Information Systems Review
Vol. 22, No. 4 November 2020 http://dx.doi.org/10.14329/isr.2020.22.4.135

가상통화거래소의 계정 및 자산 보호에 관한 사례연구: 유관기관의 프로세스를 중심으로

A Case Study on the Protection of Accounts and Assets on Cryptocurrency Exchanges: Focusing on the Processes of Related Institutions

이 윤 주 (Yoonjoo Lee) 디어젠 주식회사 사업개발부
이 동 원 (Dongwon Lee) 한성대학교 사회과학부 조교수, 교신저자
한 인 구 (Ingoo Han) KAIST 경영대학 교수

요 약

블록체인과 가상통화 관련 시장의 성장과 함께 가상통화거래소는 하나의 신규 산업으로 성장하고 있다. 그러나, 가상통화에 대한 법·규제적 정의가 진행 중에 있어서 기존 산업과 다르게 규제기관의 관리감독을 받지 않고 있으며, 이에 따라 본 연구는 거래소 해킹 및 사고로 인한 사용자(가상통화 투자자)의 피해가 다수 보고되었다. 가상통화거래소에서 발생할 수 있는 피해를 개인정보 및 계정의 탈취로 인한 자산 피해와 사용자가 외부 사기사건 등에 연루되어 발생할 수 있는 피해로 구분하여 연관성이 높은 기능을 선행 사업자와 비교 분석하였다. 회원가입(KYC: Know Your Client), 로그인, 거래 추가인증은 선행 사업자와 유사한 수준이나, 이상거래탐지(FDS: Fraud Detection System), 법화 및 가상통화 자금세탁방지(AML: Anti-Money Laundering)는 미흡한 수준으로 조속한 개선이 필요할 것으로 파악되었다.

키워드 : 가상통화, 블록체인, 자금 세탁 방지, 이상거래탐지, 보안, 투자자 보호

Ⅰ. 서 론

블록체인을 기반으로 탄생한 가상통화는 복잡한 생태계를 형성하며 다양한 사업자, 사용자, 투자자와 관계를 형성하고 있다. 비트코인(Bitcoin)을 필두로 다양한 신종 코인이 ICO(Initial Coin Offering)를 통해 발행되고 있으며 지속적으로 가상통화 시장을 팽창시키고 있다. 2017년 말 시작된 가상통화에 대한 전 세계적 투자열풍은 현재까지도 약 1,600 종에 이르는 가상통화에 대해 지속되고 있는 상황이다. 이들은 대부분 블록체인 기술을 기반으로 하고 있으며, 서비스와 어플리케이션을 제공하는 플랫폼으로 진화하고 있다(김준상, 2019). 국내에서는 가상통화의 거래가 장기적인 관점에서의 투자로 인식되는 것보다는 단기적인 시세차익을 노리는 투기적인 성격이 강했다는 비판적 시각도 존재한다(김은영, 김병초, 2020; 유상이 등, 2019).

가상통화의 초기 거래는 사용자 개인 간에 P2P를 통해 이루어졌으나, 거래소 상장을 통해 공식적인 가상통화시장이 형성되면서, 국내의 빗썸(Bithumb), 업비트(Upbit) 및 해외의 비트피넥스(Bitfinex), 바이낸스(Binance) 등과 같이 많은 거래소가 중앙화된 형태로 운영되고 있다. 가상통화가 중앙화된 거래소에 상장되고 거래된다는 것은 법화(실물화폐)로의 환전이 가능하게 됨으로써 가상통화가 실질적인 가치를 갖게 됨을 의미한다. 가상통화를 발행하는 사업자와 가상통화에 투자해 수익을 확보하고자 하는 투자자가 가상통화거래소를 중심으로 거래를 하게 됨에 따라, 가상통화거래소의 보안에 대한 중요성이 더욱 강조될 수밖에 없는 상황이 되었다.

전 세계 상위 5위권 가상통화거래소의 1일 평균 거래량은 10억~100억 달러로서, 각 국가별 증권거래소의 거래량을 능가하는 매우 높은 수준에 해당한다. 그럼에도 불구하고, 국내에서는 가상통화와 관련된 법적, 정책적 정의가 명확히 내려지지 않아 가상통화거래소를 전자상거래법상 통신판매업자로 보고 있다.

최근에 가상통화 관련 범죄로 인해 이용자들이 큰 피해를 입는 사건이 빈번이 발생하고 있다. 이미 시장에서 큰 영향력을 행사하는 가상통화거래소는 고객 보호를 위한 최선의 조치를 취하고 이에 맞도록 운영할 책임과 의무를 갖는다. 본 연구는 사례연구를 통해 가상통화거래소의 고객 계정 및 자산 보호와 관련된 주요 기능을 파악하고 선행 유사 사업자와 비교 분석하여 가상통화거래소의 안전성을 제고할 수 있는 방안을 제시하고자 한다.

본 연구에서는 해외 2개(미국의 비트피넥스(Bitfinex), 중국의 바이낸스(Binance))와 국내 2개(업비트(Upbit), 빗썸(Bithumb))의 가상통화거래소를 사례연구의 대상으로 선정하였다. 가상통화거래소와 유사한 기능을 수행하는 기존 사업자로서 카카오뱅크, 구글, 카카오톡 등을 벤치마킹 대상으로 선정하여 가상통화거래소의 기능별 보안수준을 비교분석하고 개선방안을 제시하였다.

주요 기능별로 벤치마킹 대상인 인터넷 은행, 플랫폼 사업자와 비교 분석한 결과, 회원가입, 로그인, 거래 추가인증과 같은 기본적인 프로세스에서는 가상통화거래소들이 기존 사업자에 준하는 수준의 보안통제를 적용하고 있으나, 법화(실물화폐) 및 가상통화에 대한 자금세탁방지(AML), 이상거래탐지(FDS) 측면에서는 매우 미흡한 수준이며 개선이 시급한 것으로 파악되었다.

가상통화거래소의 범죄를 예방하고 고객 및 자산 보호의 수준을 제고함으로써 고객뿐만 아니라 정부 및 기존 금융권으로부터 신뢰를 획득하는 것이, 가상통화의 거래를 활성화하고 향후 관련 사업을 확장하고 추진하는 데에 긍정적 영향을 주는 길일 것이다.

본 연구의 구성은 다음과 같다. 제Ⅱ장에서는 가상통화 관련 범죄 및 거래소의 주요 기능과 역할, 거래소의 문제점과 발전방향을 논의할 것이다. 제Ⅲ장은 사례연구의 대상으로서 대표적인 가상통화거래소를 선정하고 단계별 주요기능을 파악하고 기능별 비교대상인 기존 사업자를 선정할 것이다. 제Ⅳ장에서는 사례연구 대상인 가상화폐 거래소의 주요 기능별 보안 수준을 벤치마킹 사업자와 비교분석하고 시사점을 제시할 것이다. 제Ⅴ장은 연구의 기여와 시사점을 요약하고 한계점 및 미래연구방향을 제시할 것이다.

Ⅱ. 가상통화거래소

2.1 가상통화 관련 범죄 및 대응

가상통화를 이용한 사이버 범죄는, 기존 사이버 범죄에 포함될 수 있으며 금전적 탈취의 대상이 가상통화라는 특징을 갖는다. 그 유형은 가상통화거래소에서 사용되는 고객의 개인정보 또는 ID/PW를 탈취하거나 거래소 내에 보관 중인 자산을 외부로 불법적으로 출금하는 범죄로 나뉠 수 있다. 구체적으로는, 가상통화가 자금세탁(Fanusie

and Robinson, 2018; Möser *et al.*, 2013)이나 불법거래의 대금지불(Christin, 2013; Soska and Christin, 2015) 또는 사기(Vasek and Moore, 2015; Vasek and Moore, 2018)의 수단으로 사용되는 등 다양한 유형의 범죄가 있다.

가상통화를 이용한 범죄의 수사는 기존 실물화폐와는 달리 금융기관 거래를 통한 금융범죄 수사 방법을 적용할 수 없는데, 이는 다음과 같은 가상통화 관련 범죄의 특징 때문이다. 첫째, 가상통화를 보관할 수 있는 지갑은 블록체인 개발 기술을 가진 사람이면 누구나 개발이 가능해서 발행 주체를 통제할 수 없다. 이는 은행 계좌 및 예금 또는 적금 상품과 같이 발행기관의 통제를 기반으로 규제할 수 없음을 의미한다. 둘째, 블록체인 상에 생성되는 지갑에는 개인정보를 제외한 최소한의 거래정보만을 담고 있어 이를 범죄 수사에 활용하는 것이 사실상 불가능하다. 효과적인 수사가 이루어지려면, 가상통화 지갑의 주소를 기준으로 거래 흐름을 파악하고, 개인식별정보를 관리하고 있는 기관을 통해 가상통화가 실물화폐로 환전되는 과정을 추적하는 것이 필요하다.

이와 같은 이유로 범죄가 발생하기 전에 이를 방지할 수 있는 방안이 더욱 중요하다고 할 수 있다. 자금세탁을 방지하기 위한 노력으로서 블랙리스트(Blacklist)를 작성하여 코인의 거래를 제한하도록 하는 방식이 제안된 바 있으며(Abramova *et al.*, 2017; Möser and Narayanan, 2019; Möser *et al.*, 2014; Rueckert, 2019), 거래소의 운영과 관련하여, Mccorry *et al.*(2018)은 핫키(Hot Keys), 콜드키(Cold Keys), 금고키(Vault Keys)의 3개의 키를 사용하여 계약을 체결하고, 핫월렛(Hot Wallet)과 콜드월렛(Cold Walet) 사이에 코인이 이동할 때에 시간을 지연하며, 코인에 대한 탈취행위가 감지되면 금고를 잠그거나 폭파시킬 수 있도록 하는 지연된 환전금고(Time-Delayed Exchange Vaults) 방식을 제안한 바 있다.

이와 같이 가상통화 관련 범죄의 경우 기존과 다른 수사 방법이 적용되어야 하며, 국경의 제한을 받지 않는 가상통화의 특성으로 인해 국제적 공조가 필요한 경우도 자주 발생한다. 또한, 이러한 범죄를 예방하기 위해서는 개별 사례에 적합한 수단을 마련할 수도 있으나, 보다 근본적으로는 가상통화거래소의 운영 프로세스 전반에 걸쳐 보안을 강화하는 방안을 수립하는 것이 중요하다고 할 수 있다. 본 연구에서는 가상통화 관련 범죄의 특수성을 고려하고, 유관기관의 프로세스를 벤치마킹하여 이를 가상통화거래소의 프로세스에 반영하기 위한 목적으로 사례연구를 진행한다.

2.2 가상통화거래소

가상통화거래소는 암호화폐 거래소(Cryptocurrency Exchange) 또는 디지털화폐 거래소(Digital Currency Exchange)라고도 불리며, 사용자들이 비트코인 등 암호화폐나 디지털화폐를 서로 교환할 수 있는 거래소를 의미한다. 현재 국내의 경우 가상통화에 대한 법적 정의가 없으며 가상통화거래소 사업자에 대한 규제 또한 명확하지 않은 상황이다(이관형, 2019). 2014년 이후 가상통화 거래를 시작한 빗썸(Bithumb), 코빗(Korbit), 코인원(Coinone), 업비트(Upbit) 등의 경우 전자상거래법상 통신판매업자로 사업을 영위해왔다. 그러나, 2018년 1월 공정거래위원회가 가상통화거래소는 통신판매업자가 아니라고 판단함에 따라 홈페이지 등에 게시한 통신판매업 신고번호를 삭제했으나[1] 여전히 사업자등록은 통신판매업자로 유지되고 있는 실정이다.

원래 가상화폐는 비중앙화된(decentralized) 성격을 갖고 있으며 이는 사생활 보호와 비즈니스 관점에서 중요한 의미를 갖는다. 그러나, 가상화폐에 대한 규제를 위해서는 가상화폐거래소와 같은 기관의 개입을 통해 개인을 식별할 수 있는 고

1) 전자신문. “공정위 ‘가상화폐거래소, 통신판매업자 아냐’…사실상 규제 법률 전무, 소비자 피해 확산 우려”, 2018년 1월 16일 수정, 2020년 6월 28일 접속, http://www.etnews.com/20180116000212.

객알기제도(Know-Your-Customer)나 거래를 통한 가상화폐의 흐름을 파악할 수 있는 자금세탁방지(Anti-Money Laundering)와 같은 규제의 시행이 불가피한 상황이다(Möser *et al.*, 2019). 가상통화거래소는 가상통화의 매수 및 매도 거래에 대해 서비스를 제공할 수 있으나 가상통화의 최초 매수를 위해서는 금융위원회의 허가를 받은 은행에서 발행한 계좌와 사용자 계정을 연결하여 실물화폐 입출금을 지원해야 한다. 2017년 12월 28일 발표된 가상통화 투기근절을 위한 특별대책으로 가상통화거래소 실명제가 2018년 1월 30일부터 시행되었다. 실명제 시행에 따라, 실물화폐 입출금에 대한 자금세탁방지 의무가 제공 은행에 부과되며 사용자는 기존 가상통화거래소에 지원되던 가상계좌[2]의 사용이 불가능하게 되고 사용자 인증정보와 일치하는 실명계좌만 사용할 수 있게 되었다.

이에 따라 은행은 자금세탁방지의무의 부담을 근거로 가상통화거래소에 대한 계좌 지원에 부정적 입장을 취하고 있으며 2018년 5월 현재 3 개의 은행만 가상통화거래소에 계좌연결을 지원하고 있다(최창열, 2019). 각 거래소 별로 연결된 은행을 보면 빗썸은 NH농협, 업비트(Upbit)는 기업은행, 코인원과 코빗은 신한은행에서 계좌연결이 가능하다.

가상통화 및 관련 사업자에 대한 정부기관의 규제와 가이드라인의 부재로 인해 사업 추진에 어려움을 호소한 거래소 및 사업자들은 2018년 1월 26일 한국블록체인협회를 출범하고 <표 1>과 같이 가상통화거래소 자율규제안을 마련하며 2018년 5월부터 약 14개 회원사에 대한 자율규제 심사를 추진한다고 발표했다. 그러나, 협회의 자율규제안은 강제성이 없으며 자율규제 내용 및 심사방법이 기존 은행과의 제휴 시 진행되는 실사와 크게 다를 바 없어 실효성에 대한 의문이 제기되고 있다. 중국, 마카오, 파키스탄과 같이 ICO를 전면적으로 규제하는 국가로부터 벨기에, 남아프리카, 영국처럼 블록체인 기술을 기회로 보고 육성하려고 노력하는 국가에 이르기까지 규제와 육성에 관한 동향은 전 세계적으로 다양하게 이루어지고 있다(정현준, 이홍노, 2018). 가상통화거래소의 법적 지위와 역할 및 의무는 가상통화의 법적 지위와 정의가 선행되어야 확립될 것으로 보인다.

〈표 1〉 2018/05 한국블록체인협회 자율규제안 주요 심사 내용

구분	주요 내용
일반 심사	- 자금세탁방지 시스템 마련 여부 - 이용자 자산보호 체계 적정성 여부 - 신규 코인 상장 시 투자정보 제공 여부
보안성 심사	- 사용자 인증과 네트워크 관리 시스템 - 서버와 월렛 관리 - 복구와 운영 시스템 - 개인정보 보호 부문

2.3 가상통화거래소 주요 기능 및 역할

가상통화거래소는 투자자의 실물화폐 자산이 가상통화로 환전되는 대표 채널로서, 은행과 같은 기존 금융기관과 가상통화를 매개로 하는 신규 서비스 사업자 사이의 중간자적 역할을 하고 있다. 구체적으로, 가상통화거래소는 투자자(일반 사용자) 접점 채널로서 개인정보 인증을 통한 회원의 가입/탈회, 계좌의 등록, 실물화폐의 입금/출금, 가상통화의 매입/매도 및 입금/출금 기능을 제공한다. 또한, 투자자 명의의 계좌를 등록하고 실물화폐의 입금/출금 기능을 제공하기 위해 은행과 업무협약을 맺고 관련 시스템을 구축하여 시스템화된 실물화폐 거래를 중개한다. 가상통화거래소의 기능을 요약하면 회원의 인증/가입/탈회, 실물화폐의 입금/출금, 가상통화의 상장 및 시장형성, 가상통화의 매입/매도, 가상통화 입금/출금의 다섯 가지로 볼 수 있다.

2) 은행에서 발행하는 무기명 일회성 계좌로, 온라인 결제 시 주로 사용된다. 결제금액이 지정되어 입금 확인 시 즉시 결제 처리되며 재사용이 불가능한 특징이 있다.

2.3.1 회원의 인증/가입/탈회 기능

가상통화거래소는 투자자의 신원정보를 확인해 ID/PW를 생성할 수 있도록 지원하며, 생성된 개인정보를 보호하고 관리하는 책임을 진다. 회원가입을 위해 필요한 개인정보는 이메일 주소, 휴대폰 번호, 본인 인증 정보(휴대폰 본인인증 등), 본인 신분증 정보(여권, 주민등록증, 운전면허증 등)이 있다. 많은 거래소가 로그인 비밀번호에 보안 비밀번호를 추가한 복수 비밀번호 체계로 개인정보를 관리함으로써 보안을 강화하고 있다. 또한, 로그인 시의 보안을 강화하기 위해 구글 OTP(One-Time-Password)의 사용을 권고하는 경우도 있다.

회원이 탈회를 원할 경우 계정 내 자산을 모두 처분/출금하고, 탈회 동의를 득한 후, 회원을 탈회 처리하고 개인정보를 삭제한다. 다만 '전자상거래 등에서의 소비자보호에 관한 법률'에 의거하여 "계약/청약 철회에 관한 기록(5년), 대금결제 및 재화 등의 공급에 관한 기록(5년), 소비자 불만 또는 분쟁 처리에 관한 기록(3년)은 법률에서 정한 기간만큼 보존 후에 폐기한다."

2.3.2 실물화폐 입금/출금 기능

가상통화거래소는 가상통화의 매입/매도를 위한 법화(실물화폐)의 입출금을 지원한다. 전 세계적으로 가상통화거래소에 대한 관심이 높지 않던 2016년 중반 이전까지는, 계좌입금(실명계좌, 가상계좌), 신용카드 충전, Paypal 등 간편결제 서비스 및 상품권을 이용하여 실물화폐를 충전할 수 있도록 지원하였으나, 각 국가별 규제 가이드라인 제정을 통한 관리감독이 시작된 이후, 신용카드, Paypal 등 간편결제 서비스, 상품권을 이용한 충전은 대다수의 나라에서 금지되었다.

국내 은행은 금융위원회 산하의 은행법을 적용받는 금융기관으로서, 금융감독원으로부터 매우 엄격한 관리감독을 받고 있다. 또한, 1989년 G7 정상회의 합의에 따라, 자금세탁방지를 위한 국제기준의 제정과 이에 대한 이행상황의 평가/감독을 위해 신설된 국제기구인 국제자금세탁방지기구(FATF: Financial Action Task Force)의 가이드라인 수행을 위해 내부통제체계를 구축해야 하는 의무가 있다. 현재 국내 가상통화거래소는 법적으로 금융기관 또는 금융사업자로 인정되지 않고 가상통화거래소에 계좌연결을 지원하는 은행에게 고객에 대한 자금세탁방지(AML: Anti-Money Laundering) 의무를 부과하고 있어 은행에 큰 부담이 되고 있다. 이로 인해, 가상통화거래소에 계좌 입출금을 지원하는 기능을 제공하는 국내 은행들은 신규 계좌의 개설을 허용하지 않거나 매우 엄격한 절차를 통해 제한적으로 허용하고 있다(최창열, 2019).

특히, 법인회원(국내/국외)에 대한 KYC(Know Your Client) 및 AML에 관련해 은행권은 더욱 큰 부담을 느끼며, 현재로는 개인회원에 한하여 은행계좌 연결기능을 제공하고 있으며, 향후 법인회원에 대한 KYC 및 자금세탁방지 시스템을 구축하기 위한 방안을 마련 중인 상황이다.

2.3.3 가상통화의 상장 및 시장형성, 유동성 관리 기능

가상통화거래소는 가상통화의 신규 상장 및 상장 폐지를 결정할 수 있다. 가상통화 상장 기준에 대한 법/규제 및 가이드라인이 부재한 상황에서, 개별 거래소는 자체 운영정책에 따라 사업성 및 기술성 등을 검토한 후 상장을 결정하고, 당일 상장공지 후 거래를 개시한다. 상장 직후 가격 상승/하락폭이 너무 크게 발생하여 문제가 된 사례가 있으며, 거래량을 증대하기 위한 노력은 거래소 간의 치열한 상장경쟁을 야기시키는 우려도 있다. 거래소에서 가상통화를 상장하는 유형은 두 가지로 구분된다. 한 가지는 거래소에서 가상통화 지갑을 직접 보유하고 운영하는 방식이며, 다른 한 가지는 타 거래소의 지갑을 대여하여 사용하는 방식이다. 빗썸/빗썸프로 마켓, 업비트(Upbit) 원화(KRW) 마켓은 첫 번째 유형으로서, 거래소에서 지갑을 보유하고 사용자가 해당 마켓 가상통화를 입금 및 출금할 수 있도록 지원한다. 반면, 비트코

인(BTC: Bitcoin)/이더리움(ETH: Ethereum) 마켓은 두 번째 유형으로서, 업비트(Upbit)는 비트피넥스(Bitfinex)와 제휴하여 서비스를 제공한다. 비트피넥스(Bitfinex) 마켓에 상장된 가상통화를 업비트(Upbit) 회원이 매입/매도할 수 있는 기능을 제공하고 있으나, 거래소에서 지갑을 보유하지 않아 가상통화 입출금은 불가능한 경우가 많다.

상장 후 거래소에서 보유한 가상통화와 고객이 입금한 가상통화는 시장 형성의 기반이 된다. 이런 이유로, 대다수의 거래소에서는 신규 상장된 가상통화에 대한 입금 프로모션을 진행하여 유동성을 확보하기도 한다. 가상통화를 기반으로 투자하는 'Crypto Fund' 또는 가상통화 시장에 투자하는 기관투자자 중 일부는 시장형성(Market Making)의 역할을 하기도 한다.

가상통화거래소는 대다수 법화(실물화폐) 마켓과 비트코인(BTC), 이더리움(ETH)와 같은 기축통화 마켓을 지원하고 있으며 일부 거래소는 자체 개발한 가상통화를 기축통화로 이용하는 마켓을 제공하기도 한다. 바이낸스(Binance)는 자체 가상통화 'BNB token'을 개발/발표해 마켓을 운영하고 있으며, Huobi도 자체 가상통화 'HT token'을 개발/발표해 마켓을 운영하고 있다.

2.3.4 가상통화 매입/매도 기능

가상통화거래소는 개별 가상통화에 대한 매입/매도 기능을 제공한다. 이는 일반적인 증권사 시스템과 유사하나, 시장이 하루 중 24시간 내내 운영된다는 점, 가격의 상한/하한 제한이 없다는 점이 증권사와는 구별되는 특징이라 할 수 있다.

가상통화 거래량이 폭증했던 2017년 11월에서 12월 무렵에 대다수의 가상통화거래소에서 서버가 다운되는 등 운영상의 문제가 발생했고, 이후 가상통화거래소는 시스템을 보강하는 등 운영의 안정화를 위해 노력하고 있다. 가상통화 매입/매도 거래의 안정화는 가상통화거래소의 핵심 기능이기도 하여 '가상통화거래소에 대한 법/규제 가이드라인' 및 '자율규제 가이드라인' 등에 필수적으로 포함되고 있다.

2.3.5 가상통화 입출금 기능

대다수의 가상통화거래소에서는 매수한 가상통화를 거래소 외부의 지갑으로 전송(송금/출금)할 수 있는 기능을 제공한다. 은행의 계좌번호와 같은 역할을 하는 지갑 주소를 이용하여, 일반적인 은행 계좌를 이용한 송금과 유사한 형태로 가상통화를 전송할 수 있다. 거래소 내부의 지갑 주소 간에 전송(블록체인 상에서 거래가 발생/체결)이 이루어지는 방식과 거래소 외부의 지갑 주소로 전송(블록체인에서 분리된 별도의 체인에서 거래가 발생/체결, 블록체인 네트워크 사용)되는 방식의 두 가지 형태가 있다. 전자의 경우, 거래소 내부에서 처리가 이루어져, 후자보다 전송 속도가 빠르고 전송 수수료 역시 무료이거나 저렴하다.

사용자 개인정보 및 계정정보 해킹을 통해 발생하는 가상통화 자산의 손실은 대부분 가상통화의 입금/출금 기능을 이용하는 것으로 알려져 있다. 은행의 계좌를 통한 오입금은 사고 신고를 통해 해당 계좌를 동결하는 등 제한적 조치가 가능한 것과는 달리, 가상통화 송금의 경우 지갑주소에 대한 제어가 불가능하다. 더욱이, FDS(Fraud Detection System)와 같이 이상거래를 사전에 탐지하여 사고로 인한 고객 피해를 방지할 수 있는 기능을 갖춘 거래소는 거의 없는 상황이다.

위에서 언급한 다섯 가지의 기능이 가상통화거래소의 핵심기능이라고 볼 수 있으며, 본 연구에서는 이들 중 특히 ① 회원의 인증 및 가입/탈회 기능, ⑤ 가상통화 입금/출금 기능에 초점을 맞추어 고객의 계정과 자산을 보호할 수 있는 방안을 연구해 보고자 한다.

2.4 가상통화거래소의 문제점과 발전 방향

현재 대다수의 가상통화거래소는 중앙집중형으로 운영되고 있다. 블록체인의 기본 사상은 탈중앙화로 절대 다수의 합의에 의해 계약이 성사되

고 진위여부가 판명된다는 것이나, 현재로서는 탈중앙화 거래소 구현에 필요한 기술적 한계로 인해, 일반적 IT서비스사에서 중앙형 데이터 서버를 두고 관리하는 방식과 유사하게 운영되고 있다. 모든 가상통화의 거래는 off-chain 상에서 거래가 가능하도록 별도의 폐쇄적 원장시스템을 구축할 수 있는데, 대다수의 가상통화거래소는 이와 같은 형태로 운영되고 있다. 중앙화된 구조로 운영되는 거래소는 일반적인 IT서비스와 마찬가지로 해킹 및 보안 관련 위협으로 자유롭지 못하며, 거래소 운영에서도 내부/외부적 리스크를 내포하고 있다.

2.4.1 중앙화된 서버에 대한 해킹을 통한 자산 탈취 및 위변조의 위협

중앙화된 거래소는 회원의 계정 및 정보, 자산의 내역을 중앙 서버에서 관리한다. 해당 서버가 해킹에 노출될 경우, 서버에 저장된 데이터를 탈취당하거나 해커의 의도대로 데이터가 변조될 수 있다. 일본 마운트곡스, 코인체크 등 거래소 해킹으로 발생한 투자자 피해 사례가 모두 이에 해당한다. 중앙화된 서버를 보호하기 위해서는 보안에 높은 비용을 지불해야 한다. 이에 중앙화된 거래소에서는 가상통화의 유실을 방지하기 위해 콜드월렛(Cold-Wallet)이라는 가상지갑의 형태로 일부 자산을 물리적으로 독립된 장소에 보관하며 사용자에게 접근 및 지불과 같은 관리 기능을 제공하기도 하는데(Dikshit and Singh, 2017), 이러한 기능을 전문적으로 제공하는 Bitgo와 같은 솔루션 사업자도 존재한다.

2.4.2 거래소 운영의 불투명성

거래소에는 회원의 법화(실물화폐) 자산 및 가상통화 자산이 보관되며, 이에 대한 매입/매도 거래 기록이 남는다. 증권거래와 유사하게 가상통화 거래에도 'Maker'라는 거래 생성자와 'Taker'라는 거래 체결자가 존재하며, 이들의 활동으로 '거래 호가'가 형성된다. 중앙화된 거래소의 경우, 이러한 거래 호가를 내부 서버에서 관리하기 때문에 실제로 'Maker'가 존재하는 호가인지, 혹은 운영자가 강제로 지정한 호가인지 확인하기 어려운 것이 사실이다. 또한, 거래소 서버가 중앙형으로 운영되기 때문에, 서버 장애가 발생할 경우 사용자들은 정말 운영상의 문제로 발생한 장애인지 악의적 조작인지 구분하기 어렵다. 2017년 말, 거래량이 폭증하며 국내 대다수의 거래소에서 서버장애가 발생해 적시에 매입/매도를 체결하지 못한 사용자들이 민원과 소송을 제기하는 문제가 발생했던 사례가 있었다. 또한, 거래 자산의 보유여부에 대한 감독기관의 관리가 이루어지지 않고 있어 '장부거래'에 대한 의혹이 끊이지 않는다. 이는 거래소에서 실제 매입/매도 거래를 지원하는 가상통화를 보유하지 않고 장부상 기록으로만 관리하다가 회원의 출금 요청이 있을 경우에는 타 거래소를 이용하여 출금액에 해당하는 금액만을 확보하는 거래방식으로서, 가상통화거래소의 운영 악화에 따라 파산이 발생할 경우, 고객은 보유 자산을 회수할 수 없어 큰 피해를 볼 수 있다.

2.4.3 블록체인 사상과 배치되는 운영방식

근본적으로 블록체인 기술은 탈중앙화에 기반하며 가상통화는 이를 가능하게 하는 수단임에도 불구하고, 가상통화거래소가 중앙화되어 운영된다는 것은 블록체인의 기본 사상과 배치되는 것이다. 현재로서는 탈중앙화 거래소를 운영하기에는 기술적 한계가 존재한다. 즉, 블록체인 상에 오더북을 생성만 하더라도 수수료의 부과(거래 체결과 무관), 가격 매칭 실패(최고 매도 가격, 최소 매수 가격에서 거래가 이루어지지 않을 수 있음), 속도 저하(블록체인 거래 컨펌 시간에[3] 의존적), 유동성 문제(매입/매도 거래 매칭에 시간이 소요되며 매칭 거래를 찾지 못할 수도 있음)와 같은

3) 블록체인 거래를 확정하는 데 걸리는 시간을 의미하며, 사업자별 및 기술 구현 방법/수수료 등에 따라 다르다. 1컨펌, 2컨펌 등으로 표현하며, 컨펌 시간이 짧을수록 전송 속도가 빠르다(1컨펌은 거의 즉시 송금됨을 의미한다).

문제점이 발생한다. 그러나, 가상통화거래소의 미래는 중앙화된 서버가 존재하지 않는 탈중앙화 거래소(Decentralized Exchange)라는 것이 업계의 전망이며, 이에 따라 대다수의 가상통화거래소는 탈중앙화를 준비하기 위해 자체적으로 기술을 개발하거나 외부 블록체인 개발사에 투자하는 등을 준비하고 있다.

탈중앙화 거래소에서는 블록체인 상의 개인 지갑에서 매입/매도 거래를 요청하면 탈중앙화된 거래소에서 자동으로 가상통화의 가격을 매칭하여 거래를 성사시키고 중간 대리인 없이 블록체인 상의 스마트 컨트랙트(Smart Contract)를 이용해 즉시 거래가 체결되는 형태의 서비스를 제공할 것이다. 거래소는 고객의 자산을 보유하지 않으며 다만 매칭 가능한 가상통화의 종류와 가격을 찾아주는 역할을 하게 되는 것이다. 여기서 관건은 위에서 언급한 문제점을 얼마나 빠르고 정확하게 해결할 수 있는가에 달려 있다. 카이버 네트워크(Kyber Network), 제로엑스 프로토콜(0x Protocol) 등 현재까지 다수의 탈중앙화 기술 기반의 블록체인 사업자가 서비스를 개발하고 있다. 여기서, 제로엑스 프로토콜은 분산형 거래소를 위한 공개형 프로토콜로서, 2018년 5월 현재 시장에 공개되어 있는 탈중앙화 거래소 관련 대표 서비스이다.

중앙화된 거래소는 기존 IT플랫폼 서비스와 유사한 구조로 운영되고 있어 기존 사이버 범죄의 대다수 유형이 발생할 수 있다. 중앙화된 가상통화거래소에서 발생 가능한 범죄에 의한 피해로는 고객의 개인정보 또는 계정 탈취를 통한 자산 피해, 사용자가 외부 사기에 연루되어 자발적으로 자산을 전송하는 피해 등이 있다.

Ⅲ. 연구방법

3.1 가상통화거래소의 선정

가상통화거래소의 현황 및 개선사항을 도출하기 위해, 글로벌 가상통화거래소 상위 10개 중 대표적이라 할 수 있는 미국의 비트피넥스(Bitfinex), 중국의 바이낸스(Binance), 한국의 업비트(Upbit)와 빗썸(Bithumb) 등 해외 2개, 국내 2개를 사례연구 대상으로 선정하였다. 각 서비스 사업자가 공식적으로 공개/배포한 정책 및 보도자료를 이용하여 분석하였다(<표 2> 참고).

3.2 가상통화거래소의 이용단계별 주요 기능

가상통화거래소는 초기에 전자상거래법상 통신판매업자로 등록하고 사업을 영위했던 만큼 서

〈표 2〉 사례분석 대상 가상통화거래소

구분		특징 및 선정 사유
해외	비트피넥스 (Bitfinex)	- 법화(실물화폐) 입출금 미지원 - KYC 및 계정관리에 있어서 매우 엄격한 편 - 다수의 가상통화를 지원하며 국내 업비트(Upbit)와 제휴 관계에 있음
	바이낸스 (Binance)	- 법화(실물화폐) 입출금 미지원 - 글로벌 거래량 1~2위 수준(Coinmarketcap.com 기준) - 다수의 가상통화 지원
국내	업비트 (Upbit)	- 기업은행 계좌 제휴로 법화(실물화폐) 입출금 지원 - 다수의 가상통화를 지원하며, 비트피넥스(Bitfinex)와 제휴하여 BTC/ETH마켓 지원 중
	빗썸 (Bithumb)	- NH농협은행 계좌 제휴로 법화(실물화폐) 입출금 지원 - 빗썸(Bithumb)과 빗썸프로(Bithumb Pro)의 2종 서비스 운영 중 - 지원하는 가상통화는 위 3사 대비 상대적으로 적은 편

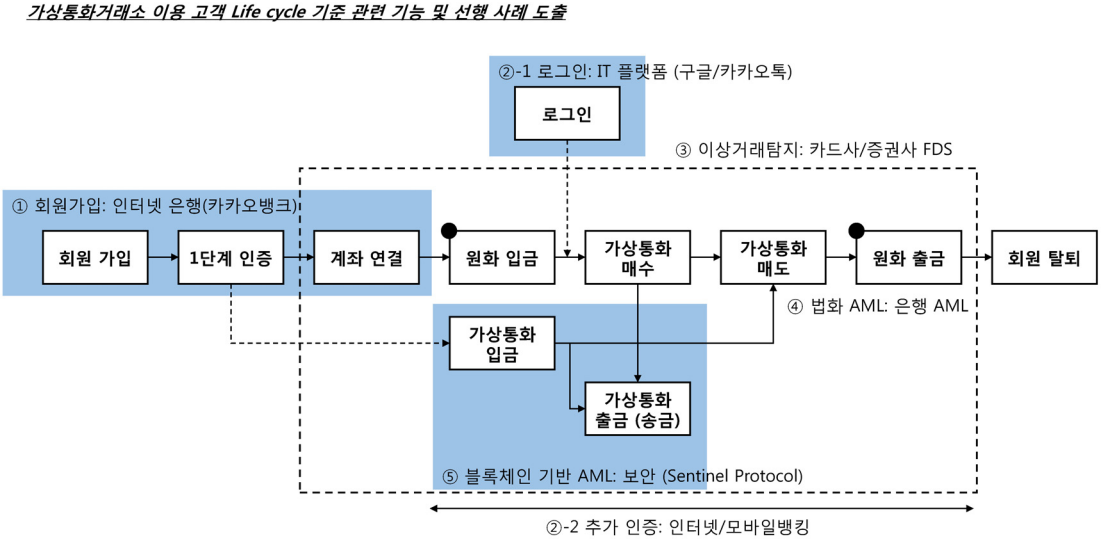
비스 제공 방식 및 구조는 온라인 서비스 사업자와 유사하고, 서비스의 성격은 금융서비스와 유사하다. 가상통화거래소가 고객의 계정과 자산을 보호하기 위해서 회원가입, 로그인, 자금세탁방지, 이상거래탐지 등의 기능을 효율적으로 제공해야 한다. 이러한 기능을 성공적으로 제공하는 기업을 벤치마킹하고 이를 가상화폐거래소의 현재의 기능을 비교하고자 한다. 가상화폐거래소 사용자의 이용단계별 주요 기능과 벤치마킹 대상은 <그림 1>과 같다.

제Ⅱ장에서 언급된 가상거래소에서 발생할 수 있는 주요 피해는 크게 두 가지로 나뉠 수 있다. 첫번째는 고객 개인정보 또는 계정을 탈취하여 자산에 손실을 발생시키는 피해이다. 이는 불법적으로 취득한 정보를 활용하여 회원으로 가입하거나, 로그인한 후, 해당 회원의 자산을 불법적으로 거래하여 피해를 끼치는 행동이다. 이러한 피해를 방지하기 위해서는 탈취한 정보만으로는 회원가입을 할 수 없도록 하거나, ID/Password만으로는 로그인이 이뤄질 수 없도록 추가적인 장치를 사용하는 방법을 적용할 수 있다. 또한, 로그인까지는 성공했다고 하더라도 이용하고자 거래에 따라 차등적인 추가 인증을 적용하거나, 특히 매입/매도 또는 입금/출금과 같이 자산이 탈취될 수 있는 민감한 기능을 이용하는 경우에는 이상거래를 탐지할 수 있는 보안기능을 통해 해당 시도를 사전에 차단할 수 있어야 한다.

두번째는, 사용자가 해킹이나 사기에 연루되어 자발적으로 자산을 전송하는 피해이다. 이는, 범죄자가 불법적으로 취득한 자금을 가상통화거래소의 기능을 통해 환전하거나 현금(법화)으로 출금하는 자금세탁행위에 해당한다. 이를 방지하기 위해서는 해당 혐의의 거래를 포착하여 이에 대해 적절한 조치를 취하는 방법이 있을 수 있다. 또한, 사고/신고 이력이 있는 가상통화 지갑주소를 파악하여 해당 지갑주소로는 거래자체를 시도할 수 없도록 사전에 방지하는 방법이 있을 수 있다.

중앙화된 가상통화거래소에서 발생할 수 있는 피해의 형태와 대응 기능 및 예방을 위한 요건을 정리하면 <표 3>과 같다.

<표 3>에서 표현된 중앙화된 거래소에서 발생 가능한 사이버범죄를 예방하기 위한 주요 기능을 중심으로, 유사사례와의 비교를 통해 개선점을 도출함을 본 연구의 목표로 한다.



〈그림 1〉 가상통화거래소 이용단계별 주요 기능과 벤치마킹 기업

〈표 3〉 중앙화된 거래소에서 발생 가능한 사이버 범죄 유형 및 대응 기능

피해 형태	대응 기능	예방을 위한 요건
① 고객 개인정보 또는 계정 탈취를 통한 자산 피해	회원가입	탈취된 개인정보만을 가지고 회원가입을 할 수 없어야 함
	로그인	탈취된 ID/PW 만으로 로그인에 성공할 수 없도록 추가적인 장치가 필요함 로그인 시도 시 이상징후를 민감하게 감지하여 문제 시 로그인을 차단할 수 있어야 함
	거래 추가 인증	기능의 민감도에 따라 인증 레벨을 차등 적용하여 제3자의 자산 탈취를 막을 수 있어야 함
	이상 거래 탐지(FDS)	계정의 로그인 및 매입/매도, 입금/출금 거래를 민감하게 모니터링하여 이상거래를 탐지, 거래를 사전 차단할 수 있어야 함
② 사용자가 외부 사기에 연루되어 자발적으로 자산을 전송하는 피해	법화 자금세탁방지 (AML)	범죄자가 해킹/사기 등으로 취득한 자금을 가상통화거래소를 통해 환전 및 현금 출금할 수 없도록 내부통제 시스템을 구축하여 혐의거래를 발견 및 적절한 조치를 취할 수 있어야 함
	가상통화 자금세탁방지(AML)	사고/신고 이력이 있는 가상통화 지갑주소를 파악하여 거래를 차단하거나, 일반 사용자들에게 정보를 전파하여 피해를 최소화할 수 있어야 함

3.3 기능별 벤치마킹 사례의 선정

본 연구에서는 가상통화거래소와 유사한 기능을 제공하는 선행 사업자와의 비교를 통해 가상통화거래소의 기능의 보안수준을 파악하고 개선방안을 제시할 것이다.

3.3.1 회원 가입

회원 가입은, 서비스 이용을 희망하는 사용자가 가상통화거래소의 이용약관에 동의하고, 사업자가 정한 인증단계를 거쳐, 계좌 연결까지 완료하는 단계를 의미한다. 기존 금융서비스의 경우, 사용자가 지점을 방문하여 대면상태의 인증을 거쳐 상품가입을 완료한 이후, 이용 채널로서 인터넷/모바일에 대한 사용을 등록하는 절차가 진행되나, 2017년 국내 최초의 인터넷 은행인 카카오뱅크는 전 과정에 걸쳐 비대면 채널을 통해 회원 인증 및 상품 판매를 진행한다는 측면에서 가상통화거래소의 회원가입 방식과 유사하다고 볼 수 있다. 이런 이유로, 회원가입 기능에서는 카카오뱅크를 사례 분석의 대상으로 삼고자 한다.

3.3.2 로그인

구글, 페이스북, 카카오톡 등 플랫폼에서 제공하는 서비스의 유형이 다양해지고 해당 플랫폼 회원 ID(사용자 계정)에 보관 혹은 저장된 정보가 증가함에 따라, 계정탈취에 관련된 사이버 범죄는 지속적으로 증가하고 있다. 이를 사전에 예방하거나 피해를 최소화하기 위해 IT플랫폼사들은 다양한 부가적 보안 기능을 제공하고 있으며 이는 PC 또는 모바일을 통해 로그인 가능한 가상통화거래소의 모델에도 적용해 볼 수 있을 것이다. 비자산성 사용자 데이터를 다수 보유(사진, 메일, 드라이브 등)하고 글로벌 서비스를 제공하고 있는 구글의 로그인 정책과 국내 사용자 98%가 사용하며 비자산성 정보(메신저, 쇼핑, 친구/관계정보, 계정과 연결된 기타 서비스 등)와 자산성 정보(카카오페이)를 보유하고 다양한 서비스를 제공하고 있는 카카오톡의 로그인 정책을 유사 사례로 분석하고자 한다.

3.3.3 거래 실행을 위한 추가 인증

사용자는 가상통화거래소에 회원으로 가입하고 법화/가상통화를 입금하여 거래 준비를 마친 후 매입/매도 거래 및 법화/가상통화 입금 및 출금 거래를 실행하게 된다. 이는 기존 인터넷/모바일 뱅킹을 통해 은행거래를 실행하는 과정과 유사하다고 볼 수 있다는 점에서, 은행의 인터넷/모바일 뱅킹의 거래 시 추가 인증방법과 증권사 인터넷/

모바일 뱅킹의 거래 시 추가 인증방법에 대해 사례 분석을 진행하고자 한다.

3.3.4 법화 자금세탁방지(AML: Anti-Money Laundering)

가상통화거래소에서 거래를 시작하기 위해 사용자가 취하는 가장 첫번째 행동은 일반적으로 은행계좌를 연결하여 법화(실물화폐)를 입금하는 일이다. 이렇게 입금한 실물화폐를 이용해 가상통화 매입/매도 등의 거래를 진행한 후 최종적으로는 다시 은행 계좌에서 실물화폐를 출금하게 된다. 은행의 경우 모든 자금의 이동과 관련된 거래에 대하여 FATF에서 제시한 자금세탁방지 가이드라인을 따르고 있다. 현재 가상통화거래소에 자금세탁방지 의무가 부과되지는 않았으나 한국블록체인협회에서 발제한 자율규제(안)은 해당 규정을 포함하고 있다. 이에 기존 금융권에서 준수하고 있는 자금세탁방지 내부통제방안(운영정책 및 시스템)의 일반적인 내용을 중심으로 사례를 분석하고자 한다.

3.3.5 가상통화 자금세탁방지(블록체인기반 AML)

가상통화거래소에서 가상통화를 외부 거래소 또는 지갑으로 출금할 수 있고 외부에서 입금할 수 있다. 이는 가상통화라는 자산의 이동으로 볼 수 있다는 측면에서, 법화와 마찬가지로 자금세탁방지 기능을 도입할 필요가 있다고 볼 수 있다. 또한, 자산의 외부 이동이라는 점에서 사용자 계정 또는 개인정보 탈취를 통한 사이버 범죄의 가장 중요한 표적이 된다. 이런 이유로, 가상통화를 통한 자금세탁을 방지하고 사이버 범죄 발생 시 피해를 최소화하기 위한 장치가 필요하다. 가상통화의 입금/출금은 블록체인 상에서 이루어지므로 블록체인 기반의 새로운 시스템 도입이 필요하다. 따라서, 블록체인 보안 솔루션인 센티넬 프로토콜(Sentinel Protocol)의 서비스 모델을 중심으로 사례를 분석하고자 한다.

3.3.6 이상거래탐지(FDS: Fraud Detection System)

가상통화거래소에 로그인하여 가상통화를 매입/매도, 입금/출금하거나 실물화폐를 입금/출금하는 행위는 일반적으로 인터넷/모바일 뱅킹에 로그인하여 송금/결제 등에서 사용하는 패턴과 유사할 것이다. 은행, 카드, 증권사에서는 인터넷/모바일상의 이상거래를 사전에 차단하고 피해를 방지하기 위해 FDS를 도입하고 있다. 2014년 금융보안연구원에서 발표한 '이상금융거래 탐지시스템 기술 가이드'에 따르면, FDS는 "정보수집, 분석 및 탐지, 대응, 모니터링 및 감사"의 4가지 기능으로 구성되어야 한다. AML이 자금세탁을 위한 이상거래 및 수사를 위한 보고체계를 다루는 반면, FDS는 사용자의 로그인 및 거래실행 전반을 대상으로 사용자 피해를 사전 차단함을 목적으로 한다. 은행, 카드, 증권사의 일반적인 FDS의 시스템 구성과 주요 정책을 중심으로 분석하고자 한다.

본 연구에서 다루는 가상통화거래소의 기능과 각 기능 별 벤치마킹 사례를 정리하면 <표 4>와 같다.

〈표 4〉 기능별 벤치마킹 사례 선정

No	구분	사례 분석 대상	선정 사유
1	회원가입	카카오뱅크	비대면 회원인증 및 상품 가입 지원
2	로그인	구글, 카카오톡	인터넷/모바일 로그인 정책 고도화
3	거래 추가 인증	은행/증권사	매입/매도 거래 및 입/출금 거래 유사
4	법화 자금세탁방지(AML)	은행 자금세탁방지 정책/시스템	가상통화거래소 내 법화(실물화폐) 이전과 유사
5	블록체인기반(AML)	센티넬 프로토콜	블록체인기반 보안 및 자금세탁방지 모델 제시
6	이상거래탐지(FDS)	카드/증권 FDS 시스템	가상통화거래소 내 로그인 및 거래실행 전반과 유사

Ⅳ. 사례분석

4.1 회원가입: 카카오뱅크

카카오뱅크는 2017년 7월 영업을 시작한 인터넷 은행으로서, 회원 가입 및 상품 판매 전 과정을 모바일 앱을 통해 서비스하고 있다. 카카오뱅크는 은행법의 적용을 받고 있으므로 기존 금융권에 적용되던 비대면 실명확인 허용방안(2015년 5월 개정)을 따르고 있다(<표 5> 참고).

〈표 5〉 비대면 실명확인 허용방안(2015년 5월 개정)

구분	방법
이중확인 (필수)	① 신분증 사본 제출 ② 영상통화 ③ 접근매체 전달 시 확인(대면) ④ 기존 계좌 활용 ⑤ 기타 이에 준하는 새로운 방식(바이오 인증 등)
다중확인 (권고)	⑥ 타기관 확인결과(휴대폰인증 등) ⑦ 다수의 개인정보까지

비대면 금융상품 개설 시 아래 방법 중 필수 실명확인 방법 중 2가지를 사용 후 사업자의 선택에 따라 기타 추가 인증방법을 선택할 수 있다. 2015년 이후 다수 등장한 '간편결제/간편송금' 등 대부분의 핀테크 서비스들은 회원가입 시 사용자 식별을 위해 '⑥ 타기관 확인결과(휴대폰인증 등)'를 사용하고, 서비스 이용을 위해 계좌연결 시 '④ 기존 계좌 활용'을 채택하고 있다.

카카오뱅크는 회원가입 시 '⑥ 타기관 확인결과(휴대폰인증 등)'를 사용하고, 비대면 계좌개설 시 '① 신분증 사본 제출'과 '④ 기존 계좌 활용'을 필수 인증방법으로 제시하고 있다. 이는 비대면 실명확인 가이드라인을 준수하면서도 사용자 편의성을 가능한 한 높이기 위한 선택이라 볼 수 있으며, '신분증 사본 제출'의 경우 이미지 스캔/분석 기술을 활용하여 즉시 신분증 검증을 통과할 수 있도록 지원한다.

먼저 카카오뱅크의 회원가입 절차를 가상통화거래소와 비교해 보면 <표 6>과 같다. 회원가입 과정에 있어서는 대부분 유사한 방식을 취하고 있으며 공통적으로 로그인을 위한 추가 인증 수단을 등록하도록 권장하고 있다. 카카오뱅크의 계정은 카카오계정으로 로그인 후 사용하는 방식을 취하며, 일단 카카오계정으로 로그인된 상태에서는 카카오뱅크 앱을 재실행할 때 추가 인증만 진행하면 된다. 추가 인증은 필수적이고 사용자는 단말기 지원 기능 및 개인의 선호에 따라 지문, 패턴, 인증비밀번호 중 1가지를 선택하여 적용할 수 있다.

〈표 6〉 회원가입 과정 비교

구분	카카오뱅크	해외		국내	
		비트피넥스(Bitfinex)	바이낸스(Binance)	업비트(Upbit)	빗썸(Bithumb)
1. 가입 방법 (ID/PW 등록)	휴대폰 번호	이메일 계정	이메일 계정	이메일 계정	휴대폰 번호
	카카오 계정				이메일 계정
2. 약관 동의	O	O	O	O	O
3. 본인인증	휴대폰 본인인증	신분증 인증(신분증/여권 등)		휴대폰 본인인증, 신분증 인증(신분증/여권 등) 선택	
4. 추가 인증	지문	구글 OTP		카카오페이 인증[1]	보안비밀번호, 구글OTP
	패턴				
	인증비밀번호				
5. 회원가입 완료					

주) 1) 공인인증서와 동일한 공개키 PKI 전자서명 방식으로 블록체인을 활용한 카카오톡 기반의 인증 서비스.

이미지 스캔 기술을 이용해 자동화한 카카오뱅크와는 달리, 해외 가상통화거래소는 위해 신분증을 통해 사용자의 본인 인증을 수행하며, 이는 상품 개설 시 영업일 기준 1~3일이 소요된다. 이는 일반적으로 글로벌 서비스를 제공하는 가상통화거래소가 전 세계 각지로부터 수집된 신분증 각각에 대해 진위여부를 검증할 수는 없더라도 최소한 해당 국가의 신분증 형태가 맞는지를 검증하기 위해서는 인적 확인 절차가 필요하기 때문이다. 국내 거래소는 기본적인 본인인증 방식으로 '휴대폰 본인인증'을 수행하고, 일부 타인 명의의 휴대폰을 사용하는 개인이나 외국인/법인의 신원확인을 위해 신분증 인증도 지원하고 있다.

위와 같은 회원가입 과정에서 발생할 수 있는 사이버 범죄는 개인의 이름 및 주민등록번호 등의 개인정보를 탈취하여 제3자가 가입을 시도하고 범죄에 사용할 수 있는 계정을 마련하는 것이다. 이를 방지하기 위해 이름 및 주민등록번호와 같은 기본적 신상정보 외 현재 가입을 시도하는 사람이 본인임을 확인할 수 있도록 하기 위해 신분증 인증, 휴대폰 본인인증 등 타 기관 발급 수단을 통한 본인인증을 의무화하고 있다. 추가 인증을 권장하는 또다른 이유는, 회원가입 이후 ID/PW를 해킹, 피싱, 스미싱 등의 방법으로 탈취당하더라도 추가 인증을 통해 범죄로부터 보호하기 위한 최소한의 장치를 마련할 수 있기 때문이다.

가상통화거래소의 회원가입 과정은 카카오뱅크와 거의 유사한 형태로 가입을 시도하는 개인의 신분정보 확인(KYC) 및 ID/PW 외 추가 인증수단을 등록하도록 함으로써 향후 발생할 수 있는 계정 탈취 사고의 발생을 예방하고 있다. 회원가입 과정은 인터넷은행 서비스와 유사한 수준으로 이루어지고 있으나 사용자 편의성 및 친화성은 부족하다.

위에서 분석한 국내 가상통화거래소는 국내 거래량 1~2위를 다투며, 규제기관의 관심을 받고 있어 보안 및 개인정보 취급현황에 대한 관리감독 이력을 충분히 확보할 수 있는 대상이다. 그러나, 소형 가상통화거래소 및 기타 가상통화 거래와 관련된 사업자(ICO 및 기타 사업자)는 관리감독의 대상이 아니다. 때문에 KYC를 요구하는 가상화폐거래소 및 ICO 사업자 등의 개인정보 관리현황에 대한 조사 및 관리감독이 이루어진 이력이 거의 없어 사용자의 주의가 요구된다.

회원가입 시 휴대폰 본인인증에 대한 높은 의존도를 개선이 필요한 점으로 들 수 있다. 2015년 전자서명법 개정으로 공인인증서 의무화가 폐지 결정되어 시행 예정되어 있다.[4] 전자서명법 개정으로 인해, 기존 금융권은 카카오뱅크처럼 더 이상 공인인증서를 의무적으로 사용하지 않아도 된다. 공인인증서 이외에도 통신사의 휴대폰 본인인증, 카카오페이의 카카오페이 인증 등을 통해 본인인증이 가능하며, 2017년 12월 신용카드 본인인증이 허용됨에 따라 세 가지의 인증수단을 사용할 수 있게 되었다. 비대면 인증수단이 완벽하게 제3자의 악의적 회원가입을 막을 수는 없겠으나 복수의 인증수단을 번갈아 사용할 수 있게 하는 등 개선 방안이 필요하다.

4.2 로그인: 구글, 카카오톡

인터넷 서비스의 등장 이후 각 서비스 사업자는 회원을 식별하고 관리하기 위해 ID(Identification)를 사용하기 시작했고, 해당 ID에 저장된 정보 및 실행 가능한 행위가 다양해짐에 따라 ID/PW의 탈취는 사이버 범죄의 대표적 유형이 되고 있다. 일반적으로 해커는 피싱, 파밍, 스미싱과 같은 방법을 이용해 ID/PW를 탈취하거나 자동화된 봇(Bot)을 이용해 ID에 비밀번호를 무작위로 반복 입력함으로써 계정 해킹을 시도한다.

이렇게 계정을 탈취한 이후 해당 계정으로 로그인하여 정보 삭제, 광고 게재, 계정 내 자산가치

4) ZDNet Korea, "21년만에 '공인' 뗀 전자서명법, 업계 속내 엇갈려", 2020년 5월 26일 수정, 2020년 7월 7일 접속, https://zdnet.co.kr/view/?no=20200521165959.

있는 서비스를 악용, 자산의 직접적 탈취 등의 범죄를 저지르게 되는데, 이를 방지하기 위해 로그인 과정에 IP정보를 이용한 위치정보 확인, 캡차(Captcha)와 같은 봇(Bot) 방지기능 적용, 접속 단말기 정보 추가 확인 등 보조적인 정보를 추가적으로 활용하고 있다.

<표 7>에서 볼 수 있듯이, 가상통화거래소는 다수의 고객을 보유한 구글, 카카오톡과 같은 플랫폼 서비스와 유사한 로그인 정책을 적용하고 있다. 이는 고액의 고객 자산을 보유하고 있어 비교적 짧은 운영기간 동안 다수의 해킹 공격을 경험함으로써 빠르게 개선방안을 마련해온 결과로 볼 수 있다. 그러나, 가상통화 시장이 성장함에 따라 거래소에 대한 해킹 공격은 지속적으로 증가할 수 있다는 점을 고려하여 사용자 편의성을 일부 양보하더라도 로그인 정책을 강화하는 방향을 고수하는 것이 고객보호 관점에서 타당하다. 로그인 기능을 강화하기 위한 수단으로서, 지정된 단말기에서만 로그인 가능하도록 등록하거나, 로그인 시 ARS 인증을 추가하거나, 보안 비밀번호를 다양화하는 등의 방안을 사용자 선택에 따라 추가하는 것을 고려해볼 수 있다.

〈표 7〉 구글[1]/카카오톡[2] 및 가상통화거래소 로그인 절차

구분		사례		가상통화거래소			
				해외		국내	
		구글	카카오톡	비트피넥스 (Bitfinex)	바이낸스 (Binance)	업비트 (Upbit)	빗썸 (Bithumb)
1. 정보 입력	ID/PW	직접 입력(5회 누적 오류 시 동일 ID 로그인 30분 이상 차단)					
	Bot 검증	없음		Captcha Text	Captcha Slide	없음	Captcha Image
2-1. 추가 확인	IP	확인(지역격차 큰 경우 차단)					
	접속 단말기	확인		없음			
	추가 인증	SMS인증, 구글OTP	가입 시 입력한 휴대폰번호 인증	SMS인증, 구글OTP	SMS인증, 구글OTP	카카오톡 알림톡 인증	보안 비밀번호, SMS인증, 구글OTP
2-2. 이상탐지 시 조치		로그인 일시 차단, 해당 이메일/연결된 보조 이메일/SMS 등의 채널로 로그인 시도 알림 (계정 차단 해제 시 일반적으로 비밀번호 변경 과정 필요)					
3. 로그인 알림		이메일/SMS 알림(설정 가능)	카카오톡 플러스친구 알림	이메일 알림	이메일 알림	없음	이메일/SMS 알림
4. 계정 보호를 위한 안내		계정 로그인 이력(일시/단말기정보/IP 등) 확인 가능 & 한 번에 로그아웃 가능 비밀번호 수시 변경 안내 기타 비정기적 자동 알림(보호 조치 방법)	계정 로그인 이력(일시/단말기정보/IP 등) 확인 가능 & 한 번에 로그아웃 가능 정기적 비밀번호 변경 알림	계정 로그인 이력(일시/단말기정보/IP 등) 확인 가능	계정 로그인 이력(일시/단말기정보/IP 등) 확인 가능	계정 로그인 이력(일시/단말기정보/IP 등) 확인 가능 & 한 번에 로그아웃 가능	계정 로그인 이력(일시/단말기정보/IP 등) 확인 가능

주) 1) 구글(계정정책), https://support.google.com/accounts/?hl=ko#topic=3382253.
2) 카카오(계정정책), https://cs.kakao.com/helps?category=170&locale=ko&service=52.

모바일앱으로 가상통화거래소의 서비스를 제공할 경우, 접속 단말기로부터 수집된 정보는 악의적 로그인의 수단으로 활용될 수 있다. 소위 '알뜰폰'이라고 불리는 가상 이동 통신망 사업자(MVNO: Mobile Virtual Network Operator) 사용자가 증가함에 따라 다수의 서비스에서는 MVNO 휴대폰 번호에도 ARS/SMS인증을 열어주게 되었고 이를 악용하여 일부 해커 집단은 MVNO 가맹점으로 등록하여, 탈취한 개인정보로 수만 개의 MVNO 유심(USIM)을 발급, 동일 단말기에 USIM을 교체하는 방식으로 신규 계정을 생성하여 개인의 자산을 탈취하는 등의 범죄를 저지르기도 한다.

로그인과 추가 인증 측면에서는 기존 플랫폼 사업자 및 금융사업자와 유사한 수준의 서비스를 제공하고 있다고 볼 수 있다. 현재 수준에서 보안을 강화하고 사용자 신뢰도를 높이기 위해서는 FDS 기반 위험 레벨링을 통해 위험수준에 대응하는 사용자 인증/재인증을 요구하도록 시스템의 설계, 사용자 안전성향에 따라 추가 설정이 가능하도록 다양한 인증 옵션을 제공하는 방안 등을 고려해 볼 수 있다.

4.3 거래 추가 인증

기존 금융권에서는 인터넷/모바일 뱅킹을 통한 거래 시 로그인 방법 및 인증 수준에 따라 사용 가능한 기능을 차등적으로 제공하고 있다. 이는 로그인 정보 탈취를 통한 자산 탈취를 방지하기 위함이나, 사용자 편의성 측면에서는 불편한 측면이 있다.

보안 안전성을 위해 대다수의 은행은 공인인증서와 보안카드 및 OTP(One-Time Password)의 사용을 의무화해왔으나, 2015년 전자서명법 개정과 2016년 간편결제 및 송금 서비스들의 등장으로 소액 거래 이력이 있는 계좌로의 송금이나 공과금

〈표 8〉 로그인 방법 및 기능별 인증 방법 비교

구분		은행	증권사	해외		국내	
				비트피넥스 (Bitfinex)	바이낸스 (Binance)	업비트 (Upbit)	빗썸 (Bithumb)
로그인 방법	ID/PW 기반	단순 조회만 가능	단순 조회만 가능	매입/매도, 가상통화 입/출금 가능		전 기능 사용 가능	
	공인인증서 기반	이체, 상품 가입/해지 등 가능	매입/매도, 이체 등 가능	해당 없음			
거래 시 인증	기본	계좌 비밀번호, 공인인증서, 보안카드 /OTP, (옵션) ARS/ SMS 인증	- 입/출금 거래, 계좌 비밀번호, 공인인증서, 보안카드/OTP, (옵션) ARS /SMS 인증, - 매입/매도 거래, (옵션) 거래 비밀번호	(법화 및 가상통화 출금 시) 구글 OTP (매입/매도 거래 시) 없음		(법화 및 가상통화 출금 시) 카카오페이 인증 (매입/매도 거래 시) 없음	(법화 및 가상통화 출금 시) SMS인증, 보안비밀번호 (매입/매도 거래 시) 없음
	간소화	별도 등록한 거래 비밀번호 입력 (약 30~50만원 한도, 특정 계좌 대상으로만 지원 중)	- 매입/매도 시 비밀번호 입력 생략 가능	해당 없음			

〈표 9〉 가상통화거래소의 FDS 구축 현황

구분	기존 금융사	간편결제사	해외		국내	
	은행/카드/증권	핀테크 기업	비트피넥스 (Bitfinex)	바이낸스 (Binance)	업비트(Upbit)	빗썸(Bithumb)
FDS	의무 도입 중	대다수 도입 중 - 카카오페이 - 네이버페이 - 페이코 - Toss	공식적으로 알려진 바 없음		Chainalysis 도입	자율규제안 수준 대응 준비 중

납부 등의 이체에 대해서는 이런 보안절차를 요구하지 않게 되었다.

<표 8>에서 나타난 것처럼 가상통화거래소도 실질적 자산 유출이 발생하는 가상통화 출금 시에는 추가 인증수단을 보안 장치로 두고 있다. 은행/증권사의 추가 인증 옵션을 고려할 때 사용자의 성향(안전성향)에 따라 추가 인증을 선택적으로 사용하는 방안을 고려해 볼 수 있을 것이다.

4.4 이상거래탐지시스템(FDS)

비대면 채널을 이용한 금융거래(인터넷/모바일 뱅킹, 신용카드 결제, 증권거래 등)가 증가하면서 금융권은 점차 이상거래탐지시스템(FDS: Fraud Detection System)을 도입하게 되었다. FDS는, 해외에서는 1990년대 중반부터 구축되기 시작하였으며, 국내의 경우 2000년대 초반 신용카드사들을 시작으로 은행, 보험사, 증권사로 점차 확산하여 도입되고 있는 상황이다(김태은 등, 2015).

2016년 코스콤(Koscom) 이 국내 31개 증권사가 이용 중인 코스콤 종합 증권 - 파생상품 업무시스템인 파워베이스(PowerBASE)에 FDS를 도입[5]함으로써 카드/은행에 이어 증권사에도 FDS가 사용되기 시작했다. 이와 유사하게 지금까지 대다수의 금융사는 FDS 솔루션을 자사의 상황에 맞게 커스터마이징하는 방식으로 시스템을 구축해 왔는데, 가상통화거래소에서도 유사한 방식으로 구축을 고려해 볼 수 있다. 특히 회원의 로그인, 법화(실물화폐)의 입금/출금 거래, 가상통화의 매입/매도 거래 및 입금/출금 거래 등 거래의 흐름을 고려하여 이상거래를 탐지할 수 있는 시스템의 설계가 필요하다.

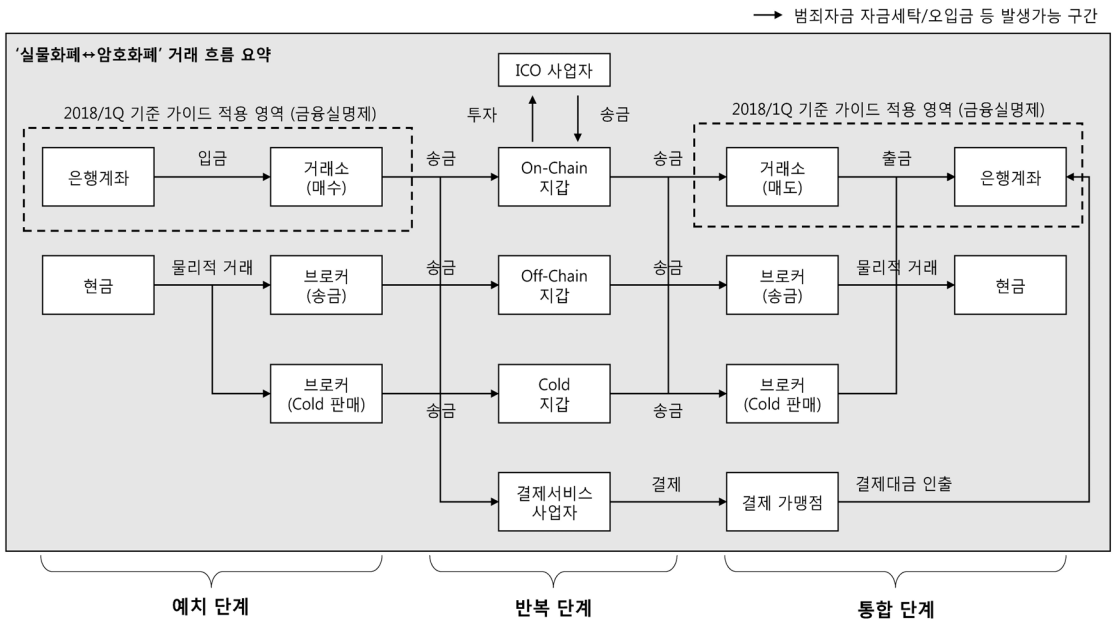
최근 기술의 발달로 FDS에도 기계학습 및 딥러닝의 적용에 대한 연구가 이루어지고 있다. 기존 FDS를 이미 도입한 금융회사들은 기계학습을 활용해서 기존 시스템을 개선시키는 방향으로 진행하고 있는 반면, 신생 핀테크 기업들은 기계학습 기반의 FDS를 바로 도입하기도 한다. 가상통화거래소에 대한 FDS 도입 의무가 법적으로 정의된 바는 없으나, 한국블록체인협회의 가상통화거래소 자율규제(안)에는 포함되어 있다. 가상통화거래소의 FDS 구축현황은 <표 9>와 같다.

현재까지 가상통화거래소에 FDS가 적용된 사례는 거의 전무하다. 로그인, 법화(실물화폐) 기반 거래(입금/출금), 가상통화 기반 거래(매입/매도, 입금/출금) 간의 연관성을 파악하여 이상거래를 탐지할 수 있는 시스템을 구축하기 위해서는 다량의 데이터의 축적과 관련 기술이 필요할 것이다. 국내 가상통화거래소들은 FDS를 향후 자체적으로 구축하거나 외부 솔루션을 도입할 것으로 보인다. 글로벌 수준의 은행/증권사로부터 성공적인 FDS를 벤치마킹하여 도입할 수도 있을 것이다.

4.5 법화 자금세탁방지(AML)

우리나라는 1989년 G7 정상회의에서 금융기관

5) ZDNet Korea, “증권사 공동 FDS 본격 가동,” 2016년 2월 1일 수정, 2020년 6월 28일 접속, https://zdnet.co.kr/view/?no=20160201095105.



〈그림 2〉 법화(실물화폐)↔가상통화 간 환전/입출금을 통한 자금세탁 가능 프로세스

을 이용한 자금세탁에 대처하기 위해 설립된 경제협력개발기구(OECD: Organization for Economic Cooperation and Development)의 산하 국제기구인 FATF에 2009년 정회원으로 가입하였고 FATF의 권고를 받아들여, 2005년 개정된 특정금융거래보고법에서 '고객알기제도'와 '고액현금거래보고제도'를 도입하였다(손영화, 2015). 이에 따라, 국내 금융기관은 자금세탁방지체제로서, 위험기반 자금세탁방지 절차를 수립하고, 보고체계를 수립하며(STR, CTR), 자금세탁방지에 대한 모니터링 시스템을 구축하고, 자금세탁방지 내부통제를 구축해야 한다.[6)]

제Ⅱ장에서 설명한 바와 같이 가상통화거래소는 법화(실물화폐)의 입금을 통해 가상통화 매입/매도 기능을 지원하고 있고, 이렇게 실물화폐로부터 환전된 가상통화는 블록체인상 입금/출금 기능을 통해 제3의 지갑(거래소, 기타 사업자)으로 전송될 수 있다. 반대로 외부에서 법화(실물화폐)로부터 환전된 가상통화가 블록체인 상에서 입금/출금되어 거래소로 전송되고, 이후에는 거래소에서 매도과정을 거쳐 법화(실물화폐)로 환전된 후 은행계좌로 출금될 수 있다.

현재 가상통화거래소와 은행 간에 발생하는 계좌 입출금 거래에 대한 자금세탁방지 의무는 은행에게만 한정되어 부과되어 있으며 가상통화거래소의 운영에 대해 책임은 은행에게 있다. 즉, 금융기관인 은행이 계좌 입금 및 출금으로 발생하는 현금거래에 대한 모니터링을 통해 AML을 수행하고 사고 발생 시 그 책임을 져야 하는 것이다.

은행은 이와 같은 의무와 책임에 대해 큰 부담감을 표하고 있는데, 그 이유는 계좌에서 현금이 출금된 이후 계좌로 입금되기 이전까지 자금의 흐름을 알 수 없으며 자금흐름에 대한 정보가 명확히 제공되지 않기 때문이다.

<그림 2>와 같이 가상통화를 이용한 자금세탁은 다양한 방법과 경로를 통해 이루어질 수 있다.

6) 금융투자협회, "금융투자회사의 컴플라이언스 매뉴얼 공통 · 증권 · 선물편", http://law.kofia.or.kr/service/law/lawView.do?seq=284&historySeq=0&gubun=cur&tree=part.

가상통화거래소는 법화(실물화폐)와 가상통화 간 환전 정보와 사용자의 매입/매도 수익률, 가상통화의 입출금 기록 등을 보유하고 있다. 따라서, 가상통화거래소가 은행의 자금세탁방지 의무를 분담할 경우, 이런 기록을 활용함으로써 이상거래로 추정되는 거래의 건수를 감소시킬 수 있을 것으로 예상되며, 이는 은행이 본연의 업무에 집중하면서 가상통화거래소와의 제휴를 통해 수익성을 향상시킬 수 있는 기반이 될 수 있다.

가상통화거래소의 자금세탁방지를 위한 내부통제체계의 구축을 위해서는 운영정책 및 시스템상의 설계가 필요하다. 현재 가상통화거래소의 법적 정의가 명확하지 않아 금융기관에 부여되는 자금세탁 의무를 강제할 수는 없겠으나 주요 기능과 업무 성격을 고려할 때 시스템 구축 및 운영을 통해 규제기관의 요청이 있을 경우 빠르게 대응할 수 있도록 거래소 사업자들이 자율적으로 사전에 대응하는 것이 필요할 것으로 보인다. 한국블록체인협회에서는 가상통화거래소 자율규제(안)에 자금세탁방지 의무를 포함하고 있으며, 국내 점유율 상위권 거래소의 경우 자율적으로 내부적 시스템 구축 및 운영정책을 수립하고 있다.

2017년 2월 22일 개정된 '외국환거래법 시행령 및 외국환거래규정 개정안 입법예고'는 비금융기관에 대한 자금세탁방지 의무 부과 사례를 보여준다(정지열, 2017).

> "2016년 11월 기획재정부는 전자금융업자인 센트비를 비롯하여 13개 업체가 외국환거래법을 위반하였다고 보고 금융감독원에 조사를 요청, 이에 2017년 2월 1일 한국핀테크산업협회는 성명서('비트코인 해외송금 서비스 위법 판단한 기재부 해석유감')를 내면서 강하게 반발하였다. 이에 2017년 2월 22일 기획재정부는 소액해외송금업 제도 구체화 및 외환거래 편의성 제고를 위한 '외국환거래법 시행령 및 외국환거래규정 개정안 입법예고'를 발표하였다. 기획재정부는 이 입법예고를 통하여 소액해외송금업 제도를 구체화하였으며, 해당 소액해외송금업의 등록요건, 업무범위(자금세탁방지 의무 포함), 거래안전성 확보 및 소비자 보호 방안을 발표하였다"(정지열, 2017).

위의 '소액 외환송금업체' 관련 사례와 같이 관련 법규가 개정됨에 따라 소액송금업자는 '금융실명거래 및 비밀보장에 관한 법률' 및 '특정 금융거래정보의 보고 및 이용 등에 관한 법률'의 적용을 받고 관련법에 따라 금융실명제 및 자금세탁방지 관련 의무를 부담하게 되었다. 이에 따라, 소액송금업자는 고객확인 및 요주의 대상자 확인(WLF: Watch List Filtering)[7] 시스템을 구축하여 개획재정부에서 제시한 금융거래 등 제한 대상자 Filtering, FATF 비협조국가 등의 고객 Filtering, 송금에 따른 고객정보 제공 등을 필수적으로 수행해야 한다.

소액송금업자의 자금세탁방지 시스템 구축 방법으로서 정지열(2017)은 자체 구축 및 상용 패키지 구입 방안으로 나누어 효율성 측면에서 검토하였으며 고객확인제도 지원 서비스(KYC 또는 CDD: Customer Due Diligence), WLF 지원 서비스, 한국은행 보고 시스템, 거래 모니터링 시스템, 의심 거래 보고 시스템 등을 지원할 수 있도록 상용 패키지를 커스터마이징하여 클라우드 컴퓨팅에 탑재하여 사용하는 방안을 제시하였다.

가상통화거래소를 금융사업자로 규정하게 될 경우 자금세탁방지의무가 부과될 것으로 보이며 이에 대비하기 위해 사업자별로 운영정책 및 운영체계를 수립하고 시스템을 구축하여야 할 것이다. 소액송금업자의 사례에 비추어 기존 금융권에 제시되고 있던 자금세탁방지의무 전체를 가상통화거래소에 부과하기보다는 기능 및 주요 내용을 고

7) 금융기관 등이 계좌개설 및 자금이체 등의 금융거래 완료 전에 요주의 리스트 정보와 고객정보를 비교/확인하는 절차(① UN에서 발표하는 테러리스트, ② 외국의 정치적 주요인물 리스트, ③ FATF에서 발표하는 비협조국가 리스트 및 FATF Statement 등).

〈표 10〉 가상통화거래소의 자금세탁방지 업무 현황

구분		해외		국내	
		비트피넥스(Bitfinex)	바이낸스(Binance)	업비트(Upbit)	빗썸(Bithumb)
내부통제	계획 수립	알려진 바 없음			
	보고체계				
	내부교육				
시스템	KYC/CDD	자체 수행	자체 수행	월드체크 도입[1]	자율규제안 수준 대응 준비 중
	AML	알려진 바 없음	없음	자율규제안 수준 대응 준비 중	

주) 1) ZD Net Korea, “업비트, 자금세탁 방지 위해 월드체크 도입”, 2018년 4월 30일 수정, 2020년 6월 28일 접속, https://zdnet.co.kr/view/?no=20180430160538.

려하여 효율적으로 운영정책 및 시스템 구축 요건을 정의해야 할 것으로 보인다.

<표 10>에서 볼 수 있듯이, 해외 가상통화거래소는 법화(실물화폐)를 취급하지 않으므로 실물화폐에 대한 자금세탁방지 기능은 해당사항이 없다고 볼 수 있다. 국내 가상통화거래소의 경우 정부 규제와 무관하게 외부 시스템을 도입하거나 내부 구축을 준비 중인 것으로 알려져 있다.

한국블록체인협회의 자율규제(안)에도 자금세탁방지 의무가 포함되어 있는 만큼, 가상통화거래소는 규제 이전에 자율적으로 법화의 자금세탁방지 내부통제체계를 구축할 필요가 있다. 이런 노력은 모범적 자금세탁방지 체계를 구축함으로써 금융권 및 규제기관, 사용자의 신뢰를 획득하고 안정적으로 사업을 확장/추진할 수 있는 기반이 될 것이다.

4.6 블록체인 기반 AML: 센티넬 프로토콜

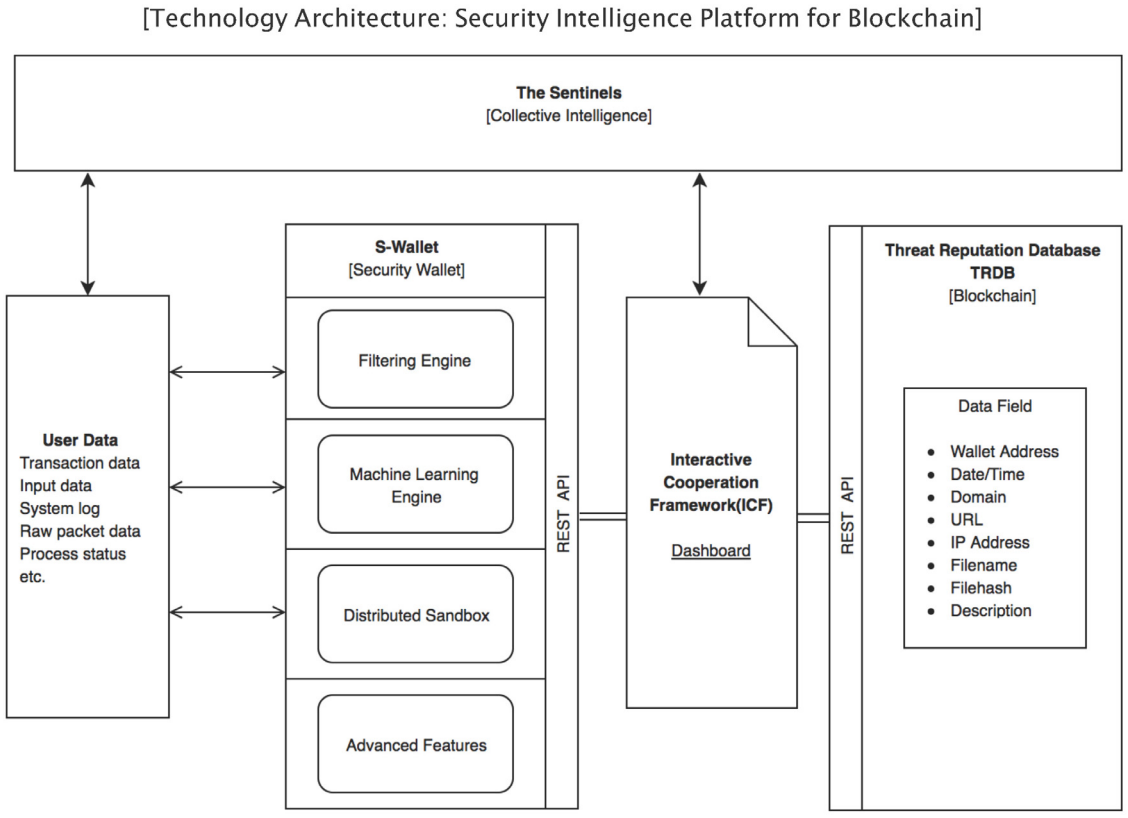
가상통화거래소는 법화(실물화폐)뿐만 아니라, 가상통화 자체에 대한 입출금도 지원한다. 따라서, 법화(실물화폐)의 자금세탁방지를 지원하기 위해서는 가상통화에 대한 자금세탁방지 및 이상거래탐지도 필수적이라 할 수 있다.

센티넬 프로토콜은 블록체인 기반의 보안 프로토콜을 지향하는 서비스 사업자로서 분권화된 가상통화 자산보호 방법을 제시하고 있다. 본 사례분석에서는 센티넬 프로토콜에서 제시하는 방법이 블록체인 상의 어떠한 특징에 기반한 것이며 가상통화거래소를 비롯한 유관 사업자에게 유용성이 있는지를 파악하고자 한다. 센티넬 프로토콜은 <그림 3>과 같은 구조로 시스템을 구성하고 있으며 각각의 기능은 다음과 같다.

① The Sentinels: 보안 분야 전문성을 인증 받은 집단 지성 그룹 및 개인을 의미하며 센티넬 프로토콜의 합의시스템[8]을 거쳐 자격을 획득하고 평가받을 수 있다. 아직 초기 시장인 블록체인 기반의 가상통화 보안을 위해 지속 등장할 새로운 방식의 위협/해킹을 빠르게 파악하고 분석, 대응방법을 찾는 자발적 보안 전문가들이라 할 수 있다. 인공지능의 기술적 불완전성을 보완하기 위해 인적 기능을 추가한 것으로 프로토콜에 확보된 다양한 정보를 바탕으로 이상 패턴 및 거래, 신고에 대한 분석 및 보정작업을 수행하게 된다. The Sentinels의 활동 역시 합의시스템을 거치게 되는데, 이는 The Sentinels의 악의적 행위를 사전에 방지하고 보안 대응의 정확성을 높이기 위한 방안으로 보인다.

② User Data: 유저 입력 데이터, 거래 데이터, 시스템 로그, 패킷 데이터 등 이상/위험거래 모니터링의 기반이 되는 데이터를 의미한다. FDS와

8) 집단지성 기반으로, 다수의 동의를 획득해 The sentinels의 의견을 시스템에 반영할 수 있도록 하고 있다.



자료: Uppsala Security, "센티넬 프로토콜 백서," 2020년 6월 28일 접속, https://uppsalasecurity.com/whitepapers/sentinelprotocol_whitepaper_korean.pdf.

〈그림 3〉 Sentinel Protocol 구조도

유사하게 개별 유저의 데이터가 다수 확보될수록 이상거래를 탐지하기 용이해지고 다수 유저의 데이터가 누적될수록 더 세분화된 위협/해킹 및 기타 이상거래에 대한 탐지가 가능하게 된다고 볼 수 있다.

③ S-Wallet: 센티넬 프로토콜에서 제공하는 통합 보안 지갑으로 Filtering Engine(암호화폐 주소, 사기성 도메인 주소, URL, IP, 그리고 파일에 대한 필터링용 엔진), Machine Learning Engine(이상 행위 분석을 위한 로컬 머신러닝 엔진), Distributed Sandbox(멀웨어 분석용 분산 샌드박스), Advanced Features(VPN, 제3자 통합 암호화폐 지갑과 같은 기능 강화 보안솔루션 추후 개발 예정) 등 네 가지 기능을 제공한다. 특히, Filtering Engine은 지갑 주소에 대한 모니터링을 통해 사고 지갑주소를 사전 감지하여 전송을 차단하는 등 가상통화에 특화된 기능으로 눈 여겨 볼만하다.

④ Interactive Cooperation Framework(ICF): 전 세계에서 발생하는 보안 위협행위에 대한 근본 원인 분석과 보안사고 분석 및 대응 정보가 담겨 있는 Sentinel Protocol 포탈의 대시보드로서, 권한을 소유한 The Sentinels들이 활용할 수 있는 기능이다. 센티넬 프로토콜을 사용하는 다양한 3rd party 사업자들로부터 확보한 데이터를 통합 제공함으로써 단일 솔루션사의 데이터베이스에 비해 양적/질적으로 풍부해질 수 있다.

⑤ Threat Reputation Database(TRDB): 사이버 범죄 정보가 저장된 지능형 데이터베이스로 3rd party 사업자가 센티넬 프로토콜을 이용하고자 할 경우 API 방식으로 간편하게 개발할 수 있도록 제공하고 있는 기능이다. TRDB에는 Wallet Address, Data/Time, Domain, URL, IP Address, Filenave, Filehash, Description 등의 정보가 담겨 있어 별도 보안 데이터를 수집/분석하지 않아도 이미 발견된 위협에서 3rd party 사업자를 보호할 수 있다.

위의 시스템 구조를 기반으로 센티넬 프로토콜은 <표 11>과 같은 기능을 수행한다.

<표 11>에 설명된 센티넬 프로토콜의 다섯 가지 기능은 모두 가상통화거래소의 사용자 계정 및 자산 보호에 필요한 기능이기에 본 사례를 참고하여 해당 프로토콜 도입, 또는 유사/타 사업자 제휴, 내부적 시스템 구축 등 방안을 모색할 필요가 있다. <표 12>에 나타난 것처럼, 현재 해외 가상통화거래소는 논외로 하더라도, 국내 가상통화거래소도 고객 자산보호를 위한 운영/시스템 상 대응이 매우 미흡한 상황임을 알 수 있다.

가상통화를 법화(실물화폐)로 환전할 수 있는 기능을 고려한다면, 가상통화거래소에 가상통화에 대한 자금세탁방지 의무를 부과하는 것이 필요하다고 할 수 있다. 이는 법화(실물화폐) 자금세탁방지 기능을 보완하는 역할을 할 수 있고 자금세탁 이상징후 파악을 통해 실제 가상통화거래소 고객의 자산을 보호하는 데 기여할 수 있을 것이다. 그러나, 현재 가상통화거래소의 가상통화에 대한

〈표 11〉 센티넬 프로토콜 주요 기능[1)]

구분	주요 내용
1. 상호협력 프레임워크(ICF, or Sentinel Portal)	가상통화 관련 사업자들이 센티넬 프로토콜을 이용함으로써 모든 보안 문제에 대한 지식과 지원을 쉽게 얻을 수 있도록 하고, 지속 업데이트되는 보안 정보를 가장 빠르게 습득할 수 있도록 한다.
2. 도난 방지	기존의 '자금세탁방지' 단계에 적용되는 '예치- 반복- 통합' 단계와 유사하게 가상통화도 거래소 매입/매도, 타 지갑 간 송금을 반복하며 범죄 자산을 세탁할 수 있다. 이때 거래에 사용된 '사고 지갑'이 확정될 경우 해당 지갑을 통해 입금/출금된 자산의 이동 경로가 모두 트랙킹됨으로써 사고지갑과 연관된 모든 지갑에서 '출금 금지' 처리가 가능하다. 출금금지 처리는 '은행 계좌에 대한 동결' 처리와 유사하여 자금의 유실을 일정 기간 지연시킬 수 있다. 나아가 범죄 자산의 출금 난이도를 높임으로써 범죄 성공을 어렵게 만들고 이는 범죄율의 감소에 영향을 줄 수 있다.
3. 거래 오류 방지	최근 유사수신 사기 등에 가상통화가 이용되고 있어, '사기 등록된 주소'에 대한 빠른 확산을 통한 피해 방지가 필요하다. 센티넬 프로톨은 사기/정상 지갑에 대한 정보를 빠르게 확산, 송금 시점에 자동으로 필터링해줄 수 있어 유사수신 사기를 인지하지 못하고 사기 지갑주소로 가상통화를 송금하고자 하는 사용자, 또는 ICO 참여 시 해킹(해커가 사업자의 지갑주소를 일시 변경/우회하도록 하여 잘못된 지갑주소로 전송)피해에 노출된 사용자를 보호할 수 있다.
4. 알려지지 않은 위협 차단	해커가 알려지지 않은 해킹 프로그램을 다양한 방법으로 유포할 경우, S-wallet의 머신러닝 엔진은 해당 소프트웨어의 위험성을 감지, 실행을 차단하여 해킹 피해를 사전 방지할 수 있다. 이렇게 파악된 정보는 The Sentinels의 분석을 통해 TRDB에 등록되고, 해당 정보는 센티넬 프로토콜을 사용하는 모든 3rd party 사업자에 전달되어 빠르게 신종 해킹 프로그램으로부터 사용자를 보호할 수 있게 된다.
5. 거래 추적	위 1~3의 기능을 하기 위해 위협감지/사고신고 된 지갑주소와 관련된 자산의 모든 거래이력을 트랙킹할 수 있다. 이는 공개된 블록체인 노드 모니터링을 통해 이루어지며 추후 범죄에 대한 수사 등에 활용될 수 있다.

주) 1) Uppsala Security, "센티넬 프로토콜 백서", 2020년 6월 28일 접속, https://uppsalasecurity.com/whitepapers/sentinelprotocol_whitepaper_korean.pdf.

〈표 12〉 가상통화거래소 현황

구분	해외		국내	
	비트피넥스 (Bitfinex)	바이낸스 (Binance)	업비트(Upbit)	빗썸(Bithumb)
1. 상호협력 프레임워크 (ICF, or Sentinel Portal)	운영/시스템 상 알려진 활동 없음		운영/시스템 상 알려진 활동 없음	
2. 도난 방지			비트코인 주소를 클러스터링하여 이상거래 탐지/추적 지원하는 Chainalysis[1] 도입, 유사수신 사기 신고 포상제 운영[2] 등 부분적 활동 중	시스템 상 활동 알려진 바 없음, '전자금융사기 예방 캠페인'을 통해 금융범죄 및 사기에 대한 사용자 인지도를 높여 피해를 감소시키고자 활동 중[3]
3. 거래 오류 방지				
4. 알려지지 않은 위협 차단				
5. 거래 추적				

주) 1) ZDNet Korea, "업비트, 암호화폐 불법자금 추적 솔루션 도입", 2018년 4월 3일 수정, 2020년 6월 28일 접속, https://zdnet.co.kr/view/?no=20180403132852&re=R_20180419152338.
2) ZDNet Korea, "업비트, 다단계 코인 신고제 시작...포상금 100만원," 2018년 3월 23일 수정, 2020년 6월 28일 접속, https://zdnet.co.kr/view/?no=20180323153606.
3) 글로벌경제신문, "'당신의 가치를 지키다' 빗썸 안전거래 교육 앞장서", 2018년 5월 3일 수정, 2020년 6월 28일 접속, http://cnews.getnews.co.kr/view.php?ud=67058.

자금세탁방지 시스템은 거의 전무하다고 볼 수 있다. 자체적 시스템 구축에는 많은 시간과 비용이 소요될 것이므로 블록체인 산업계에서 보안 기술을 가진 업체와 적극적으로 파트너십을 맺고 사업자 연합 내 지식공유를 통해 블록체인 산업 전반의 가상통화 자금세탁방지 시스템을 구축하는 것이 바람직할 것이다. 또한, 발견된 위협 또는 사고, 위험한 지갑계좌 등을 사용자에게 빠르게 전파함으로써 피해를 최소화할 수 있도록 정보의 전파 및 관리 채널의 구축과 운영도 중요한 개선 방안으로 고려할 수 있을 것이다.

4.7 사례분석 시사점 및 요약

다섯 가지 주요 기능별로 벤치마킹 대상인 기존 사업자와 가상통화거래소의 현황을 비교 분석해 보았다. 가상통화거래소는 사용자 계정에 실물화폐로 환전 가능한 가상통화를 보유하고 있고 가상통화 매입/매도 거래를 지원하기 위해 사업자 소유의 가상통화를 보유하고 있는 등 금전적 가치가 크기 때문에 초기부터 해커 및 사이버 범죄로부터 많은 위협을 받아왔다. 이러한 위협에 대응하기 위해 회원가입, 로그인, 거래 추가인증과 같은 기본적인 프로세스에서는 기존 인터넷 은행, 플랫폼 사업자에 준하는 수준의 보안통제를 적용하고 있는 것으로 보인다.

그러나, 법화(실물화폐) 및 가상통화에 대한 자금세탁방지(AML), 이상거래탐지(FDS)의 측면에서는 대응이 매우 미흡한 상황으로 파악되어 이를 개선하기 위해 가상통화 거래소 업계의 차원에서 보안수준을 높이기 위한 노력이 필요하고 개별 거래소에서도 운영정책 및 시스템을 마련함으로써 신뢰도를 높여야 할 것이다.

V. 결 론

5.1 연구의 기여 및 시사점

본 연구는 고객 계정과 자산을 보고하기 위한 목적으로, 가상통화거래소에서 사용자와 관련된 프로세스에서 핵심 기능 및 대상 항목을 도출하고, 각 항목별로 사례분석을 통해 가상통화거래소

의 시스템 현황을 확인한 후, 개선 방안을 제시하는 과정으로 수행되었다. 가상통화거래소 사업자, 가상통화 투자자. 솔루션 사업자에게 본 연구가 제시하는 실무적 시사점은 다음과 같다.

우선, 국내 가상통화거래소 사업자들은 2017년 말부터 폭발적으로 증가한 가상통화 투자자 및 거래량의 증가로 서버 장애 및 시스템 개선을 바쁘게 진행하고 있는 한편, 점차 엄격해지는 규제기관 및 은행 등 제휴 금융기관의 요구에 대응하고 있다. 본 연구는, 가상통화거래소의 구체적인 기능을 기존의 유관 사업자와 비교함으로써, 현재 가상통화거래소의 계정 및 자산보호의 기능별 수준을 파악하는 데에 도움을 줄 수 있을 것이다. 이를 바탕으로 필수적으로 보완이 필요한 것으로 파악된 법화(실물화폐) 및 가상통화 자금세탁방지(AML), 이상거래탐지(FDS)에 대한 구축 계획을 수립하는데 기여할 수 있을 것이다. 이러한 개선방안은 정부 규제기관 및 기존 금융권의 신뢰도를 높이고 사용자에게 안전한 서비스를 제공함으로써 가상통화거래소 시장을 활성화시키는 효과를 가져올 것으로 기대된다.

또한, 본 연구에서 실시한 사례분석의 결과를 통해 가상통화 투자자들은 자신이 거래 중인 가상통화거래소의 구조 및 기능별 취약점을 파악하고 사전에 주의함으로써, 가상통화거래소에서 가상통화에 대한 투자 및 입출금 과정에서 발생할 수 있는 피해를 방지할 수 있을 것으로 기대된다. 한국금융투자자보호재단에서 수행한 '2017년 가상화폐 이용자 조사 결과'에 따르면 전체 응답자의 13.9%가 가상통화에 투자한 경험이 있으며, 전체의 6.4%가 현재 보유하고 있었다.[9] 2017년 연말을 기점으로 국내 가상통화 투자자 및 거래량이 폭발적으로 증가하였고, 이에 따라 블록체인이나 가상통화에 대한 지식 없이 소위 '묻지마 투자'를 통해 큰 손실을 본 사례들이 다수 보도되고 있다. 또한, 가상통화의 높은 변동성을 이용하여 다단계나 유사수신 사기에 가상통화를 이용하는 경우도 지속 증가하고 있어 투자자 스스로도 가상통화 투자에 대한 위험성을 충분히 인지할 수 있도록 학습이 필요하다 할 수 있다.

2016년 핀테크의 등장 이후, 기존 금융권에만 도입되던 AML, FDS 등 솔루션을 필요로 하는 사업자들이 증가함에 따라 최근 레그테크 사업이 활발히 진행되고 있다. 기존 법화(실물화폐) 기반의 시스템을 넘어 블록체인 및 가상통화 특화 솔루션을 개발하고 가상통화거래소와 적극적으로 업무제휴를 진행함으로써, 기존에는 금융/비금융IT사를 대상으로 하던 금융보안솔루션의 시장이 블록체인 및 가상통화로 확대될 수 있을 것이다. 이는, 레그테크 솔루션사가 수익 창출을 기대할 수 있는 유망한 잠재 고객을 확보함과 동시에, 블록체인 및 가상통화 시장의 안정적 발전에 기여하는 기반이 될 것이라 기대된다.

5.2 한계점 및 향후 연구 방향

본 연구에서는 블록체인 및 가상통화, 가상통화의 거래를 가능케 하는 가상통화거래소, 가상통화를 이용한 범죄를 검토하고, 가상통화거래소의 주요 기능 및 각 영역 별 벤치마킹 사례와의 비교분석을 통해 가상통화거래소의 계정 및 자산보호의 현황을 파악해 보았다.

역사가 짧은 가상통화거래소의 특성으로 인해 아직까지는 가상통화에 대한 공격 사례와 이에 대한 대응방안에 대한 연구가 충분히 이루어지지 못한 상황이다. 특히, 가상통화거래소의 운영 프로세스 관점에서 보안을 유지하기 위한 관점으로 진행된 연구는 국내외를 매우 미진한 상황이다. 이로 인해, 공식적인 보도자료 등 공개된 자료에 많이

9) 한국금융투자자보호재단, "2017년 가상화폐 이용자 조사 보도자료", 2018년 3월 7일 수정, 2020년 6월 28일 접속, http://www.invedu.or.kr/mobile/information/m_report_mtrls.jsp?currentPage=1&boardNo=7&postingNo=14433&postingFlag=view&movePageURL=http%3A%2F%2Fwww.invedu.or.kr%2Fmobile%2Finformation%2Fm_report_mtrls.jsp&categoryNo=0&searchKey=A&searchValue=.

의존할 수밖에 없었으며, 이는 본 연구가 깊이 있는 분석에 이르지 못하게 하는 한계점으로 작용하기도 하였다. 그러나, 본 연구에서는 이런 한계점에도 불구하고 유관기관의 사례를 통해 거래소가 갖춰야 할 주요한 기능에 대한 방향성을 제시했다는 측면에서 의의를 갖는다고 할 수 있을 것이다.

후속 연구에서는 가상통화거래소만의 특징을 좀 더 고려함으로써, 가상통화거래소 내부 구조 및 운영을 심도 있게 분석하고, 보안수준을 획기적으로 높일 수 있는 구체적인 정책 및 시스템 개선방안이 제시되는 노력이 필요할 것이다. 또한, 블록체인 및 가상통화 산업이 성장하고 활성화됨에 따라 규제기관, 기존 금융회사, 가상통화 관련 사업자, 투자자의 관계 및 협력방안에 대한 연구가 지속적으로 이루어져 블록체인 및 가상통화 시장이 발전하고 기존 금융회사 및 관련 산업이 시너지를 창출하게 되기를 기대한다.

참 고 문 헌

[1] 글로벌경제신문, '당신의 가치를 지키다' 빗썸 안전거래 교육 앞장서, 2018. 5. 3., Available at Http://Cnews.Getnews.Co.Kr/View.Php?Ud=67058.

[2] 김은영, 김병초, "암호화폐 투자에서 투자자들의 투기적 행동을 야기하는 원인 규명: 제한된 합리성 이론을 기반으로", *Information Systems Review*, 제22권, 제1호, 2020, pp. 33-57.

[3] 김준상, "블록체인 기반 암호화폐의 조사", *한국컴퓨터정보학회논문지*, 제24권, 제2호, 2019, pp. 67-74.

[4] 김태은, 이정미, 황선호, 김광용, "금융 Fraud Detection System 운영 프레임워크 연구", *예술인문사회융합멀티미디어논문지*, 제5호, 2015, pp. 9-17.

[5] 손영화, "자금세탁방지업무를 위한 금융기관의 내부통제체계의 구축", *법과기업연구*, 제5권, 제2호, 2015, pp. 121-161.

[6] 유상이, 현지연, 이상용, "소셜 감성과 암호화폐 가격 간의 관계 분석: 빅데이터를 활용한 계량경제적 분석", *Information Systems Review*, 제21권, 제1호, 2019, pp. 91-111.

[7] 이관형, "암호화폐 관련 범죄의 예방과 수사에 관한 형사정책적 고찰: 최근 국회 입법 논의를 중심으로", *경찰학연구*, 제19권, 제4호, 2019, pp. 63-96.kjom16@naver.com

[8] 전자신문, 공정위 '가상화폐거래소, 통신판매업자 아냐'…사실상 규제 법률 전무, 소비자 피해 확산 우려, 2018. 1. 16., Available at http://www.etnews.com/20180116000212.

[9] 정지열, "소액송금업자를 위한 레그테크(Regtech) 고객확인 솔루션 제안", *Regtech Forum 세미나 발표 2*, 2017.

[10] 정현준, 이홍노, "암호화폐 투자와 규제현황", *정보과학회지*, 제36권, 제12호, 2018, pp. 48-56.

[11] 최창열, "금융투자 자산으로서 가상화폐 규제에 관한 연구", *E-비즈니스연구*, 제20권, 제1호, 2019, pp. 113-128.

[12] 한국금융투자자자보호재단, 2017년 가상화폐 이용자 조사 결과, 2008. 3. 7., Available at http://www.invedu.or.kr/mobile/information/m_report_mtrls.jsp?currentpage=1&boardno=7&postingno=14433&postingflag=view&movepageurl=http%3a%2f%2fwww.invedu.or.kr%2fmobile%2finformation%2fm_report_mtrls.jsp&categoryno=0&searchkey=a&searchvalue=.

[13] Abramova, S., P. Schöttle, and R. Böhme, "Mixing coins of different quality: A game-theoretic approach", In: *International Conference On Financial Cryptography And Data Security*, Springer, Cham, 2017, pp. 280-297.

[14] Christin, N., "Traveling the silk road: A measurement analysis of a large anonymous online marketplace", In: *Proceedings Of The 22Nd International Conference On World Wide Web*, 2013, pp. 213-224.

[15] Dikshit, P. and K. Singh, “Efficient weighted threshold ecdsa for securing bitcoin wallet”, In: *2017 Isea Asia Security And Privacy (Iseasp)*, IEEE, 2017, pp. 1-9.

[16] Fanusie, Y. and T. Robinson, *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*”, Center on Sanctions and Illicit Finance Memorandum, January, 2018.

[17] Mccorry, P., M. Möser, and S. T. Ali, “Why preventing a cryptocurrency exchange heist isn’t good enough”, In: *Cambridge International Workshop On Security Protocols*, Springer, Cham, 2018, pp. 225-233.

[18] Möser, M. and A. Narayanan, *Effective Cryptocurrency Regulation Through Blacklisting*, Preprint, 2019.

[19] Möser, M., R. Böhme, and D. Breuker, “An inquiry into money laundering tools in the bitcoin ecosystem”, In: *2013 Apwg Ecrime Researchers Summit*, IEEE, 2013, pp. 1-14.

[20] Möser, M., R. Böhme, and D. Breuker, “Towards risk scoring of bitcoin transactions”, In: *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2014, pp. 16-32.

[21] Rueckert, C., “Cryptocurrencies and fundamental rights”, *Journal of Cybersecurity*, Vol.5, No.1, 2019, pp. 1-22.

[22] Soska, K. and N. Christin, “Measuring the longitudinal evolution of the online anonymous marketplace ecosystem”, In: *24Th {Usenix} Security Symposium ({Usenix} Security 15)*, 2015, pp. 33-48.

[23] Vasek, M. and T. Moore, “Analyzing the bitcoin ponzi scheme ecosystem”, In: *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2018, pp. 101-112.

[24] Vasek, M. and T. Moore, “There’s no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams”, In: *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2015, pp. 44-61.

[25] ZDNet Korea, 21년만에 ‘공인’ 뗀 전자서명법, 업계 속내 엇갈려, 2020. 5. 26., Available at https://zdnet.co.kr/view/?no=20200521165959.

[26] ZDNet Korea, 업비트, 다단계 코인 신고제 시작...포상금 100만원, 2018. 3. 23., Available at https://zdnet.co.kr/view/?no=20180323153606.

[27] ZDNet Korea, 업비트, 암호화폐 불법자금 추적 솔루션 도입, 2018. 4. 3., Available at https://zdnet.co.kr/view/?no=20180403132852&re=r_20180419152338.

[28] ZDNet Korea, 업비트, 자금세탁 방지 위해 월드체크 도입, 2018. 4. 30., Available at https://zdnet.co.kr/view/?no=20180430160538.

[29] ZDNet Korea, 증권사 공동 Fds 본격 가동, 2016. 2. 1., Available at https://zdnet.co.kr/view/?no=20160201095105.

Information Systems Review
Volume 22 Number 4
November 2020

A Case Study on the Protection of Accounts and Assets on Cryptocurrency Exchanges: Focusing on the Processes of Related Institutions

Yoonjoo Lee* · Dongwon Lee** · Ingoo Han***

Abstract

With the growth of blockchain and cryptocurrency-related markets, cryptocurrency exchanges are growing as a new industry. However, as the legal and regulatory definitions of cryptocurrencies are still in progress, unlike existing industrial groups, they are not under the supervision of regulatory agencies. As a result, users (i.e., cryptocurrency investors) have suffered two types of damage that could occur from hacking and other accidents on the exchanges. One type of the damage is the loss of assets caused by the extortion of personal information or account and the other is the damage from users who might be involved in external frauds. Both are analyzed in comparison with existing operators whose functions are like the exchanges. The results of this study show that membership (KYC: Know Your Client), log-in, and additional authentication in transactions are on the similar level to those of the operators while the fraud detection system (FDS) and anti-money laundering (AML) of fiat currencies and cryptocurrencies need rapid improvement.

Keywords: Cryptocurrency, Blockchain, Anti-money Laundering, Fraud Detection System, Security, Investor Protection

* Investors & Partners relationship lead, Deargen inc.
** Corresponding Author, Assistant Professor, College of Social Sciences, Hansung University
*** Professor, College of Business, KAIST

◐ 저 자 소 개 ◑

이 윤 주 (yoonjoo.lee@daum.net)

중앙대학교 문예창작 및 불어불문학을 전공하고, KAIST 경영대학에서 정보경영 전공으로 석사학위를 받았다. KAIST, 비씨카드, 비티씨코리아닷컴(빗썸)에서 신규사업 개발 업무를 주로 했으며, 현재 AI기반 바이오 스타트업 디어젠에서 사업개발 및 투자유치업무를 하고 있다.

이 동 원 (dongwonlee@hansung.ac.kr)

한양대학교에서 재료공학을 전공하고, KAIST 경영대학에서 경영정보학 석사학위와 경영공학박사학위를 취득했다. LG CNS에서 시스템 엔지니어로 근무한 바 있고, 한성대학교에 교수로 재직 중이다. 주요연구분야는 데이터마이닝, 딥러닝, 추천 시스템, 온라인 소비자 행동 등이다.

한 인 구 (ighan@kaist.ac.kr)

서울대학교에서 국제경제학을 전공하고 KAIST에서 경영과학 전공으로 석사학위를 받고 미국 University of Illinois at Urbana-Champaign에서 회계정보시스템 전공으로 경영학박사학위를 받았다. 현재 KAIST 경영대학 교수로 재직 중이며 주요 연구분야는 인공지능을 이용한 재무분석, 신용평가시스템 및 가치평가 등이다. SCI급 국제학술지에 70여 편, 국내학술지에 80여 편의 논문을 발표하였다. 경영정보학연구 편집위원장, 한국경영정보학회장, 한국지능정보시스템학회장, 한국경영학회장을 역임하였다.

논문접수일 : 2020년 07월 20일 **게재확정일 : 2020년 09월 25일**
1차 수정일 : 2020년 09월 19일