정 보 보 호 학 회 지
제28권 제4호, 2018. 8

자금세탁 방지를 위한 디지털 자산 거래 시스템 개선 방안

박 근 덕*, 염 흥 열**

요 약

최근 국내외적으로 암호화폐 거래소(이하 '디지털 자산 거래소')를 대상으로 빈번히 발생하고 있는 암호화폐(이하 '디지털 자산') 탈취, 무단 입출금 등 보안 사고를 통하여 자금세탁 및 테러자금조성 등 사회적인 문제를 일으키는 불법 행위가 증가할 가능성이 높다. 본 논문에서는 국제 표준화 기구에서 다루고 있는 디지털 자산 거래소 보안에 관한 표준안, 국내외 법·규정 등을 분석하고 디지털 자산 거래 과정에서 발생할 수 있는 잠재적인 보안 위협을 식별함으로서 자금세탁 및 테러자금조성 방지를 위한 디지털 자산 거래 시스템의 개선 방안을 제시한다.

Ⅰ. 서 론

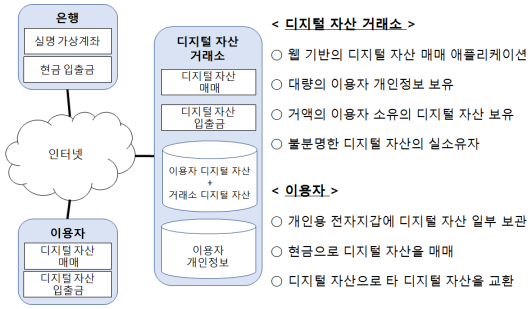
최근 블록체인 및 암호화폐 기술이 급속히 발전함에 따라 2018년 7월 현재, 전 세계적으로 영업 중인 디지털 자산 거래소(예: 비트플라이어, 바이낸스, 빗썸 등)는 약 130개이고 해당 거래소에 등록되어 거래되는 디지털 자산의 종류(예: 비트코인, 이더리움, 리플 등)는 약 1,600종으로 24시간 거래 규모는 약 10조원으로 추정되고 있다.[9] 개인 이용자는 디지털 자산 거래소를 통하여 법정화폐(예: 원화 등)로 디지털 자산을 매매할 수 있고 또한 디지털 자산(예: 비트코인 등)으로 타 디지털 자산(예: 리플 등)으로 교환할 수도 있다. 그러나 최근에 이러한 디지털 자산 거래소를 대상으로 하는 해킹 공격이 급증하여 디지털 자산 도난 등 보안 사고가 끊임없이 발생하고 있고 이로 인해 개인 이용자의 경제적인 손실이 크게 증가하고 있다.[10] 또한 해킹으로 도난당한 디지털 자산은 블록체인의 거래 익명성을 악용하여 자금세탁 및 테러자금조성 목적으로 활용될 가능성이 높다.[11] 따라서 본 논문에서는 디지털 자산 거래소 보안에 관한 국제 표준안, 국내외 자금세탁 방지 관련 법·규정 등을 분석하고 디지털 자산 거래 과정에서 발생할 수 있는 잠재적인 보안 위협을 식별함으로서 자금세탁 및 테러자금조성 방지를 위한 디지털 자산 거래 시스템의 개선 방안을 제시한다.

Ⅱ. 관련 연구

본 장에서는 디지털 자산 거래 시스템 운영 현황 및 사고 현황, 디지털 자산 거래소 보안 관련 국제 표준안, 국내외 자금세탁 방지 관련 법·규정, 정보보호관리체계(ISMS)의 보호 대책을 설명한다.

2.1. 디지털 자산 거래 시스템 운영 현황

디지털 자산 거래 시스템은 통상적으로 은행, 이용자, 디지털 자산 거래소 등으로 구성되어 있다. [그림 1]에서 보는 바와 같이 은행은 이용자의 현금 입출금을 위한 실명제 가상 계좌를 제공하고, 이용자는 디지털 자산 거래소에서 제공하는 디지털 자산 매매 애플리케이션을 통하여 디지털 자산 매매, 교환 및 입출금 등을 실행한다.



〔그림 1〕 디지털 자산 거래 시스템 운영 현황

* 서울외국어대학원대학교 AI블록체인연구소 (jacepark926@gmail.com)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

[그림 1]에서 보는 바와 같이 디지털 자산 거래소는 이용자의 접근성과 편리성을 위하여 인터넷에 개방된 웹기반의 디지털 자산 매매 애플리케이션을 운영함으로서 대량의 이용자 개인 정보와 거액의 디지털 자산을 보유하고 있으나, 해당 디지털 자산의 소유자가 불분명한 실정이다.

2.2. 디지털 자산 거래소 사고 현황

최근 3년간 국내 디지털 자산 거래소에 모두 7건의 해킹사건이 발생해 총 1288억 원 상당의 디지털 자산(암호화폐)이 부정인출 되었다.[12]

과기정통부와 한국인터넷진흥원은 2017년 9월부터 12월까지 10개사, 2018년 1월부터 3월까지는 21개사('17년 기 점검 디지털 자산 거래소 7개 포함, 3개소는 폐업)의 보안 점검을 실시한 바, ▲방화벽 등 정보보호시스템 구축 미흡(14개社) ▲시스템 접근 통제 미흡(19개社) ▲악성코드 예방 미흡(9개社) ▲침해사고 대응 절차 및 지침 미흡(16개社) ▲비밀번호 보안 관리 미흡(10개社) ▲가상통화 지갑관리 미흡(23개社) ▲이상 징후 모니터링 수행 미흡(20개社) 등 상당수의 업체가 취약점이 있는 것으로 드러났다. 이 가운데 전년도에 이어 올해도 주요 점검 항목에서 취약점이 발견된 업소는 7개에 달했다.[12]

〔표 1〕 디지털 자산 거래소 사고 사례〔12〕

연번	발생 일시	피해 내역
1	16.07.26	- R사, 3억원 상당의 가상통화 부정인출
2	17.04.22	- Y사, 55억원 상당의 가상통화 부정인출
3	17.06.28	- B사, 70억원 상당의 가상통화 부정인출 - B사, 약 3.6만여 건 개인정보 유출
4	17.09.23	- C사, 21억원 상당의 가상통화 부정인출
5	17.12.19	- YB사, 259억원 상당의 가상통화 부정인출
6	18.06.10	- CR사, 540억원 상당의 가상통화 부정인출
7	18.06.19	- B사, 350억원 상당의 가상통화 부정인출

2.3. 디지털 자산 거래소 보안 관련 국제 표준안

2018년 5월에 영국 런던에서 개최된 제3회 ISO/TC 307 (Blockchain and distributed ledger technologies) 국제 표준화 회의에서 일본에서 제안한 신규 워크 아이템인 '디지털 자산 거래소 보안 (ISO/NP TR 23576 Security of Digital Asset Custodians)'이 기술 보고서(TR, Technical Report) 수준의 표준안으로 개발할 것을 결의하였다.[2] 본 신규 워크 아이템이 채택된 배경에는 디지털 자산 거래소에서 현금(법정화폐)으로 디지털 자산 매매가 가능함에 따라 해킹에 의한 디지털 자산 도난 등 보안 사고가 증가하고 있는 현시점에서 거래소 보안을 강화할 필요성에 대하여 회원 국가들이 합의를 이루었기 때문이다. 본 신규 표준안의 제목(Title), 범위(Scope), 구조(Table of contents)는 다음과 같다.

(1) 제목(Title)[1]

블록체인 및 분산원장기술 -- 디지털 자산 거래소 보안 (Blockchain and distributed ledger technologies - Security of Digital Asset Custodians)

(2) 범위(Scope)[1]

본 기술 보고서는 시스템 모델, 보안 관리, 디지털 자산 생명주기 관리, 보안 목표와 통제 등을 포함하는 디지털 자산 거래소를 위한 보안 실무를 설명한다.

(3) 구조(Table of contents)[1]

○ 범위(Scope)
○ 용어 정의
○ 디지털 자산 거래 시스템
  - 시스템 모델
  - 처리 과정
  - 시스템 내 암호키
  - 블록체인 및 암호화폐에 대한 보안 고려 사항
○ 보안 관리
○ 디지털 자산 생명주기 관리
○ 보안 목표 및 통제
○ 참고문헌

따라서 본 표준안이 개발되는 과정에서 한국은 자금세탁 및 테러 자금 조성 방지 등과 관련된 국내 법·규정(2.4절 참조)이 표준안에 반영될 수 있도록 적극적인 대응이 필요하다.

2.4. 자금 세탁 방지 관련 국내외 법·규정

본 절에서는 자금세탁 및 테러자금조성 방지를 위한 국내 법·규정과 유럽연합의 자금세탁방지 지침을 분석한다.

(1) 특정 금융거래법 일부개정안

2018년 3월에 더불어민주당 제윤경 의원 등 10인이 발의한 『특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안』(의안번호 : 12592)은 2018년 7월 현재 국회의 소관 위원회에서 처리 중에 있다. 본 법안의 제안 이유는 디지털 자산 거래소(가상통화취급업소)에 대해서도 자금세탁행위 및 공중협박자금조달행위의 효율적 방지를 위한 의무를 부과하고, 금융회사가 디지털 자산 거래소와 금융거래를 수행할 때 준수할 사항을 규정하기 위한 것이다. 본 법안의 주요 내용은 다음과 같다.[5]

가. (안 제2조제1호·제2호) 가상통화 취급업소를 정의('금융회사등'에 포함)하고, 가상통화 취급업소가 보관, 관리, 알선 등을 위해 가상통화를 금융자산과 교환하는 거래 등을 의무부과 대상거래('금융거래등'에 포함)로 규정함
나. (안 제5조제2항) 금융회사등이 자금세탁행위 및 공중협박자금조달 행위를 방지하기 위하여 내부의 절차 및 업무지침에 반영·운용해야 할 사항을 규정함
다. (안 제6조) 가상통화 취급업소와 금융거래를 하는 금융회사등은 가상통화 취급업소의 신고의무(안 제10조) 이행 여부 등을 추가적으로 확인하도록 함
라. (안 제8조) 금융회사등은 의심거래보고, 고액현금거래보고, 고객확인 등 의무 이행과 관련한 금융거래 자료 및 정보를 5년간 보존하도록 규정함
마. (안 제10조 및 제11조)가상통화 취급업소에 대해서 금융정보분석원의 장에게 상호 및 대표자의 성명 등을 신고하도록 하는 한편, 이용자별 거래내역 분리 등 자금세탁행위 및 공중협박자금조달행위를 방지하기 위하여 이행해야하는 조치를 규정함
바. (안 제24조제1항·제2항) 금융회사등에 대하여 부과할 수 있는 과태료의 한도를 1억원으로 상향하는 한편, 과태료 부과사유로 금융회사등이 이행해야 할 조치 의무(안 제5조) 위반, 자료보관의무(안 제8조) 위반 등을 추가함

(2) 가상통화 관련 자금세탁방지 가이드라인

2018년 1월에 금융위원회는 가상통화 취급업소(디지털 자산 거래소)를 통한 자금세탁 및 테러자금조성을 방지하기 위하여 금융회사(은행)를 대상으로 『가상통화 관련 자금세탁방지 가이드라인』을 시행하였다. 본 가이드라인의 주요 내용은 다음과 같다.[6]

제1절 총 칙

□ (정의)
○ (가상통화) 거래상대방으로 하여금 교환의 매개 또는 가치의 저장 수단으로 인식되도록 하는 것으로서 전자적 방법으로 이전 가능한 증표 또는 그 증표에 관한 정보. 다만, 다음 각 호의 것은 이를 제외함
1. 화폐·재화·용역 등으로 교환될 수 없는 전자적 증표 또는 그 증표에 관한 정보로서 발행인이 사용처와 그 용도를 제한한 것
2. 상품권
3. 「게임산업진흥에 관한 법률」 제32조제1항제7호에 따른 게임물의 이용을 통하여 획득한 유·무형의 결과물
4. 「전자금융거래법」 제2조제14호에 따른 선불전자지급수단 및 같은 법 제2조제15호에 따른 전자화폐
○ (가상통화 취급업소) 가상통화를 보관·관리·교환·매매·알선 또는 중개하는 것을 업으로 하는 자(이하 '취급업소')
□ (적용대상) 이 가이드라인은 금융회사등을 대상으로 함
○ 이 가이드라인은 금융회사등이 가상통화와 관련한 금융거래를 수행하는 경우 적용되는 사항을 규정
..중략..
제2절 취급업소에 대한 확인사항 등
나. 금융회사등이 금융회사등의 고객을 취급업소로 인식한 경우
1 (고객확인 강화) 금융회사등은 취급업소를 자금세탁등의 위험이 높은 고객으로 고려*하여 취급업소에 대해 업무규정이 열거한 추가적 확인사항(업무규정 제42조제2항·제3항)과 다음 각 호의 정보를 확인
1. 취급업소가 제공하는 서비스의 내용
2. 취급업소의 실명확인 입출금계정서비스 이용여부 및 이용계획
3. 취급업소가 이용자의 생년월일, 주소, 연락처 등을 포함한 신원사항 확인 여부
4. 취급업소가 취급업소의 고유재산과 이용자의 예탁·거래금을 분리하여 관리하고 있는지 여부
5. 취급업소가 이용자별 거래내역을 구분하여 관리하고 있는지 여부
6. 취급업소가 이용자를 상대로 가상통화는 법정 화폐가 아니라는 사실과 가상통화의 내용, 매매 및 그 밖의 거래에 따르는 위험 등을 이용자가 이해할 수 있도록 설명하고 그 의사를 확인하는지 여부
7. 취급업소가 가상통화거래 관련 집금을 위해 임직원 계좌 등 별도의 계좌를 운용하는지 여부
8. 대한민국 정부에서 발표하는 가상통화와 관련한

정책의 준수 여부
9. 기타 금융회사등이 자금세탁등의 방지를 위해 필요하다고 인정하는 사항
○ 추가적인 정보의 확인은 취급업소의 사무소, 영업점 등에 방문하여 현지실사 방법으로 실시
② (취급업소가 법인·단체 또는 개인의 계좌*를 통해 가상통화관련 금융거래를 하는 경우) 금융회사등은 자금세탁등을 효과적으로 방지하기위하여 다음 각 호의 사항을 이행
1. 취급업소의 임직원 계좌가 가상통화관련 금융거래에 활용되는 것으로 의심되는 경우 임직원 명의 계좌에 대한 강화된 고객확인 및 금융거래모니터링 강화(나①에 따른 사항 포함)
2. 금융회사등의 고객 중 민법상 미성년자, 외국인 등의 가상통화관련 금융거래를 식별
3. 금융회사등은 취급업소 이용자의 금융거래내역 관리를 대행하거나 실시간 관리가 가능하도록 하는 등 취급업소의 가상통화관련 금융거래내역 관리에 편의성을 제공하는 용역 행위를 자제
4. 기타 금융회사등에서 자금세탁등의 방지를 위해 필요하다고 인정되는 사항
③ (고객에 대한 지속적 확인) 금융회사등은 취급업소를 자금세탁등의 위험이 높은 고객으로 고려하여 6개월 이하의 주기마다 지속적으로 확인
○ 취급업소가 실명확인 입출금계정서비스를 이용하지 않는 등 특별한 주의를 요하는 경우 3개월 이하의 주기마다 지속적으로 확인

제5절 거래의 거절 등

① 금융회사등은 다음과 같은 경우에는 특별한 사유가 없는 한 금융거래를 거절하거나 해당 금융거래를 종료
1. 금융회사등의 고객이 신원확인 등을 위한 정보 제공을 거부하여 금융회사등이 고객확인을 할 수 없는 경우
2. 금융회사등의 고객이 취급업소인 것으로 의심되는 경우로서 고객이 확인을 위해 제공한 정보를 신뢰할 수 없어 사실상 정보 제공을 거부한 것과 동일시할 수 있는 경우
② 금융회사등은 다음과 같은 경우에는 금융거래를 거절할 수 있음
1. 금융회사등의 고객이 취급업소인 경우로서 실명확인 입출금계정 서비스를 이용하지 않는 등 자금세탁등의 위험이 특별히 높다고 판단하는 경우
③ 금융거래 거절 및 종료의 경우 금융정보분석원에 의심거래로 보고

금융회사(은행)는 본 가이드라인을 준수하여 자금세탁방지 체계가 미흡한 디지털 자산 거래소에게는 신규 계좌 개설 등의 거래를 거절하고 있는 실정이다.

(3) 유럽연합의 자금세탁방지 지침 개정안

2018년 5월에 유럽연합에서는 자금세탁 및 테러자금 조성을 방지하기 위하여 자금세탁방지 지침의 5번째 개정안(『DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU』)을 발표하였고 2018년 7월에 이를 시행하였다. 본 지침의 주요 내용은 다음과 같다.[3]

(1) 목적[3]

○ 금융 기술과 관련된 익명성 문제 해결
○ 암호 자산(디지털 자산)을 통한 자금세탁 방지
○ 테러자금조성 및 탈세 방지 등

(2) 적용 대상[3]

○ 암호 자산(디지털 자산) 거래소
○ 전자지갑 제공자 등

(3) 주요 내용[3]

○ 불투명한 구조에 의한 자금세탁 및 테러자금조성을 방지하기 위한 실제 소유자의 투명성 제고
○ 중앙은행 계좌 등록에 의한 정보에 대한 접근성 향상으로 통하여 금융정보국(FIU, Financial Intelligence Units)의 업무 개선
○ 가상 화폐(Virtual Currencies) 및 선불 도구의 익명 이용과 관련된 테러자금조성 위험에 대처
○ 자금세탁 방지 감독자와 유럽 중앙은행 간의 정보 교환 및 협력 증진
○ 자금세탁 및 테러자금조성 관련 고위험 수준의 국가를 평가하기 위한 기준을 확대하고 그러한 국가의 금융 흐름에 대한 공통의 높은 수준의 안전장치를 확보 등

유럽연합의 각 회원국은 2020년 1월까지 본 지침의 개정된 내용을 자국의 국내법에 반영하여 이행할 예정이다.[4]

2.5. 정보보호관리체계의 보호 대책

본 절에서는『정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 근거하여 운영하고 있는 인증 제도인 정보보호관리체계(ISMS, Information Security Management System)의 인증기준을 분석하여 자금세탁 방지를 위한 디지털 자산 거래소에 우선적으로 적용할 수 있는 보호대책을 제시한다.

(1) 보호대책 9.1.1 암호정책 수립[7]

조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.

(2) 보호대책 9.2.1 암호키 생성 및 이용[7]

암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.

(3) 보호대책 10.3.1 사용자 인증[7]

정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고. 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.

(4) 보호대책 10.3.2 사용자 식별[7]

정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.

(5) 보호대책 10.4.1 네트워크 접근[7]

네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.

(6) 보호대책 11.5.1 악성코드 통제[7]

바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.

(7) 보호대책 11.6.2 로그기록 및 보존[7]

정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.

(8) 보호대책 11.6.3 접근 및 사용 모니터링[7]

중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.

Ⅲ. 디지털 자산 거래 시 보안 위협

본 장에서는 디지털 자산 거래소를 통하여 디지털 자산 거래 시 발생할 수 있는 잠재적인 보안 위협을 식별한다. 다만, 일반적인 IT 서비스에서 보편적으로 발생할 수 있는 보안 위협은 다루지 않는다.

3.1. 디지털 자산 도난

외부의 해킹(예: APT공격, 피싱 등)에 의하여 디지털 자산 거래소에 보관되어 있는 디지털 자산을 도난당할 수 있다. 디지털 자산의 거래 내역이 기록된 블록체인의 불가역성 등과 같은 특성 때문에 한 번 도난당한 디지털 자산을 되찾아오기는 매우 어렵다.

3.2. 디지털 자산 무단 입출금

디지털 자산 거래소 내부자의 의하여 이용자(고객) 소유의 디지털 자산에 대한 무단 입출금이 발생할 수 있다. 디지털 자산 거래소는 자신의 이익을 극대화하기 위한 목적으로 이용자 소유의 디지털 자산을 활용하여 불법 행위

(예: 시세조정, 폰지, 돌려막기 등)에 필요한 디지털 자산을 조달할 수 있다.

3.3. 디지털 자산 소유자 익명성

디지털 자산 거래소는 자신 소유의 디지털 자산과 이용자(고객) 소유의 디지털 자산을 별도로 분리(예: 이용자별 전자지갑 등)하여 보관하지 않기 때문에 해당 디지털 자산의 소유자가 누구인지 불분명하다.

3.4. 디지털 자산 거래 원장 위·변조

디지털 자산 거래소는 자신 또는 이용자(고객) 소유의 디지털 자산 거래(예: 매매, 교환 등) 내역을 위·변조할 수 있다. 이것은 중앙화된 데이터베이스에 저장된 거래 원장을 위·변조하여 '디지털 자산 무단 입출금'에 대한 증적을 훼손하려는 의도일 수 있다.

3.5. 암호키 유출

디지털 자산 거래소는 디지털 자산을 안전하게 보관하기 위하여 해당 자산을 암호화 할 때 사용한 암호키를 외부에 유출할 수 있다. 이러한 암호키 유출은 디지털 자산 도난 및 무단 입출금 등에 악용될 것이다.

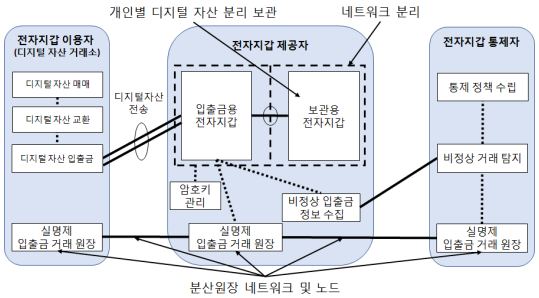
상기에서 설명한 보안 위협으로 인하여 발생한 보안사고는 디지털 자산을 통한 자금세탁 및 테러자금조성을 가능하게 한다.

Ⅳ. 디지털 자산 거래 시스템 개선 방안

본 장에서는 제3장에서 식별한 디지털 자산 거래시 보안 위협에 대응할 수 있는 디지털 자산 거래 시스템의 개선 방안으로서 분산원장기술 기반의 전자지갑 서비스 모델과 보안 요구사항을 설명한다.

4.1. 분산원장기술 기반의 전자지갑 서비스 모델

분산원장기술 기반의 전자지갑 서비스 모델은 전자지갑 이용자(예: 디지털 자산 거래소 등), 전자지갑 제공자, 전자지갑 통제자로 구성된다. 또한 전자지갑 이용자, 전자지갑 제공자, 전자지갑 통제자는 완전히 독립된 기관으로서 상호 이해관계(예: 임원 겸직, 상호 출자 등)가 없어야 한다.



〔그림 2〕 분산원장기술 기반의 전자지갑 서비스 모델

[그림 2]에서 보는 바와 같이 전자지갑 이용자(예: 디지털 자산 거래소), 전자지갑 제공자, 전자지갑 통제자의 역할은 다음과 같다.

(1) 전자지갑 이용자(디지털 자산 거래소)

○ 전자지갑 이용자(디지털 자산 거래소)는 인터넷을 통하여 응용 프로그램을 디지털 자산 거래 이용자(이하 '고객')에게 제공한다.
○ 전자지갑 이용자(디지털 자산 거래소)는 고객에게 디지털 자산 매매(법정화폐로 디지털 자산을 매매) 및 교환(디지털 자산(예: 비트코인 등)을 타 디지털 자산(예: 리플 등)으로 교환) 서비스를 제공한다.
○ 전자지갑 이용자(디지털 자산 거래소)는 고객에게 법정화폐 및 디지털 자산 입출금 서비스를 제공하되, 전자지갑 제공자에게 디지털 자산 입출금을 요청한다.
○ 전자지갑 이용자(디지털 자산 거래소)는 고객의 개인정보를 보관 및 관리한다.
○ 전자지갑 이용자(디지털 자산 거래소)는 고객의 디지털 자산을 별도 보관하지 않는다.
○ 전자지갑 이용자(디지털 자산 거래소)는 분산원장 네트워크 기반의 노드를 운영하여 실명제 입출금 거래 원장을 관리한다.

(2) 전자지갑 제공자

○ 전자지갑 제공자는 물리적 또는 논리적으로 네트워크를 분리하여 '입출금용 전자지갑'과 '보관용 전자지갑'을 별도 운영한다.

○ 전자지갑 제공자는 전자지갑 이용자(디지털 자산 거래소)의 요청에 의한 디지털 자산 입출금시 '입출금용 전자지갑'을 통하여 처리하되, '입출금용 전자지갑'에는 디지털 자산을 보관하지 않는다.
○ 전자지갑 제공자는 '보관용 전자지갑'에 고객별 전자지갑을 각각 생성하여 디지털 자산을 암호화하여 보관한다.
○ 전자지갑 제공자는 분산원장 네트워크 기반의 노드를 운영하여 디지털 자산 입출금시 송금인 및 수취인의 신원을 확인하고 해당 거래 내역을 실명제 입출금 거래 원장에 기록하여 관리(합의·저장·공유·보관·동기화)한다.
○ 전자지갑 제공자는 디지털 자산 등을 암·복호화 하기 위한 암호키를 관리(생성·이용·보관·배포·복구·파기)하고, 생성·이용·보관·배포·복구·파기에 관한 이력을 기록 및 보관한다.
○ 전자지갑 제공자는 디지털 자산 입출금시 비정상적인 입출금 정보를 수집하고 이를 전자지갑 통제자에게 제공하여 비정상거래를 탐지 및 모니터링 한다.

(3) 전자지갑 통제자

○ 전자지갑 통제자는 통제 정책(예: 보안 정책, 비정상 거래 탐지 정책 등)을 수립하여 전자지갑 제공자에게 이행하도록 한다.
○ 전자지갑 통제자는 전자지갑 제공자의 통제 정책 이행 여부를 관리 및 감독한다.
○ 전자지갑 통제자는 디지털 자산 입출금시 비정상적인 거래를 탐지하여 후속조치를 취한다.
○ 전자지갑 통제자는 분산원장 네트워크 기반의 노드를 운영하여 실명제 입출금 거래 원장을 관리한다.

4.2. 보안 요구사항

본 절에서는 4.1절에서 제시한 분산원장기술 기반의 전자지갑 서비스 모델에 대한 보안 요구사항은 이용자 식별 및 인증, 네트워크 분리, 악성코드 통제, 데이터 암호화, 데이터 무결성, 암호키 생성 및 이용, 로그 기록 및 보존, 비정상 거래 탐지 시스템 운영으로 분류하여 설명한다.

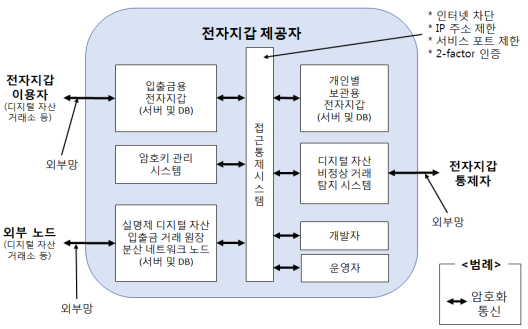
(1) 이용자 식별 및 인증

전자지갑 제공자는 디지털 자산 거래 이용자(소유자)를 유일하게 식별하고 인증할 필요가 있다. 이용자 인증 시 비대면 인증 수단(예: 생체 인증, PKI 기반 인증서 등)을 사용할 수 있다. (2.5절 (3), (4) 참조)

(2) 네트워크 분리

전자지갑 제공자는 중요 정보(예: 암호키, 디지털 자산 등) 유출 및 악성코드 감염을 통제하기 위하여 물리적 또는 논리적으로 네트워크를 분리할 필요가 있다. (2.5절 (5) 참조)

[그림 3]에서 보는 바와 같이 전자지갑 제공자는 입출금용 전자지갑, 개인별 보관용 전자지갑, 암호키 관리 시스템, 디지털 자산 비정상 거래 탐지 시스템, 실명제 디지털 자산 입출금 거래 원장 분산 네트워크 노드, 개발자, 운영자 등을 물리적 또는 논리적으로 네트워크를 분리하고 접근통제시스템(예: 방화벽, 네트워크접근통제, 서버 접근통제, DB접근통제 등)을 통하여 비인가된 접근을 차단한다.



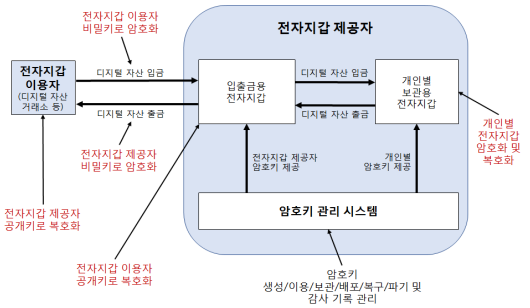
〔그림 3〕 네트워크 분리 예시

(3) 악성코드 통제

전자지갑 제공자는 악성코드(예: APT, 랜섬웨어 등) 감염에 의하여 중요 정보(예: 디지털 자산, 암호키, 디지털 자산 입출금 거래 원장 등)가 위·변조(삭제 포함) 및 유출되지 않도록 보호 대책을 수립하고 이행할 필요가 있다. (2.5절 (6) 참조)

(4) 데이터 암호화

전자지갑 제공자는 [그림 4]의 '개인별 보관용 전자지갑'에 디지털 자산을 저장시 안전한 암호 알고리즘(예: SEED, AES-128 이상)으로 암호화할 필요가 있다.[8] 또한 전자지갑 이용자(디지털 자산 거래소)와 전자지갑 제공자, 전자지갑 통제자 간의 중요 정보 전송시 전송 구간 암호화(예: TLS, 암호 모듈 등)를 적용할 필요가 있다. (2.5절 (1) 참조))



〔그림 4〕 암호키 관리 예시

(5) 데이터 무결성

전자지갑 제공자는 디지털 자산 입출금 거래 내역의 위·변조를 방지할 필요가 있다. 분산원장 네트워크의 보안 특성 상 한번 기록된 디지털 자산 입출금 거래 원장을 위·변조하는 것은 매우 어렵다. 이를 위하여 [그림 5]에서 보는 바와 같이 분산원장 네트워크 기반의 노드를 운영하여 디지털 자산 입출금시 송금인 및 수취인의 신원을 확인하고 해당 거래 내역을 실명제 입출금 거래 원장에 기록하여 관리(합의·저장·공유·보관·동기화)할 수 있다. (2.5절 (1) 참조))

(6) 암호키 생성 및 이용

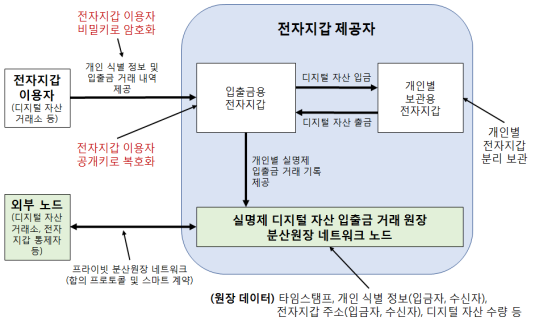
전자지갑 제공자는 디지털 자산 등을 암·복호화 하기 위한 암호키를 관리(생성·이용·보관·배포·복구·파기)하고, 생성·이용·보관·배포·복구·파기에 관한 이력을 기록 및 보관할 필요가 있다. (2.5절 (2) 참조))

[그림 3]에서 보는 바와 같이 전자지갑 제공자는 개인(디지털 자산 소유자)별 암호키를 제공하여 개인별 전자지갑을 암·복호화하고, 전자지갑 이용자(디지털 자산 거래소)와 중요 정보 교환 시 PKI 기반 비대칭 암호키로 암·복호화 한다.

(7) 로그 기록 및 보존

전자지갑 제공자는 디지털 자산 입출금 거래 내역을 기록하고 일정기간 동안 보존할 필요가 있다. (2.5절 (7) 참조))

[그림 5]에서 보는 바와 같이 전자지갑 제공자는 실명제 디지털 자산 입출금 거래 원장을 기록 및 관리할 수 있는 분산원장 네트워크 및 노드를 운용한다. 분산원장 네트워크에 참여하는 노드는 전자지갑 이용자(디지털 자산 거래소), 전자지갑 제공자, 전자지갑 통제자가 운영하는 정보시스템(서버, 데이터베이스 등) 이다. 원장 데이터는 타임스탬프, 개인 식별 정보(송금인, 수취인), 전자지갑 주소(송금인, 수취인), 디지털 자산 수량 등을 포함할 수 있다.

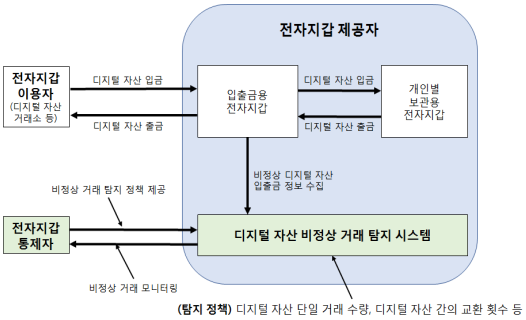


〔그림 5〕 분산원장 네트워크 기반의 디지털 자산 입출금 거래 원장 관리 예시

(8) 비정상 거래 탐지 시스템 운영

전자지갑 제공자는 디지털 자산 입출금시 비정상적인 입출금 정보를 수집하고 이를 전자지갑 통제자에게 제공하여 비정상거래를 탐지 및 모니터링 할 필요가 있다. (2.5절 (8) 참조))

[그림 6]에서 보는 바와 같이 전자지갑 제공자는 전자지갑 통제자로부터 제공받은 비정상 거래 탐지 정책(예: 디지털 자산 단일 거래 수량, 디지털 자산 간의 교환 횟수 등)을 적용하여 디지털 자산 입출금시 비정상적인 거래를 탐지한다.



〔그림 6〕 비정상 거래 탐지 시스템 예시

4.3. 보안 위협과 보안 요구사항의 대응 관계

본 절에서는 제3장에서 식별한 디지털 자산 거래 시 보안 위협과 4.2절에서 제시한 분산원장기술 기반의 전자지갑 서비스 모델에 대한 보안 요구사항 간의 대응 관계를 설명한다.

[표 2]에서 보는 바와 같이 이용자 식별 및 인증은 디지털 자산 무단 입출금, 디지털 자산 소유자 익명성과 대응한다. 네트워크 분리는 디지털 자산 도난, 디지털 자산 무단 입출금, 암호키 유출과 대응한다. 악성코드 통제는 디지털 자산 도난, 디지털 자산 거래 원장 위·변조, 암호키 유출과 대응한다. 데이터 암호화는 디지털 자산 도난, 디지털 자산 무단 입출금, 디지털 자산 거래 원장 위·변조와 대응한다. 데이터 무결성은 디지털 자산 거래 원장 위·변조와 대응한다. 암호키 생성 및 이용은 디지털 자산 도난, 디지털 자산 무단 입출금, 암호키 유출과 대응한다. 로그 기록 및 보존은 디지털 자산 소유자 익명성, 디지털 자산 거래 원장 위·변조와 대응한다. 비정상 거래 탐지 시스템 운영은 디지털 자산 도난, 디지털 자산 무단 입출금, 디지털 자산 소유자 익명성과 대응한다. 따라서 분산원장 기술 기반의 전자지갑 서비스 모델 보안 요구사항이 디지털 자산 거래 시 보안 위협에 적절히 대응할 수 있음을 확인할 수 있다.

〔표 2〕 보안 위협과 보안 요구사항의 대응 관계

보안 위협 / 보안 요구사항	디지털 자산 도난	디지털 자산 무단 입출금	디지털 자산 소유자 익명성	디지털 자산 거래 원장 위변조	암호키 유출
이용자 식별 및 인증	-	○	○	-	-
네트워크 분리	○	○	-	-	○
악성코드 통제	○	-	-	○	○
데이터 암호화	○	○	-	○	-
데이터 무결성	-	-	-	○	-
암호키 생성 및 이용	○	○	-	-	○
로그 기록 및 보존	-	-	○	○	-
비정상 거래 탐지 시스템 운영	○	○	○	-	-

Ⅴ. 결 론

디지털 자산 거래소에서 법정화폐(예: 원화 등)로 디지털 자산(예: 비트코인 등)을 매매하거나 디지털 자산(예: 비트코인 등)으로 타 디지털 자산(예: 리플 등)을 교환하는 과정에서 자금세탁 행위가 발생할 수 있고, 외부의 해킹으로 인하여 도난당한 디지털 자산을 통하여 테러자금이 조성될 가능성이 높다. 이러한 문제는 디지털 자산을 유통하는 블록체인의 익명성을 악용한 것으로서 디지털 자산 거래 시 실명제를 바탕으로 위·변조가 어려운 분산원장기술을 활용하여 거래 원장을 관리할 필요가 있다. 또한 개인정보와 디지털 자산이 한 곳에 집중화 되어 있을 뿐만 아니라 서비스 특성 상 인터넷에 오픈되어 있는 디지털 자산 거래소는 해킹의 주요 대상이 되므로 디지털 자산 보관소 역할을 수행할 수 있는 제3의 기관에 디지털 자산을 안전하게 분리·보관하는 것이 시급하다. 이를 위하여 본 논문에서는 디지털 자산 거래 시 발생할 수 있는 보안 위협을 식별하였고, 디지털 자산 보관소 역할을 수행할 수 있는 '분산원장기술 기반의 전자지갑 서비스 모델'을 제시하고 식별된 보안 위협에 대응 할 수 있는 보안 요구사항을 도출함으로서 자금세탁 및 테러자금조성 방지를 위한 디지털 자산 거래 시스템의 개선 방안을 제안하였다. 향 후 ITU-T SG17, ISO/TC 307 등 국제 표준화 활동 시 본 논문의 내용을 적극 반영하고자 한다.

참 고 문 헌

[1] ISO/TC 307/WG 2 (Security, privacy and Identity), "Blockchain and distributed ledger technologies -- Security of Digital Asset Custodians", May 2018

[2] ISO/TC 307 (Blockchain and distributed ledger technologies), "ISO/TC 307 N300, ISO TC 307 -

Meeting 03 Resolutions - London - May 2018", May 2018

[3] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, "DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU", May 2018

[4] European Commission, "Strengthened EU rules to prevent money laundering and terrorism financing", Jul. 2018

[5] 더불어민주당 제윤경 의원 등 10인, "『특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안』(의안번호 : 12592)", 2018년 3월

[6] 금융위원회, "『가상통화 관련 자금세탁방지 가이드라인』", 2018년 1월

[7] 한국인터넷진흥원, "정보보호관리체계(ISMS) 인증기준 세부점검항목", 2013년 5월

[8] 한국인터넷진흥원, "암호 알고리즘 및 키 길이 이용 안내서", 2013년 1월

[9] Internet Homepage of Coinhills, "https://www.coinhills.com/ko/market/exchange", Jul. 2018

[10] Internet Homepage of KBS news, "http://news.kbs.co.kr/news/view.do?ncd=4006806&ref=A", Jul. 2018

[11] Internet Homepage of inews24 news, "http://news.inews24.com/php/news_view.php?g_serial=1107325&g_menu=022400&rrf=nv", Jul. 2018

[12] Internet Homepage of edaily news, "http://www.edaily.co.kr/news/news_detail.asp?newsId=01866326619272880&mediaCodeNo=257&OutLnkChk=Y", Jul. 2018

〈저 자 소 개〉

박 근 덕 (Keundug Park)
종신회원

1992년 2월 : 동아대학교 전산공학과 학사
2015년 8월 : 순천향대학교 대학원 정보보호학과 석사
2018년 2월 : 순천향대학교 대학원 정보보호학과 박사
1997년 10월~2010년 9월 : (주)센타비전 CTO
2018년 3월~현재 : 서울외국어대학원대학교 AI블록체인연구소 부소장/교수
2015년 1월~현재 : ITU-T SG17 전문위원/에디터
2017년 8월~현재 : ISO/TC 307 전문위원
<관심분야> 블록체인 및 분산원장기술 보안, 클라우드 컴퓨팅 보안, 정보보호관리체계, 개인정보보호

염 흥 열 (Heung Youl Youm)
종신회원

1981년 2월 : 한양대학교 전자공학과 학사
1983년 9월 : 한양대학교 대학원 전자공학과 석사
1990년 2월 : 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구원 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재 : 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2017년~현재 : ITU-T SG17 의장
2016년 5월~현재 : 개인정보보호표준포럼 의장
<관심분야> 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜