮤니티, 엔터프라이즈를 위한 블록체인 플랫폼(A Blockchain Platform for the Enterprise), 리눅스 재단, 2020. 4.

[7] 이더리움 커뮤니티, 이더리움 홈스테드 문서(Ethereum Homestead Documentation), 이더리움 재단, 2020. 4.

[8] 박근덕, 김대경, 염흥열, "오픈소스 기반 분산원장기술시스템을 위한 보안 강화 방안," 한국정보보호학회, 29(4), 2019. 8, pp.919-943.

[9] 이동인, 삼성페이 글로벌 진격…美서 해외송금 서비스, 매경 미디어 그룹, 2019. 10.

[10] 이데일리, [톡톡!금융] 15조 해외송금 잡아라‥뜨거운 각축전, 2020. 1.

[11] 글로벌경제신문, 세계은행 송금 수수료 보고서 (2014년)-각 나라별 및 송금 방식별 조사, 2014. 9.

[12] The Financial Action Task Force-Groupe d'action financiere(FATF-GAFI), FATF Members and Observers, 2020. 4.

[13] Heung Youl Youm, Mee Yeon Kim, and Skylar Hurwitz, "Technical Specification FG DLT D1.1 Distributed ledger technology terms and definitions," ITU-T Focus Group on Application of Distributed Ledger Technology(FG DLT), 2019. 8.

[14] 개인정보보호위원회, "EU GDPR(General Data Protection Regulation) 번역본", 2018. 11.

[15] 행정안전부, "「개인정보 보호법」," 개인정보보호정책과, 2020. 2.

[16] 코인리더스, "FBI '암호화폐, 국가 보안에 위협적'...테러에 악용 가능성 경고 잇따라", 2019. 11.

[17] Etherscan, Etherscan, Transactions, 2020. 4.

[18] CoolbitX, Signa Bridge, 2020. 5.