개정판

HELLO,

헬로, 핀테크!

보안인증 · 블록체인

FINTECH

한국핀테크지원센터
Fintech Center Korea

발간사

핀테크(Fintech)는 말 그대로 금융(Finance)과 기술(Technology)의 만남입니다. 핀테크는 기술을 통해 우리가 이용하는 금융을 더 간편하게 하고, 손안의 금융으로 만들어 줍니다. 특히, 최근에는 빅데이터, AI, 클라우드, 블록체인 등 디지털 신기술이 금융분야에 적극적으로 도입되면서 금융의 디지털화, 플랫폼화, 탈중개화 등 금융혁신이 급격히 진행되고 있습니다. 이에 따라 세계 각국은 핀테크를 금융산업의 혁신과 융합을 촉진하는 새로운 성장동력으로 삼고 국가적인 지원정책을 경쟁적으로 펼치고 있습니다.

우리나라도 핀테크 산업 육성을 위해 금융규제 샌드박스 제도 도입 · 운영, 신용정보법 등 데이터 3법 개정, 오픈 API 구축, 한국핀테크지원센터 설립 등 적극적인 혁신금융정책을 추진하여 디지털 금융서비스가 다른 나라와 비교해 빠른 속도로 시장에 안착되고 있으며, 이를 통해 소비자의 금융 편의성이 제고되고 금융권의 디지털 전환(Digital Transformation)이 빠르게 진행되고 있습니다. 한국핀테크지원센터는 이러한 정부의 노력을 뒷받침하고 핀테크 생태계 구축 및 성장 지원을 위해 핀테크 기업에 대한 멘토링, 교육, 입주공간, 금융규제 샌드박스, 해외진출, 투자유치 등을 지원하고 있으며, 특히 금년에는 새로운 아이디어를 출시 전에 금융권의 실제 데이터를 바탕으로 테스트해볼 수 있는 D-테스트베드, 금융사와 핀테크 기업의 협력을 위한 금융사-핀테크 협력플랫폼, 이미 해외진출을 추진한 기업들의 경험을 공유하는 해외진출 플랫폼 등을 통해 혁신적인 아이디어를 가진 창업자들이 창업과 스케일업을 거쳐 유니콘으로 성장할 수 있도록 돕고 있습니다. 앞으로도 한국핀테크지원센터는 금융당국과 함께 기술기반 핀테크 기업을 발굴 · 육성하여 국내 디지털 금융혁신을 촉진하고 글로벌 유니콘 핀테크 기업으로 성장할 수 있도록 적극 지원해 나가겠습니다.

한편, 핀테크 분야는 앞으로 인력 수요는 크게 늘어나는데 비해, 인력 공급이 이를 따라가지 못해 전반적으로 인력 부족 현상이 심화될 것으로 전망됩니다. 따라서 핀테크를 이해하는데 필요한 기술적 측면과 핀테크 서비스의 개발 · 출시

등을 위해 알아야 할 법령 등 각종 금융관련 규제 등을 종합적으로 다룬 핀테크 교재의 필요성이 커지고 있는 상황입니다.

이에 지난 2020년, 금융위원회와 한국핀테크지원센터는 「헬로, 핀테크!」 교재 6종을 발간하여 핀테크 산업에 관심있는 일반인부터 핀테크 분야 재직자까지 누구나 핀테크 입문부터 지급결제 · 송금, 금융플랫폼 · 금융데이터, 자산관리 · 보험, 보안인증 · 블록체인, 개인신용정보 관리 · 활용 등 분야별 지식까지 습득할 수 있도록 하였습니다.

본 교재는 발간 이후 핀테크 기업, 금융회사, 대학 등 다양한 곳에서 핀테크 지식을 습득하는데 활용되고 있습니다. 최근 1년 사이에 핀테크 분야에도 많은 변화가 있었고, 이 변화를 교재에 수록했으면 하는 요청들이 많아 이번에 새롭게 개정판을 발간하게 되었습니다.

이번 「헬로, 핀테크!」 개정판은 빠르게 변화하는 핀테크 분야 규제와 시장 현황 등 내 · 외부 변화에 맞추어 그동안 제 · 개정된 법률, 기술 등 다양한 변화를 최대한 수록하였습니다. 이와 함께, 핀테크 분야에서 꼭 필요한 기반기술인 AI, 빅데이터, 클라우드, IoT 등에 대한 기초 지식을 습득하고 실습해 볼 수 있도록 '핀테크 기반기술' 편을 새로이 발간하였습니다.

시중에 핀테크를 다룬 많은 책들이 있습니다만, 이 교재는 핀테크 분야의 현황과 각종 금융관련 규제 · 제도의 변화를 종합적으로 정리한 교재라는 점을 약속드리며, 모쪼록 본 교재가 핀테크 기업과 핀테크에 관심있는 모든 분들께 잘 활용되고, 우리나라 핀테크 분야의 경쟁력을 높이고 핀테크의 혁신과 성장에 이바지할 수 있기를 기원합니다.

2021년 11월

한국핀테크지원센터 이사장

변영한

추천사

IT 기술의 발전은 금융의 많은 것을 바꿔놓고 있습니다. 금융회사를 직접 방문하지 않고 스마트폰 앱을 이용하여 간편하게 저축 · 송금 · 투자를 진행할 수 있으며, 인공지능(AI) 기술이 도입된 로보어드바이저를 통해 금융상품 추천을 받고, 현금 · 카드가 없어도 스마트폰에 내장된 결제모듈을 이용해 언제 어디서든 편리하게 물건을 구매할 수 있게 되었습니다.

이처럼 핀테크는 이미 우리 생활 깊숙이 자리 잡아 개인이 원하는 맞춤형 금융서비스와 높은 편의성을 제공하고 있습니다. 금융소비자들은 금융서비스 이용을 위한 비용을 절감할 수 있고, 언제 어디서나 서비스를 이용할 수 있기에 시 · 공간적인 측면에서도 혜택을 누릴 수 있습니다. 여기에 중소기업 및 소상공인에 특화된 금융서비스를 개발하기도 용이하고, 저소득층, 고령층 등 금융 사각지대에도 보다 다양한 기회를 제공하는 포용적 금융을 실천할 수 있습니다.

이에 정부에서도 핀테크 산업을 지원 · 육성하기 위하여 혁신금융서비스에 대한 금융규제 샌드박스 제도를 내실화하는 등 제도적 지원을 아끼지 않고 있으며, 금융회사들도 빠르게 변화하는 금융소비자의 니즈를 충족시키기 위하여 '디지털 트랜스포메이션'을 통한 새로운 조직으로 변화를 추구하고, 핀테크를 활용한 금융서비스 개발에도 누구보다 앞장서고 있습니다. 또한 핀테크 스타트업 기업들은 새로운 디지털기술을 도입하여 기존에 없던 금융서비스를 시도하며 금융회사들과 협업 · 경쟁을 통해 금융서비스의 고도화를 가속화하고 있습니다.

핀테크 산업은 다양한 관계자들의 협업 · 경쟁에 기반한 기술의 융합을 추구하고 있으며, 이를 지속적으로 발전시키기 위해서는 전문인력을 양성하고 관련 지식을 꾸준히 보급할 수 있는 생태계 환경조성이 무엇보다 필요합니다. 그런 의미에서 금융위원회와 한국핀테크지원센터에서 핀테크 특화 전문도서를 지속적으로 발간하는 것은 매우 바람직한 일이라 생각합니다.

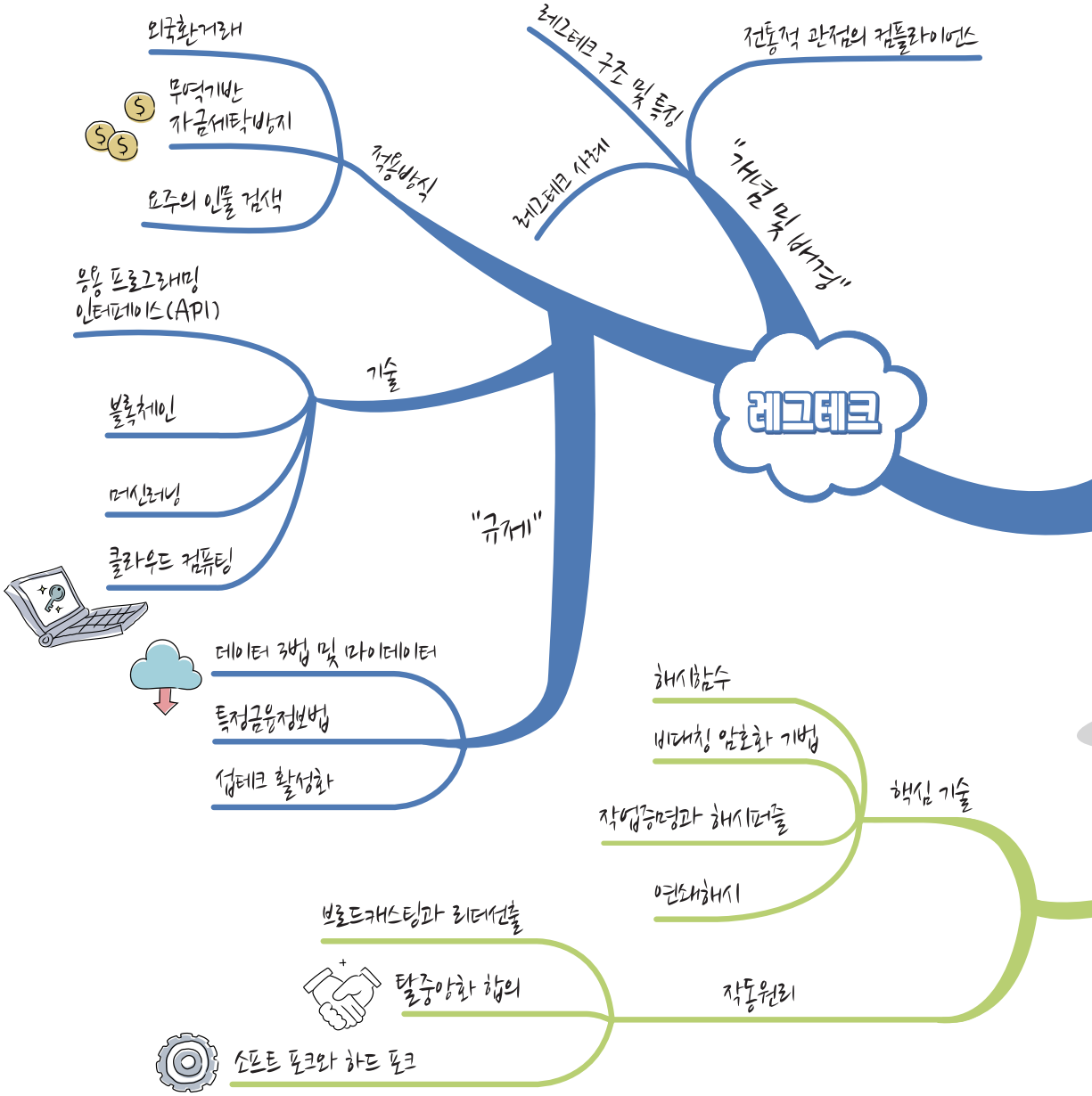
그동안 한국금융연수원은 금융 DT 아카데미를 통해 금융인의 디지털 금융 및 핀테크 역량강화를 위한 전문가 육성에 선도적인 역할을 수행해 왔습니다. 이러한 전문성을 바탕으로 우리 원이 지난 해 「헬로, 핀테크!」 6종 도서 발간에 이어 금년에도 최신정보를 반영한 6종 도서의 개정판 발간과 함께, 최근 주목받고 있는 빅데이터와 인공지능(AI), 클라우드, 사물인터넷(IoT) 등 핀테크 기반기술 관련 도서 1종의 추가 신규 발간 참여를 통해 우리나라 핀테크 산업 발전에 작게나마 기여할 수 있게 되어 매우 뜻깊게 생각합니다.

아무쪼록 본 도서가 현재 금융회사나 핀테크 업체에 근무하는 분들은 물론, 앞으로 해당 분야 취업이나 창업을 준비하는 분들에게도 많은 도움이 될 수 있기를 바랍니다. 그리고 무엇보다 핀테크 산업에 대한 국민적인 관심과 이해를 높이는 데 좋은 길잡이가 되기를 희망합니다.

2021년 11월
한국금융연수원 원장
서 태 종

HELLO, FINTECH

헬로, 핀테크!(보안인증 · 블록체인) 학습맵



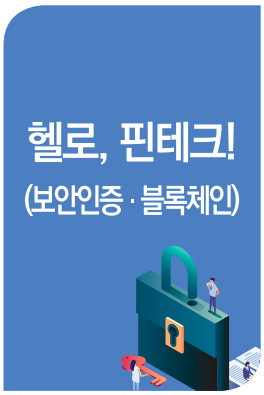
보안인증

- "개념"
  - 보안과 인증
  - 실명확인
  - 본인확인
- "인증 종류"
  - 지식기반인증
  - 소유기반인증
  - 생체기반인증
- "핵심기술 및 사례"
  - 암호기술
  - 블록체인
  - 인증서
  - 생체정보
  - 핀사이드
- "규제"
  - 전자금융거래법
  - 전자서명법
  - NYCRR 500, PSD2

블록체인

- "기술"
- "구조 및 특징"
  - 암호화폐
  - 자산유동화
  - 자금세탁
- "가상자산"
  - 비트코인과 블록
  - 분산 vs. 중복
  - 채굴
- "정의 및 변형"
  - 이더리움과 스마트 컨트랙트
  - 하이퍼레저 패브릭
  - 비트코인과 블록
- "정부정책 및 산업동향"
  - 정부정책 동향
  - 블록체인 시장 현황

CONTENTS

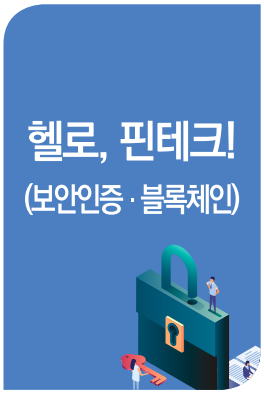


제5장 보안인증 관련 고려사항

제6장 블록체인 개요

제7장 블록체인의 작동원리와 효용

CONTENTS



제8장 블록체인과 가상자산

제9장 블록체인 정책 및 산업 동향

제10장 전통적 관점의 컴플라이언스 이해

제11장 레그테크 개요

제12장 레그테크 관련 기술 현황

제13장 레그테크 관련 법규 및 정책 동향

제14장 레그테크 시장 및 산업 동향

헬로, 핀테크!(보안인증 · 블록체인)

1장

본인인증의 이해

제1절 개요

제2절 보안인증 종류 및 특징

1장 본인인증의 이해

학습목표

1. 신원확인과 인증을 이해하고 설명할 수 있다.
2. 신원확인과 인증 관련 국내 규제를 이해하고 설명할 수 있다.
3. 신원확인과 인증을 위한 보안기술로서 보안인증의 종류 및 특징을 구분하고 이해할 수 있다.

학습개요

'신원확인(身元確認)'이란 "어떤 사람이 제공한 신상 정보가 맞는지를 확인하는 일"을 의미하고, '인증(認證)'이란 "어떠한 문서나 행위가 정당한 절차로 이루어졌다는 것을 공적 기관이 증명함" 또는 "네트워크나 서버에 접속할 때, 본인 여부와 정규 이용자 여부를 확인하는 방법. 일반적으로 사용자 아이디(ID)와 패스워드의 조합으로 본인을 특정함. 인증이 이루어지면 사용자가 가진 권한에 따라 데이터에 접근하거나 응용 소프트웨어를 이용할 수 있음"을 의미한다. 그리고 '보안인증(Security Authentication)'이란 "인터넷 뱅킹이나 특정 사이트에 로그인을 할 때, 이용자의 아이디와 비밀번호를 통하여 접속 및 사용 허가 여부를 확인하고 증명함. 또는 그러한 일"을 의미하나, 본 교재에서는 이해의 편의를 위하여 "'신원확인' 또는 '인증'을 위해 사용되는 보안기술 또는 보안절차"로 정의한다.

국내 규제로는 '신원확인' 관련하여 금융거래에 적용되는 「금융실명거래 및 비밀보장에 관한 법률(약칭: 금융실명법)」의 '실명확인'과 온라인거래에 적용되는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」의 '본인확인'이 있다. '인증' 관련해서는 「신용정보의 이용 및 보호에 관한 법률(약칭: 신용정보법)」의 '본인인증'과 「전자서명법」의 '인증'이 있다.

핀테크 회사는 「금융실명법」의 '실명확인', 「정보통신망법」의 '본인확인', 「신용정보법」의 '본인인증', 「전자서명법」의 '인증'에 따라 의무적으로 사용하여야 하는 경우를 제외하고 서비스를 제공할 때 보안인증을 적용하는 데 제한은 없다. 이는 핀테크 회사가 제공하는 금융서비스의 수준과 편리성 등을 자체적으로 고려하고 판단하여 자율에 따라 보안인증을 도입하여 사용할 수 있음을 의미한다. 보안인증은 그 방식에 따라 (ⅰ) 지식기반 인증, (ⅱ) 소유기반 인증, (ⅲ) 생체기반 인증으로 구분할 수 있다.

1장 본인인증의 이해

용어해설

❶ 핀테크 회사

특별한 제한이 없는 한 핀테크(FinTech)를 하고자 하는 IT회사 등을 통칭한다. 구체적으로, 「전자금융거래법」상 '전자금융업을 허가받거나 등록한 IT회사', '금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 IT회사', 또는 '금융회사 또는 전자금융업자와의 제휴를 통해 서비스를 제공하는 IT회사' 모두를 의미한다.

❷ 신용정보법

「신용정보의 이용 및 보호에 관한 법률*」의 약칭이다.

> * 법률 제16957호, 2020. 2. 4., 일부개정 내용 참고 [시행 2021. 2. 4.]

❸ 「신용정보법」 하위 규정

「신용정보업감독규정」을 의미한다.

❹ 「전자금융거래법」 하위 규정

「전자금융감독규정」을 의미한다.

❺ 「개인정보 보호법**」 하위 고시(개인정보처리자)

「(개인정보보호위원회) 개인정보의 안전성 확보조치 기준[1)]」을 의미한다.

> ** 법률 제16930호, 2020. 2. 4., 일부개정 내용 참고 [시행 2020. 8. 5.]

❻ 「개인정보 보호법***」 하위 고시(정보통신서비스 제공자등)

「(개인정보보호위원회) 개인정보의 기술적 · 관리적 보호조치 기준[2)]」을 의미한다.

> *** 법률 제16930호, 2020. 2. 4., 일부개정 내용 참고 [시행 2020. 8. 5.]

---

1) [시행 2020. 8. 11.] [개인정보보호위원회고시 제2020-2호, 2020. 8. 11., 제정]
2) [시행 2020. 8. 11.] [개인정보보호위원회고시 제2020-5호, 2020. 8. 11., 제정]

❼ 「정보통신망법*」

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 약칭이다.

> * 법률 제17358호, 2020. 6. 9., 일부개정 내용 참고 [시행 2020. 12. 10.]

❽ 「전자서명법**」

2020. 6. 9. 개정된 「전자서명법」을 의미한다.

> ** 법률 제17354호, 2020. 6. 9., 전부개정 내용 참고 [시행 2020. 12. 10.]

❾ 「전자금융거래법」 개정안

「전자금융거래법」 일부개정 법률안[3]을 의미한다.

❿ 개인정보 또는 개인신용정보

「개인정보 보호법」 제2조 제1호 또는 「신용정보법」 제2조 제2호에 따른 정의를 의미한다.

⓫ 처리

「개인정보 보호법」 제2조 제2호 또는 「신용정보법」 제2조 제13호에 따른 정의를 의미한다.

⓬ 금융규제당국

금융위원회(금융 관련 법령, 금융 감독정책 및 규정, 금융 산업 및 거래 감독, 금융회사 설립 및 인수 · 합병의 승인, 업무 인가 등), 금융감독원(금융회사에 대한 감독 및 검사, 시세조종 및 기타 불공정거래행위의 조사, 제재 등)을 통칭한다.

---

3) 제21대 국회 윤관석 의원 대표발의(의안번호 제2105855호)

제1절

개요

핀테크 회사가 고객과 직접 마주치지 않고(비대면) 스마트폰 등 IT기기를 통해(자동화된 방식) 고객에게 금융서비스를 제공할 경우, 핀테크 회사는 고객의 신원을 확인(신원확인)하거나 금융서비스를 이용하는 고객이 등록된 고객인지를 확인(인증)할 필요가 있다.

1 신원확인의 개념

1-1 신원확인

국내외 다수의 자료[4), 5)]에서는 '신원확인'과 'identification'이 동일한 의미로 설명되어 있다. 일부 국영문사전[6)]에서는 'identification'을 국문으로 "분별하여 알아본다"라는 의미의 '식별(識別)'로 풀이하는 경우도 있으나, 본 교재에서는 이해의 편의를 위하여 '신원확인'과 'identification'을 동일한 의미로 사용한다.

구체적으로 국립국어원의 우리말샘[7)]에 따르면, '신원확인(身元確認)'[8)]이란 "어떤 사람이 제공한 신상 정보가 맞는지를 확인하는 일"을 의미한다. 그리고 유럽연합의 「전자인증규정(eIDAS: electronic IDentification, Authentication and trust Services)」[9), 10)]에 따르면,

---

4) 금융위원회 보도자료 내 첨부, 4차 산업혁명 시대의 디지털금융 종합혁신방안 〈전자금융거래법령 등 개정방향〉(2020.7.24.)
5) 옥스퍼드 영한사전, 한국정보화진흥원(NIA), 한국전자통신연구원(ETRI) 등 네이버 사전 홈페이지 참고
6) 옥스퍼드 영한사전 등 네이버 사전 홈페이지 참고
7) 국립국어원 우리말샘 https://opendict.korean.go.kr/main
8) 국립국어원 내 우리말샘에서는 "신원 확인"으로 띄어쓰기를 하도록 설명하고 있으나, 본 교재에서는 편의상 "신원확인"으로 띄어쓰기 없이 사용함
9) REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (본문 83면)
10) 한국법제연구원(2016), 유럽연합(EU)의 전자서명 및 전자인증 법제도 동향

'전자신원확인(electronic identification)'이란 "자연인 또는 법인을 유일하게 나타내는 신원확인정보를 전자적 형태로 사용하는 과정"을 의미한다.

[관련법령] REGULATION (EU) No 910/2014 Article 3

> (1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

국내에서 신원확인 관련 규제로 금융거래에 적용되는 「금융실명거래 및 비밀보장에 관한 법률」(이하 "금융실명법")의 실명확인과 온라인거래에 적용되는 「정보통신망법」의 본인확인이 있고, 최근 논의가 활발히 진행되고 있는 「전자금융거래법」개정안의 신원확인이 있다.

1-2 「금융실명법」의 실명확인

「금융실명법」의 '실명확인'이란 금융회사와 금융거래 시(단, 개인 간의 거래는 제외) 주민등록표상의 명의, 사업자등록증상의 명의 등을 의미하는 실지명의(實地名義)를 확인하는 것을 말하며, 「금융실명법」에 그 근거를 두고 있다.

핀테크 회사가 「금융실명법」상 정의에 따른 금융회사에 해당할 경우 실명확인 의무가 부여된다. 대표적으로 「외국환거래법」 제8조 제3항 제2호에 따라 등록한 소액해외송금업자는 「금융실명법」상 금융회사에 해당하여 실명확인 의무가 있고 금융규제당국의 안내에 따른 절차 간소화 방안을 준수하여야 한다.

「금융실명법」의 실명확인과 관련하여 최근 「금융혁신지원 특별법」에 따라 혁신금융서비스로 지정된 "안면인식기술 활용 비대면 실명확인 서비스 (DGB대구은행)",[11] "은행 내점 고객 대상

11) 금융위원회 보도자료. 혁신금융서비스 3건 지정(2021.5.26.)

디지털 실명확인 서비스 (부산은행)",[12] "안면인식기술을 활용한 비대면 계좌개설 서비스",[13] "디지털 실명확인증표 기반 비대면 실명확인 서비스(아이콘루프, 파운트, SK텔레콤, 코인플러그)"[14] 사례가 있다.

[참고자료] 금융위원회 보도참고자료 중 일부 발췌

〈소액해외송금업자의 실명확인 절차 간소화 방안〉

➡ (최초 거래) 소액해외송금업자는 처음 금융거래를 개시할 때 거래상대방 (송금의뢰인)에 대한 「금융실명법」상 실명확인 필요

(추가 송금) 추가 송금실행前 ① 계약상 송금의뢰인, ② 당해 자금이체자의 실명 · 계좌번호를 확인 · 대조한 경우에 한하여 추가적인 실명확인은 생략 허용

출처: 금융위원회(2017.7.4.),
소액해외송금업자 대상 설명회 개최 – 정부는 자금세탁방지 의무, 실명확인절차 등 안내 예정

고객이 실명확인이 필요한 금융서비스를 이용하고자 할 경우, 고객은 (i) 최초 본인의 신분증을 제시하여 본인을 등록(예 주민등록증을 제시하여 계좌개설)하여야 하고, (ii) 등록절차가 정상적으로 완료된 이후부터 금융서비스(예 계좌조회, 계좌이체 등)를 이용할 때마다 등록된 본인이 맞는지, 그 고객의 요청이 정상적인 것인지, 고객의 요청이 인터넷 등 통신망을 통해 전달되는 과정에서 변경되지는 않았는지, 고객이 요청한 시점이 시간관계상 합리적인지 등을 확인하는 절차를 거치게 된다.

12) 금융위원회 보도자료. 혁신금융서비스 3건 지정(2021.4.14.)
13) 위 보도자료
14) 위 보도자료

[참고자료] 금융실명제에 대한 설명

금융실명법은 1997.12.31. 제정된 이후 2014.5.28. 불법 목적의 차명 거래를 금지하는 것을 골자로 개정되었다. 누구든지 불법 탈법 목적으로 타인의 실명으로 금융거래를 하여서는 아니 되며, 금융회사 등에 종사하는 자는 명의인의 서면상 요구나 동의 없이 금융거래정보등을 타인에게 제공하거나 누설해서는 아니 되며, 누구든지 금융회사 종사자에게 거래정보등의 제공을 요구해서도 아니 된다. 법관의 영장 또는 법원의 제출명령에 의한 경우 또는 금융위원회, 금융감독원장 등이 금융회사에 대한 감독, 검사를 위하여 필요로 하는 경우 등 예외적으로 금융거래정보를 제공하는 경우에도 그 제공범위는 사용 목적에 필요한 최소한의 범위로 제한되며, 금융회사는 거래정보를 공공기관 등에 제공한 날부터 10일 이내에 명의인에게 서면으로 이를 통보하여야 한다. 또한 금융실명법은 금융거래 시 실명의 사용 및 비밀보장과 관련하여 타 법률에 우선하여 적용된다. 불법행위를 목적으로 하는 차명 금융거래 금지 위반 및 비밀보장의무를 위반한 자에게는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해지며, 실명확인 의무 또는 거래정보의 제공사실 통보의무 등을 위반한 자에게는 3천만원 이하의 과태료가 부과된다.

출처: 금융용어사전, 금융소비자 정보포털 파인[웹사이트], http://fine.fss.or.kr/main/fin_tip/dic/financedic.js

실명확인의 방법으로는 (i) 금융회사가 고객의 '실명증표'(또는 '신분증')에 해당하는 주민등록증, 운전면허증, 여권, 외국인등록증을 확인하는 대면 실명확인 방법이 일반적이었으나, (ii) 최근 핀테크 산업의 발달로 직접 고객을 마주하지 않은 비대면 실명확인 방법이 많이 사용되고 있다.[15] 실명확인의 방법에서 주의할 사항으로 (i) 방식과 (ii) 방식은 방법상 차이가 있을 뿐 법률상 동일한 수준의 실명확인을 해야 한다는 것이다. 다시 말해, 고객이 스마트폰 어플리케이션(앱)을 통해 비대면 방법으로 계좌개설하기 위해서는 금융규제당국이 제시한 비대면 실명확인 방법을 반드시 따라야 한다.

금융규제당국이 제시한 비대면 실명확인 방법으로는 인증방식 중 2가지를 필수 의무 적용하고 1가지를 추가 적용하여 확인하는 것을 권고하고 있으며, 구체적인 내용은 다음과 같다.

15) 2015년 12월 금융규제당국은 1993년 8월 금융실명제 이후 20여 년간 유지해 온 '대면 확인(face-to-face) 원칙'을 변경하는 유권해석을 통해 온라인 금융거래 증가 및 정보통신기술 발전 등을 감안한 은행의 비대면 실명확인을 허용하고, 2016년 2월 제2금융권(금융투자업자, 상호저축은행 등)으로 확대함(2019.12.23. 금융위원회 보도자료 참고)

[참고자료] 비대면 실명확인 방법

(이중 확인: 필수) ① 신분증 사본 제출, ② 영상통화, ③ 접근매체 전달 시 확인, ④ 기존계좌 활용, ⑤ 기타 이에 준하는 새로운 방식(바이오 인증 등) 중 "2가지" 의무 적용
(다중 확인: 권고) ⑥ 타 기관 확인 결과 활용(휴대폰 인증 등), ⑦ 다수의 개인정보 검증까지 포함하여 ① ~ ⑦ 중 추가 확인

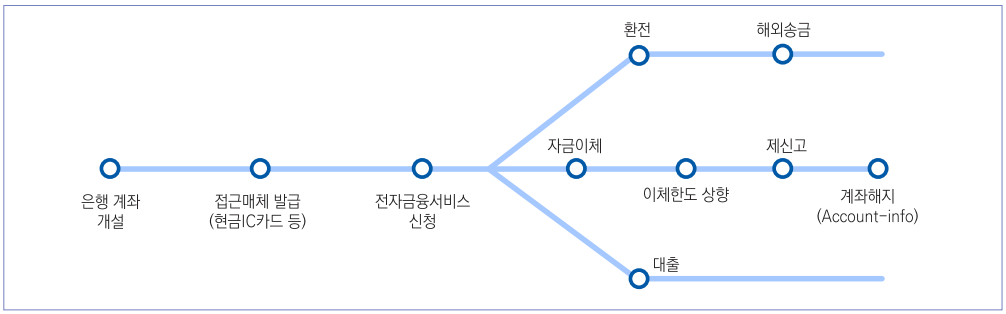
출처: 금융위원회(2016), 비대면 실명확인 운영 현황 및 향후 계획

금융위원회는 보도자료[16]로 고객이 은행업무 및 금융투자업무에서 비대면 실명확인 방법을 통해 할 수 있는 구체적인 내용을 설명하였다. 핀테크 회사 중 「금융실명법」 준수의무가 있는 회사는 이 내용을 참고하여 고객에게 제공하고자 하는 금융서비스에 따라 다양한 방식으로 비대면 실명확인 방법을 적용할 수 있게 되었다.

• 은행에서의 비대면 업무

은행에서 계좌개설 이후 종전 대면으로 이루어지던 접근매체 발급, 전자금융서비스 신청, 이체한도 상향, 해외송금 등이 모두 비대면으로 처리 가능하다.

〈그림 Ⅰ-1〉 은행 비대면 업무처리 프로세스



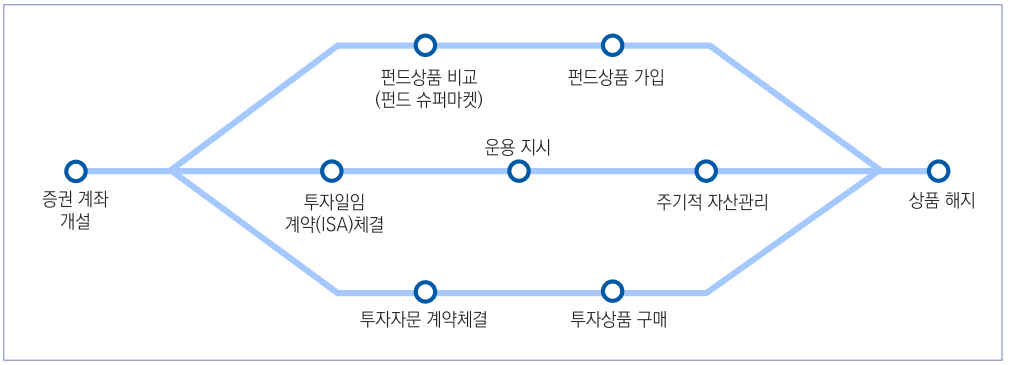
출처: 금융위원회 (2016), 비대면 실명확인 운영 현황 및 향후 계획

16) 금융위원회 보도자료, 비대면 실명확인 운영 현황 및 향후 계획(2016.5.26.)

• 금융투자에서의 비대면 업무

금융투자업무에서는 증권계좌 비대면 발급으로 고객 접근성이 크게 증가할 수 있고, 투자자문 및 ISA투자일임도 온라인으로 처리 가능하다.

〈그림 Ⅰ-2〉 증권사 비대면 업무처리 프로세스



출처: 금융위원회 (2016), 비대면 실명확인 운영 현황 및 향후 계획

1-3 「정보통신망법」의 본인확인

「정보통신망법」의 '본인확인'이란 인터넷 등 온라인을 통해 고객 본인의 확인이 필요한 경우 본인확인기관이 제공하는 본인확인서비스를 통해 본인을 확인하는 것을 말한다. 본인확인기관을 이용하는 이유는 「정보통신망법」에 따라 2012년 8월부터 별도의 법적 근거가 없을 경우 주민번호 수집 · 이용이 불가능하기 때문에 다른 정보로 대체하여 확인하는 것이다.

2021. 3. 9. 기준 본인확인기관과 관련하여 최근 방송통신위원회는 「정보통신망법」에 따라 신규 본인확인기관 지정심사를 신청한 네이버 주식회사, 주식회사 카카오, ㈜비바리퍼블리카, ㈜한국무역정보통신을 대상으로 지정심사 절차를 진행하였다.[17], ㈜한국무역정보통신은 본인

17) 방송통신위원회 보도자료, 2020년 제51차 위원회 결과(2020.9.23.)

확인기관으로 조건부 지정되었으나[18] ㈜비바리퍼블리카, 주식회사 카카오, 네이버 주식회사는 지정기준에 미치지 못한 것으로 판단되어 본인확인기관으로 지정되지 않았다.[19] 그리고 한국정보인증㈜, 한국전자인증㈜, 금융결제원, ㈜코스콤의 총 4개 '인증기관'은 「정보통신망법」 제23조의 3제1항에 따라 본인확인기관으로 조건부 지정되었다.[20]

[관계법령] 정보통신망법 제23조의3

제23조의3(본인확인기관의 지정 등)

① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발 · 제공 · 관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.

1. 본인확인업무의 안전성 확보를 위한 물리적 · 기술적 · 관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적 · 재정적 능력
3. 본인확인업무 관련 설비규모의 적정성

참고로, 본인확인은 온라인을 통해 고객 본인의 확인이 필요한 경우에 사용되는 방법이므로 금융거래에서는 「금융실명법」의 실명확인 대신 사용될 수 없다는 점을 유념할 필요가 있다.

1-4 「전자금융거래법」 개정안의 신원확인

「전자금융거래법」 개정안에는 「금융실명법」 실명확인에 대한 특례가 있다. 정무위원회 검토보고서[21]에 따르면, 전자금융거래[22]에서 실명확인 방법 등에 관한 특례를 규정하여 금융회사는 대면거래에서도 전자적인 방법 및 절차에 따라 실지명의를 확인할 수 있도록

18) 방송통신위원회 보도자료, 2020년 제69차 위원회 결과(2020.12.16.)
19) 방송통신위원회 보도자료, 2021년 제8차 위원회 결과(2021.3.9.)
20) 방송통신위원회 보도자료, 2020년 제57차 위원회 결과(2020.10.28.)
21) 정무위원회 수석전문위원 이용준(2021.2.), 전자금융거래법 일부개정법률안 검토보고
22) 금융상품 및 서비스를 제공할 때 그 전부 또는 일부가 전자문서 등 전자적 방식으로 처리되는 거래

하고(안 제6조의3 제1항), 비대면거래[23]의 실지명의 확인 시에는 주민등록증 등의 전자적 제출, 영상통화 등으로 대조하는 방법, 다른 금융회사 등에 개설된 계좌에 대한 전자자금이체 내용을 확인하는 방식, 스마트·모바일기기를 활용하여 본인확인기관으로 지정된 이동통신사업자를 통하여 알아보는 방법 등을 중첩적으로 적용하도록 하고 있다(안 제6조의3 제2항).[24]

이에 핀테크 회사는 본인이 제공하는 서비스 특성상 「전자금융거래법」 신원확인이 적용될 수도 있으니 「전자금융거래법」 개정안의 국회 통과 여부 및 시행일을 유념할 필요가 있다.

[관계법령] 전자금융거래법 개정안 제6조의3

제6조의3(전자금융거래에서 실명확인 방법 등에 관한 특례)

① 금융회사는 비대면거래가 아닌 전자금융거래에서 「금융실명거래 및 비밀보장에 관한 법률」 제3조에 따라 실지명의(이하 이 조에서 "실지명의"라 한다)를 확인하는 경우에는 대통령령으로 정하는 전자적인 방법 및 절차에 따라 실지명의를 확인할 수 있다.

② 금융회사는 비대면거래에서 실지명의를 확인하는 경우에는 「금융실명거래 및 비밀보장에 관한 법률」 제3조제7항에 따라 정하는 방법 및 절차와 다른 방법 및 절차로서 다음 각 호의 방법을 대통령령으로 정하는 바에 따라 중첩적으로 적용하여 실지명의를 확인하여야 한다.

1. 이용자의 실지명의를 확인할 수 있는 증표 또는 서류로서 주민등록증, 그 밖에 대통령령으로 정하는 증표 · 서류의 사본을 대통령령으로 정하는 전자적 방식에 따라 제출하는 방법
2. 금융회사의 종사자가 제1호에 따라 제출된 증표 · 서류의 사본 상의 사진을 확인함으로써 영상통화 등으로 이용자와 대조하는 방법
3. 해당 금융회사가 다른 금융회사나 종합지급결제사업자에 개설된 이용자의 계좌에 대한 전자자금이체 내용을 확인하는 등의 방식으로 이용자가 그 계좌를 정당하게 보유하는 자인지를 확인하는 방법
4. 이용자가 보유하는 스마트 · 모바일 기기를 활용하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3에 따라 본인확인기관으로 지정된 이동통신사업자를 통하여 이용자 본인인지를 확인하는 방법
5. 그 밖에 비대면거래에서 이용자를 확인하는 데에 사용할 수 있는 전자적 방법으로서 대통령령으로 정하는 방법

23) 금융회사 또는 전자금융업자와 이용자 간에 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 하는 전자금융거래

24) 금융위원회에 따르면, 2015년부터 비대면 실명확인이 허용되어 ① 신분증 사본, ② 영상통화, ③ 접근매체 전달시 확인, ④ 기존계좌 활용, ⑤ 기타 중 2가지를 확인하도록 하였으나 대부분의 금융회사가 신분증 사본을 요구하고 있음

2 인증의 개념

2-1 인증

국내외 자료[25]에 따르면 '인증'과 'authentication'은 동일한 의미로 설명되고 있다. 구체적으로 국립국어원의 표준국어대사전[26] 및 우리말샘[27]에 따르면, 인증(認證)이란 "어떠한 문서나 행위가 정당한 절차로 이루어졌다는 것을 공적 기관이 증명함" 또는 "네트워크나 서버에 접속할 때, 본인 여부와 정규 이용자 여부를 확인하는 방법. 일반적으로 사용자 아이디(ID)와 패스워드의 조합으로 본인을 특정함. 인증이 이루어지면 사용자가 가진 권한에 따라 데이터에 접근하거나 응용 소프트웨어를 이용할 수 있음"을 의미한다.

유럽연합의 「전자인증규정(eIDAS)」[28), 29)]에 따르면, '인증(authentication)'이란 "자연인이나 법인의 전자신원확인 또는 전자적 형태로 되어 있는 데이터의 근원과 무결성의 확인을 가능케 하는 전자적 과정"을 의미한다.

[관련법령] REGULATION (EU) No 910/2014 Article 3

> (5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

국내의 '인증' 관련 규제로는 「신용정보법」의 본인인증과 「전자서명법」의 인증이 있고, 최근 논의가 활발히 진행되고 있는 「전자금융거래법」 개정안의 인증이 있다.

---

25) 동아출판 프라임 영한사전 등(네이버 사전 홈페이지 참고)
26) 국립국어원 표준국어대사전, https://stdict.korean.go.kr/main/main.do
27) 국립국어원 우리말샘, https://opendict.korean.go.kr/main
28) REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in
29) 한국법제연구원(2016), 유럽연합(EU)의 전자서명 및 전자인증 법제도 동향

2-2 「신용정보법」의 본인인증

「신용정보법」의 '본인인증'에 대해서는 '금융분야 마이데이터 기술 가이드라인'[30]의 '제4장 마이데이터 본인인증' 부분에서 상세 내용을 다루고 있다.[31]

'본인인증'의 기본 원칙을 간략히 살펴보면 다음과 같다. 정보제공자(금융회사등)는 안전한 개인신용정보 전송을 위하여 고객이 개인신용정보 전송을 요구할 경우 해당 고객에 대해 반드시 본인인증을 수행하여야 한다.

[관련법령] 신용정보법 제33조의2 제8항

제33조의2(개인신용정보의 전송요구)

⑧ 제1항에 따라 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자등은 신용정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 전송요구를 거절하거나 전송을 정지·중단할 수 있다.

본인인증은 개인신용정보 전송요구의 정당성을 확인하기 위한 것으로 고객으로부터 개인신용정보 전송요구를 받은 정보제공자(금융회사등)가 수행한다. 이때 정보제공자는 안전성 및 신뢰성이 확보된 인증수단을 이용하여 고객 본인인증을 수행하여야 하고, 고객이 인증수단을 직접 소유하고 통제할 수 있어야 한다.

2-3 「전자서명법」의 인증[32]

「전자서명법」에서는 별도 '인증'에 대한 정의를 하지는 않으나, 전자서명인증 · 인증서 ·

30) 금융위원회/금융보안원, 금융분야 마이데이터 기술 가이드라인(2021.2.)

31) 본 교재에서는 본인신용정보관리업(또는 마이데이터업)에 한정하여 본인인증을 설명함

32) 과학기술정보통신부 보도자료, 전자서명제도 20여년 만에 개편, 다양한 신기술 전자서명 활성화 기반 조성 – 전자서명법 전부개정안 국회 통과(2020.5.20.)

전자서명인증업무 · 전자서명인증사업자 등 인증과 관련하여 중요한 용어를 정의하고 있으므로 관련 내용을 간략히 소개한다.

「전자서명법」은 특정 인증수단(공인인증서)의 시장독점 초래, 국민들의 인증수단 선택권 제한 등 문제점이 지속 제기되어 온 공인전자서명의 우월한 법적 효력을 폐지하여 다양한 신기술 전자서명수단 활성화 및 국민선택권 확대 등을 위해 2020년 6월 9일 전부개정되어 2020년 12월 10일부터 시행되었다.

개정된 「전자서명법」의 주요내용은 다음과 같다.[33] 전자서명수단 간 경쟁 활성화를 위하여 공인인증서 제도를 폐지하고(공인·사설인증서 구별 폐지, 공인인증서에 우월한 법적효력[34] 폐지), 다양한 전자서명수단 이용활성화와 관련하여 특정한 전자서명수단을 의무적으로 사용하도록 제한하고자 할 때에는 법률·대통령령·국회규칙 등 상위법령에 명시하도록 함으로써 하위법령(고시·부령 등)에 의한 불필요한 특정 서명수단 의무화를 방지한다. 또한 전자서명 이용자 보호 강화를 위하여 전자서명인증업무 운영기준 준수사실 인정제를 도입(제7조~제11조)하고, 전자서명 가입자 신원확인(제14조)을 도입하여 증명서를 발급받은 전자서명인증사업자는 대통령령이 정하는 바에 따른 적절한 방식의 신원확인 절차를 거쳐 전자서명 가입 업무를 수행하도록 한다.

한 가지 유념할 사항으로 핀테크 회사가 전자서명인증사업자로서 「정보통신망법」상 본인확인기관이 된 경우 고객의 신원확인 방법으로 「금융실명법」상 실명확인이 요구된다.

[관련법령] 전자서명법 제14조

제14조(신원확인)
운영기준 준수사실의 인정을 받은 전자서명인증사업자는 전자서명인증서비스에 가입하려는 자의 신원을 대통령령으로 정하는 바에 따라 확인하여야 한다.

33) 위 보도자료
34) 서명자의 서명이고, 전자문서가 전자서명된 이후 그 내용이 변경되지 않았다고 추정

[관련법령] 전자서명법 시행령 제9조

제9조(신원확인의 방법)

① 운영기준 준수사실의 인정을 받은 전자서명인증사업자가 법 제14조에 따라 전자서명인증서비스에 가입하려는 자의 신원을 확인할 때에는 다음 각 호의 구분에 따른 방법으로 한다.

1. 해당 전자서명인증사업자가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3제1항에 따른 본인확인기관(이하 "본인확인기관"이라 한다)인 경우: 「금융실명거래 및 비밀보장에 관한 법률」 제2조제4호에 따른 실지명의(이하 "실지명의"라 한다)를 기준으로 확인하는 방법. 다만, 가입하려는 자의 신원이 실지명의 기준으로 확인된 사실을 해당 전자서명인증사업자가 확인할 수 있는 경우에는 운영기준 준수사실의 인정을 받은 가입자 확인방법으로 할 수 있다.
2. 해당 전자서명인증사업자가 본인확인기관이 아닌 경우: 운영기준 준수사실의 인정을 받은 가입자 확인방법

② 제1항제1호에 따른 실지명의를 기준으로 신원을 확인하는 방법에 관한 세부적인 사항은 과학기술정보통신부령으로 정한다.

2-4 「전자금융거래법」 개정안[35]의 인증

「전자금융거래법」 개정안에서 '인증' 관련 주요내용은 다음과 같다. 2020년 12월 10일 시행된 개정 「전자서명법」에 의해 공인인증제도가 폐지됨에 따라 공인인증서를 전제로 하는 전자금융거래의 인증 관련 제도를 정비하려는 것으로, 현행법은 "접근매체"를 전자금융거래에서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단 또는 정보로 정의한다. 구체적으로는 ① 전자식카드, ② 전자서명생성정보 및 인증서, ③ 금융회사 등에 등록된 이용자번호, ④ 이용자의 생체정보, ⑤ 비밀번호 등 5가지를 열거하고 있다(제2조 제10호). 개정안은 접근매체를 "조회용"·"지시용" 및 "복합형"으로 구분하고, 현행 5가지 접근매체 중 ③ 금융회사 등에 등록된 이용자번호를 "일회성 비밀번호를 생성하는 전자적 장치 및 이에 준하는 수단·정보"로 변경하며, 그 밖에도 대통령령에서 전자금융거래의 안전성과 신뢰성이 확보될 수 있는 수단·정보로서 접근매체를 정할 수 있도록 하고 있다(안 제2조 제10호). 개정안은 전자금융거래의

35) 정무위원회 수석전문위원 이용준(2021.2.), 전자금융거래법 일부개정법률안 검토보고

편리성 · 안전성 · 보안성이 확보된 다양하고 혁신적인 인증수단이 개발·활용될 수 있도록, 특정 인증기술에 대한 차별 없이 다양한 기술이 인증수단으로 활용될 수 있도록 하고(안 제5조의2 제3항), 일정 금액 이상 온라인 거래 등 고위험 거래 시 강화된 인증방식 이용을 의무화하고 있다(안 제11조 제2항).

3 보안인증의 개념

국립국어원의 우리말샘에 따르면, '보안인증(保安認證)'이란 "인터넷 뱅킹이나 특정 사이트에 로그인을 할 때, 이용자의 아이디와 비밀번호를 통하여 접속 및 사용 허가 여부를 확인하고 증명함. 또는 그러한 일"을 의미하나 본 교재에서는 이해의 편의를 위하여 "'신원확인' 또는 '인증'을 위해 사용되는 보안기술 또는 보안절차"로 정의한다.

핀테크 회사는 「금융실명법」의 실명확인, 「정보통신망법」의 본인확인, 「신용정보법」의 본인인증, 그리고 「전자서명법」의 인증 및 「전자금융거래법」 개정안의 인증에 따라 의무적으로 사용하여야 하는 경우를 제외하고 서비스를 제공할 때 보안인증을 적용하는 데 제한은 없다. 이는 핀테크 회사가 제공하는 금융서비스의 수준과 편리성 등을 자체적으로 고려하고 판단하여 자율에 따라 보안인증을 도입하여 사용할 수 있음을 의미한다.

제2절

보안인증 종류 및 특징

1 보안인증 방식

보안인증은 그 방식에 따라 (ⅰ) 지식기반 인증, (ⅱ) 소유기반 인증, (ⅲ) 생체기반 인증으로 구분할 수 있다. (ⅰ) 지식기반 인증은 인증대상자인 본인이 알고 있는 지식(예 ID/PW, PIN, 패턴 등)을 이용하여 인증하는 방식이고, (ⅱ) 소유기반 인증은 본인이 소지한 OTP토큰(소프트웨어 방식 또는 하드웨어 기기)과 같이 별도의 매체에서 발생하는 인증 값을 이용하여 인증하는 방식이며, (ⅲ) 생체기반(또는 특징기반) 인증은 인증대상자인 본인의 생체정보인 지문이나 홍채, 정맥, 안면 등을 이용하여 인증하는 방식을 말한다(본인의 서명 패턴과 같은 경우도 포함되는 경우도 있으므로 '생체기반 인증' 대신 '특징기반 인증'이라고 불리기도 함).

〈표 Ⅰ-1〉 보안인증의 방식

구 분	내 용
지식기반 인증 (the Knowledge factors: Something the user knows)	알고 있는 지식으로 인증하는 방법 e.g., a password, partial password, pass phrase, or Personal Identification Number(PIN), challenge response (the user must answer a question, or pattern), security question
소유기반 인증 (the Ownership factors: Something the user has)	소유하고 있는(갖고 있는) 인증매체로 인증하는 방법 e.g., wrist band, ID card, security token, implanted device, cell phone with built-in hardware token, software token, or cell phone holding a software token
생체기반 인증 (the Inherence factors: Something the user is or does)	지문, 홍채 등 생체정보를 이용하여 인증하는 방법 e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier

출처: 한국은행 (2016), 바이오인증기술 최신 동향 및 정책과제

〈표 Ⅰ-2〉 보안인증의 구체적인 방법

구 분	인증 방법	
지식기반 인증	ID/PW (또는 비밀번호)	사용자와 발급자가 서로 공유한 비밀정보로 인증
	문답식 인증	발급자가 질의내용을 보여주고 사용자는 응답 값을 입력하여 인증
	이미지 인증	사용자가 사전에 선택하여 등록한 이미지를 보여주거나 다수의 이미지 중 특정 이미지를 선택하여 인증
소유기반 인증	SMS 인증	발급자는 사용자가 사전에 등록한 휴대폰번호에 인증정보가 포함된 SMS를 전송하고, 이후 사용자는 수신한 인증번호를 입력하여 인증
	ARS 인증	발급자는 사용자가 사전에 등록한 전화번호로 전화를 걸어 인증 (또는 화면에 표시된 문자를 입력하여 인증)
	OTP	발급자와 사용자가 서로 공유한 OTP 생성키를 이용하여 1회만 사용이 가능한 비밀번호를 생성 및 입력하여 인증
	그 외	계좌인증, 신분증 진위확인, IC카드 인증 등
생체기반 인증	지문/홍채/얼굴/ 정맥 인증	사용자의 생체정보인 지문, 홍채, 얼굴, 정맥 등을 추출하여 정보화한 후 등록하고 사용자가 해당 생체정보를 이용하여 인증 시 등록된 정보와 비교 인증
	그 외	영상통화 등

출처: 김신영 (2015), 전자금융거래의 사용자 인증 방법 평가 및 선택 가이드, 금융보안원 전자금융과 금융보안 제2호, 62-65

2 지식기반 인증[36)]

지식기반 인증은 본인이 알고 있는 지식이나 정보를 이용한 인증방식이며, 타 인증방식에 비해 구축비용이 적고 사용하기 편리하지만, 접속하는 곳마다 동일한 정보를 사용할 경우 하나의 시스템의 지식(비밀번호 등)이 노출되면 동일한 지식으로 설정한 다른 시스템의 보안도 무력화될 수 있고, 스마트폰에서 접속하는 앱이나 사이트의 비밀번호 들을 저장해

36) 인증 기술의 과거와 현재, 정보통신기술진흥센터(2017. 9. 20.), https://www.itfind.or.kr/publication/regular/weeklytrend/weekly/list.do?selectedId=995

둔 상태에서 스마트폰이 탈취 또는 해킹되어 정보유출사고가 발생할 경우 고객의 지식이나 정보가 악용될 수 있는 문제가 있다. 따라서 지식기반 인증방식은 간편함, 편리함의 이점이 존재하지만 보안수준은 낮은 방식이다.

지식기반 인증에서 가장 오래된 대표적인 방법은 ID/PW(또는 비밀번호)가 있다. ID(아이디, 계정)와 PW(비밀번호, 패스워드)의 입력으로 시간과 장소에 제약받지 않고 시스템에 인증(로그인)을 할 수 있는 접근성이 우수한 인증 방법이다.

〈그림 I-3〉 지식기반 인증의 사례(ID/PW 또는 비밀번호)

출처: 한국금융연수원 로그인 화면[웹사이트],
http://www.kbi.or.kr/platformWeb/Login.do?cmd=moveLogin

ID/PW 인증 방법 초기에는 비밀번호에 대한 자리 수, 문자열 조합 등의 제한 조건이 없었으나, 비밀번호를 탈취할 수 있는 해킹공격들의 등장으로 고객정보가 노출 또는 유출되는 사고가 발생되면서 비밀번호 생성에 대한 규제가 강화되었다. 대표적인 해킹공격인 무작위 대입공격(Brute Force Attack)은 비밀번호 입력란에 비밀번호로 추측되는 문자열을 변경하면서 반복 대입하는 공격이다.

〈표 Ⅰ-3〉 비밀번호 관리에 대한 법규 내용

법 규	내 용	
「전자금융거래법」 하위 규정	회사 임직원 (내부사용자)	제32조 • 숫자/영문/특수문자 혼합 8자리 이상 • 생년월일, 주민등록번호, 전화번호 사용 불가 • 5회 이내 범위에서 미리 정한 횟수 이상 입력 오류가 연속하여 발생하는 경우 비밀번호 이용에 대한 제한
	고객 (이용자)	제33조 • 주민등록번호, 동일숫자, 연속숫자 사용 불가 • 5회 이내 범위에서 미리 정한 횟수 이상 입력 오류가 연속하여 발생하는 경우 비밀번호 이용에 대한 제한
「개인정보 보호법」 하위 고시 (개인정보처리자)	제5조 제5항 및 제6항 • 비밀번호 작성규칙을 수립하여 적용 • 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 시스템에 대한 접근을 제한하는 등 필요한 기술적 조치	
「개인정보 보호법」 하위 고시 (정보통신서비스 제공자등)	제4조 제7항 및 제8항 • 비밀번호 작성규칙을 수립하여 적용 • 영문/숫자/특수문자 2종류 이상의 조합 최소 10자리 이상, 3종류 이상의 조합 최소 8자리 이상 • 연속적인 숫자, 생일, 전화번호 등 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 • 비밀번호를 반기별 1회 이상 변경	
「신용정보법」 하위 규정	[별표3] II.1.⑤ • 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 이행	

3 소유기반 인증[37)]

소유기반 인증은 본인이 별도의 인증매체를 소지하고 해당 매체에서 인증 값을 생성하여 이를 이용한 인증방식으로, 지식기반 인증에 비해 보안성은 높지만, 시스템 구축이 어렵고 편리성이 낮다는 단점이 있다. 소유기반 인증의 대표적인 방법으로는 SMS 인증, 인증서 인증, OTP 인증 등이 있다.

37) 정보통신기술진흥센터 (2017), 인증기술의 과거와 현재,
https://www.itfind.or.kr/publication/regular/weeklytrend/weekly/list.do?selectedId=995

3-1 SMS 인증

SMS(문자메시지)를 이용한 보안인증 방법은 고객이 소지하고 있는 휴대폰을 통해 전달되는 문자메시지상의 숫자를 입력하는 방법이다. 이 숫자는 제한된 시간(일반적으로 3분) 동안에만 유효하므로 해커에 의한 재사용이 어려운 보안성과, SMS를 수신할 수 있는 기기를 소유한 자는 누구든지 이용할 수 있다는 편리성이 있다.

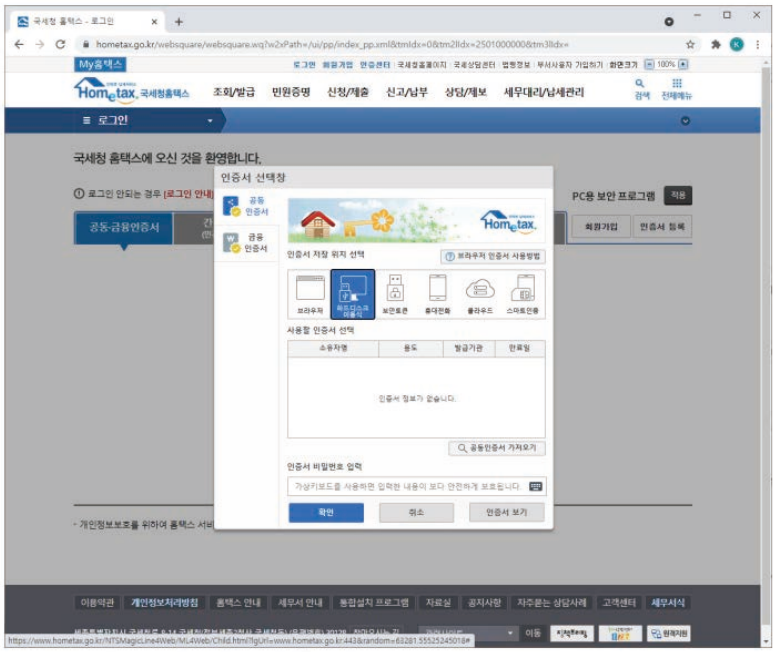
〈그림 I-4〉 SMS 인증 입력 화면

출처: LG U+ PASS 앱, 아톤(ATON)

3-2 인증서 인증

인증서란 서명이나 인감도장과 같은 역할을 하는 전자서명이 특정인에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 전자적 정보를 말한다. 인증서를 이용한 보안인증 방법은 소유기반 인증을 기초로 하고 있고, 인증서를 이용하기 위해 비밀번호를 입력해야 하므로 지식기반 인증도 포함되어 있는 방법이다. 2020년 6월 9일 「전자서명법」 전부개정을 통해 핀테크 회사에서는 인증서를 이용한 보안인증 관련 서비스를 다양하게 개발 및 운영할 수 있게 되었다.

〈그림 I-5〉 인증서 인증 화면

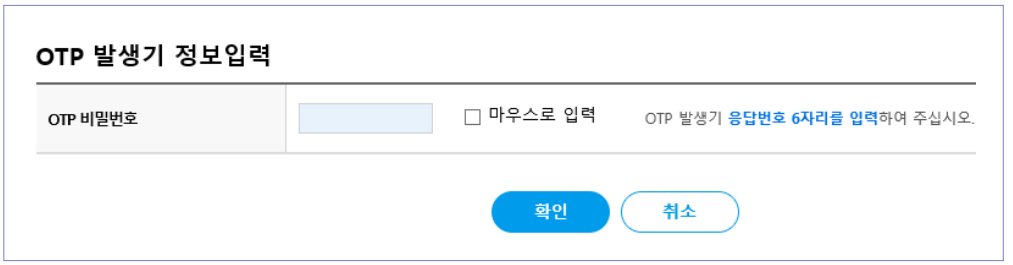


출처: 국세청홈택스 페이지[웹사이트],
Retrieved from https://www.hometax.go.kr/websquare/websquare.wq?w2xPath=/ui/pp/index_pp.xml

3-3 OTP 인증

OTP를 이용한 보안인증 방법은 OTP발생기(소프트웨어 방식 또는 하드웨어 기기)에서 생성된 임의의 숫자 값을 입력하여 본인을 인증하면 된다. OTP발생기에서 생성된 숫자는 1회만 사용이 가능하고 한 번 사용된 생성 값은 재사용이 불가능하다. 기존 비밀번호를 이용한 인증 방법의 경우 일정기간(예 3개월) 동안 변경하지 않고 사용되어 해커에게 노출될 가능성이 있고, 인증서 인증 방법의 경우 인증서가 유출되어 악용되는 사고 등이 있을 수 있으나 OTP 인증의 경우 이러한 단점을 어느 정도 해결할 수 있어 OTP를 이용한 보안인증 방법은 최근 들어 많이 활성화되고 있다.

〈그림 1-6〉 OTP 인증 화면



출처: 우리은행 로그인 페이지[웹사이트]
Retrieved from https://spib.wooribank.com/pib/Dream?withyou=PSTRS0008&__STEP=1

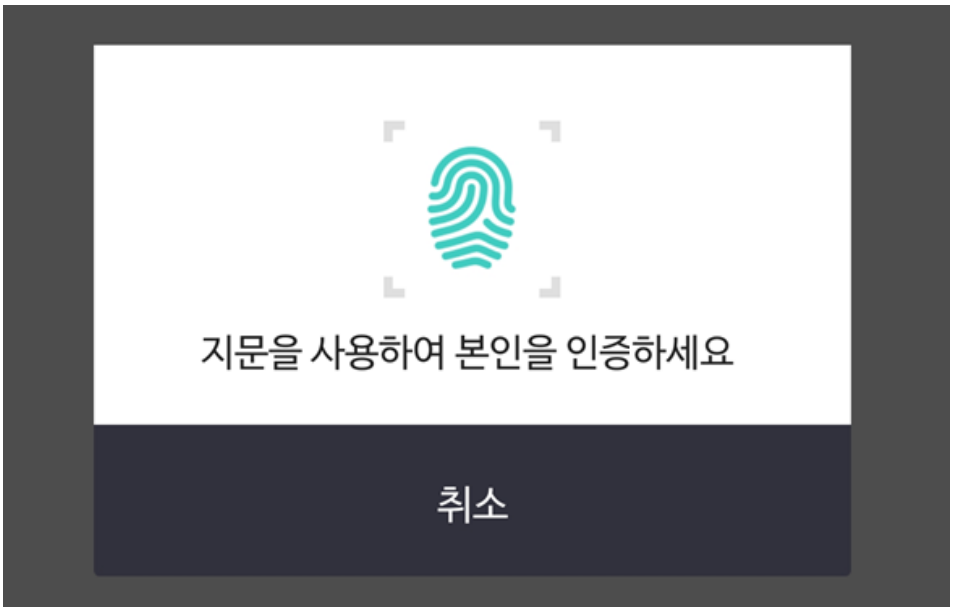
4 생체기반 인증[38)]

생체기반 인증은 본인의 생체정보인 지문이나 홍채, 얼굴, 정맥 등을 이용해 인증하는 방식으로 고객의 '존재 자체'를 이용하므로 편리성이 높지만, 생체정보가 훼손되거나 유출이 되면 교체가 어려우며, 시스템 구축이 어렵고 외부 환경에 따라 인식하는 정도에 다소 차이가 있을 수 있다는 단점이 있다. 대표적으로 스마트폰상에서의 지문 인증, 홍채 인증, 안면 인증 등이 있다.

생체기반 인증방식은 개인의 생체정보(Biometric Information)를 인식할 수 있는 장치를 통해 특징을 추출하여 정보화하여 저장하고 이 후 입력되는 정보와 저장된 정보를 비교함으로써 인증하는 형식이다. 이를 실행하기 위해서는 인증 시 사용 가능한 생체정보로서의 자격은 타인과 중복되지 않는 고유성을 갖고 있어야 함에 따라 이러한 이유로 개인의 지문, 홍채, 얼굴, 정맥 등이 사용된다. 생체인증은 스마트폰 기기의 발전과 편리한 금융서비스를 이용하고자 하는 트렌드의 변화로 적용범위가 계속 확대되고 있다.

38) 정보통신기술진흥센터 (2017), 인증 기술의 과거와 현재,
https://www.itfind.or.kr/publication/regular/weeklytrend/weekly/list.do?selectedId=995

〈그림 I-7〉 생체인증(지문) 화면



출처: 로그인 화면[모바일앱], 하나은행 1Q 앱

핵심정리

1. 보안인증 개념

- 신원확인
  - '신원확인(身元確認)'이란 "어떤 사람이 제공한 신상 정보가 맞는지를 확인하는 일"을 의미한다.
  - 국내의 신원확인 관련 규제로는 금융거래에 적용되는 「금융실명법」의 실명확인과 온라인거래에 적용되는 「정보통신망법」의 본인확인이 있고, 최근 논의가 활발히 진행되고 있는 「전자금융거래법」 개정안의 신원확인이 있다.

- 인증
  - '인증(認證)'이란 "어떠한 문서나 행위가 정당한 절차로 이루어졌다는 것을 공적 기관이 증명함" 또는 "네트워크나 서버에 접속할 때, 본인 여부와 정규 이용자 여부를 확인하는 방법. 일반적으로 사용자 아이디(ID)와 패스워드의 조합으로 본인을 특정함. 인증이 이루어지면 사용자가 가진 권한에 따라 데이터에 접근하거나 응용 소프트웨어를 이용할 수 있음"을 의미한다.
  - 국내의 '인증' 관련 규제로는 「신용정보법」의 본인인증과 「전자서명법」의 인증이 있고, 최근 논의가 활발히 진행되고 있는 「전자금융거래법」 개정안의 인증이 있다.

- 보안인증
  - '보안인증(保安認證)'이란 "인터넷 뱅킹이나 특정 사이트에 로그인을 할 때, 이용자의 아이디와 비밀번호를 통하여 접속 및 사용 허가 여부를 확인하고 증명함. 또는 그러한 일"을 의미하나 본 교재에서는 이해의 편의를 위하여 "'신원확인' 또는 '인증'을 위해 사용되는 보안기술 또는 보안절차"로 정의한다.

- 핀테크 회사는 「금융실명법」의 실명확인, 「정보통신망법」의 본인확인, 「신용정보법」의 본인인증, 그리고 「전자서명법」의 인증 및 「전자금융거래법」 개정안의 인증에 따라 의무적으로 사용하여야 하는 경우를 제외하고 서비스를 제공할 때 보안인증을 적용하는 데 제한은 없다. 이는 핀테크 회사가 제공하는 금융서비스의 수준과 편리성 등을 자체적으로 고려하고 판단하여 자율에 따라 보안인증을 도입하여 사용할 수 있음을 의미한다.

2. 보안인증 종류 및 특징

- **보안인증 방식**
  - 보안인증은 방식에 따라 지식기반 인증, 소유기반 인증, 생체기반 인증으로 구분할 수 있다. 지식기반 인증은 본인이 알고 있는 지식을 이용하고, 소유기반 인증은 본인이 소유하고 있는 매체를 이용하며, 생체기반 인증은 본인의 생체정보를 이용한 인증을 말한다.

- **지식기반 인증**
  - 지식기반 인증은 본인이 알고 있는 지식이나 정보를 이용하여 인증하는 방식으로 인증의 간편함과 편리함이 장점이나, 동일한 지식을 이용할 경우 노출에 대한 위험성이 있다. 지식기반 인증 방법으로는 ID/PW, 문답식 인증, 이미지 인증 등이 있다.

- **소유기반 인증**
  - 소유기반 인증은 본인이 별도의 인증매체를 소지하고 해당 매체에서 인증 값을 생성하여 이를 이용한 인증방식으로 지식기반 대비 보안성은 높으나 편리성이 낮고 구축이 어렵다는 단점이 있다. 소유기반 인증 방법으로는 SMS 인증, 인증서 인증, OTP 인증 등이 있다.

- 생체기반 인증
  - 생체기반 인증은 본인의 생체정보인 지문이나 홍채, 얼굴, 정맥 등을 이용해 인증하는 방식으로 '존재 자체'를 이용하기 때문에 편리성은 높으나 생체정보의 훼손 또는 저장된 생체정보 값이 유출될 경우 교체가 어려운 단점이 있다. 생체기반 인증 방법으로는 지문 인증, 홍채 인증, 얼굴 인증, 정맥 인증 등이 있다.

헬로, 핀테크!(보안인증 · 블록체인)

2장

보안인증기술의 이해

제1절 보안인증의 핵심기술

제2절 보안인증기술 사례 (인증서)

제3절 보안인증기술 사례 (생체정보)

제4절 보안인증기술 사례 (분산ID)

2장 보안인증기술의 이해

학습목표

1. 보안인증을 위한 핵심기술이 무엇인지 이해하고 설명할 수 있다.
2. 보안인증기술의 종류 및 특징을 구분하고 이해할 수 있다.

학습개요

보안인증을 위한 기반기술로는 암호기술, 해시함수, 블록체인 등이 있으며, 이러한 기반기술을 활용한 다양한 보안인증기술이 존재한다. 이 장에서는 보안인증의 핵심기술에는 무엇이 있는지, 어떠한 보안인증의 종류와 특징이 있는지에 대해 개괄적으로 알아본다.

용어해설

❶ 부인방지(否認防止, Non-repudiation)

메시지의 송수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실 부인을 방지하는 보안기술을 말한다.

❷ 해시함수(Hash Function)

입력 메시지의 길이와는 무관하게 출력 메시지는 항상 고정된 길이를 갖는 데이터 변환 함수(단, 해시 알고리즘에 따라 고정된 길이는 달라짐)를 의미한다.

❸ 블록체인

네트워크 참여자가 보관하고자 하는 정보와 이 정보의 해시 값을 저장 · 공유함으로써 정보의 신뢰성을 확보하도록 설계된 분산형 장부로서, 생성된 순서대로 블록(정보 저장 단위)을 연결하는 과정에서 유효성을 검증함으로써 정보의 위 · 변조를 방지할 수 있는 기술을 말한다.

제1절

보안인증의 핵심기술

1 암호기술(대칭키 vs 공개키)

암호기술이란 정보보안의 목적 중 정보의 기밀성 또는 무결성 등을 보장하는 기술이다. 암호기술에서 일반적으로 사용되는 용어로는 암호화 또는 복호화, 암호 알고리즘, 키(Key) 등이 있으며, 암호화는 암호 알고리즘과 키를 이용하여 사람이 인식할 수 있는 평문을 암호문으로 변환하는 것을 의미하고, 복호화는 암호 알고리즘과 키를 이용하여 암호문을 평문으로 변환하는 것을 의미한다. 이 과정에서 암호화와 복호화에 사용된 키가 동일한 경우 대칭키 암호기술이라고 하고, 동일하지 않는 경우 비대칭키(또는 공개키) 암호기술이라고 한다. 암호 알고리즘은 수학이론을 기반으로 만들어지고, 공개된 암호 알고리즘에 대해 키가 없는 상태에서 암호문을 평문으로 변환하는 과정을 해독이라고 하며, 해독에 소요되는 시간이 현재의 컴퓨팅기술을 기준으로 향후 몇 년 또는 몇 십 년 동안 소요되는가에 따라 안전성을 판단하여 실무에서 선택하여 사용한다.

대칭키 암호기술과 공개키 암호기술의 가장 큰 차이점은 앞서 설명한 바와 같이 키를 사용하는 방식(동일한 키 또는 다른 키)에 있다. 그리고 대칭키 암호기술은 정보의 기밀성에 중점을 둔 것이라면, 공개키 암호기술은 정보의 기밀성뿐만 아니라 무결성, 부인방지, 인증 등의 보안성도 적용할 수 있는 조금 더 범용적인 암호기술이다. 다만 암 · 복호화의 속도 측면에서 보면 한 개의 키를 이용하는 대칭키 방식이 공개키 방식에 비해 빠르기 때문에 암호기술을 구현하기 위해서는 상황과 환경에 맞는 방식을 선택하는 것이 중요하다.

따라서 핀테크 회사가 고객에게 금융서비스를 제공함에 있어 기반 인프라(시스템, 네트워크 등)를 어떻게 구성하느냐에 따라 보안성, 효율성, 경제성 등을 고려하였을 때 어떤 암호기술이 적합한지를 선택하는 것이 중요하다.

〈표 II-1〉 암호기술의 비교

구분	대칭키 기반	공개키 기반	
키 방식	단일(1개) (암호화 키 = 복호화 키)	한 쌍(2개) (암호화 키 ≠ 복호화 키)	
안전한 키 길이[39]	112bit	인수분해	2048bit
		이산대수	공개키: 2048bit 비밀키: 224bit
		타원곡선	224bit
암호화 키 속성	비밀	공개	
복호화 키 속성	비밀	비밀	
비밀키 전송	단일 키이므로 상대에게 전달해야 함	키 전달이 불필요	
키 개수	N(N-1)/2	2N	
암·복호화 속도	빠름	느림	
경제성	좋음	나쁨	
주요 적용 영역	데이터 암호화	통신 암호화, 전자서명	
적용 보안성	기밀성	기밀성, 무결성, 부인방지, 인증	
전자서명	복잡함	간단함	
단점	키 교환의 문제	MITM[40] 공격에 취약	
대표 알고리즘	AES, 3-DES, SEED, HIGHT	RSA, DH, ElGamal	

출처: 조현준 (2018), 2018 정보보안기사 & 산업기사, 탑스팟

2 해시함수

해시함수(Hash Function)는 입력 메시지의 길이와는 무관하게 출력 메시지는 항상 고정된 길이를 갖는 데이터 변환 함수(단, 해시 알고리즘에 따라 고정된 길이는 달라짐)를 의미하며,

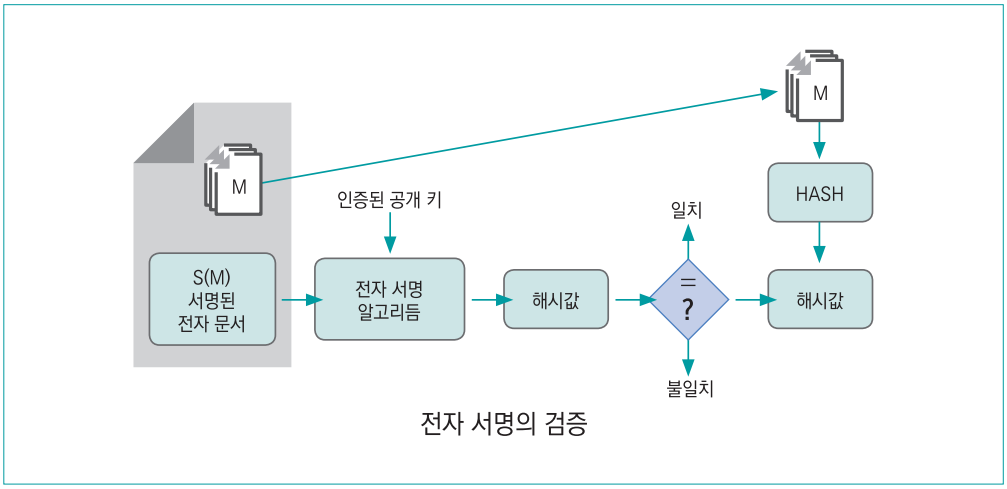
39) 한국인터넷진흥원(2018), 암호 알고리즘 및 키 길이 이용 안내서, 과학기술정보통신부/한국인터넷진흥원

40) MITM(Man In The Middle) 공격은 네트워크 통신을 조작하여 공격자가 통신 내용을 도청하거나 수정하는 공격 기법이다. https://ko.wikipedia.org/wiki/중간자_공격

단방향으로만 데이터를 변환할 수 있는 특징을 갖고 있다. 일반적으로 암호 알고리즘이라 함은 암 · 복호화 시 특정 키를 이용하는데 이에 반해 해시함수는 암 · 복호화에 대한 키 값이 존재하지 않아 흔히 말하는 암호기술이라고 보기 어려울 수 있으나, 「정보통신망법 시행령」 제15조 제4항의 암호조치와 관련된 내용을 보면 해시함수를 '일방향 암호화'라고 명시하고 있어 국내 법규에서는 해시함수를 암호기술 중 하나로 인정하고 있다. 대표적으로 해시함수는 지식기반 인증방식의 하나인 ID/PW(또는 비밀번호)에서 비밀번호가 저장될 때 사용된다. 즉, 사용자는 최초 비밀번호(A)를 등록하게 되는데, 이 비밀번호(A)는 해시함수를 통해 만들어진 결과 값(A의 해시 값) 형태로 저장된다. 이후 인증을 위해 사용자가 비밀번호(B)를 입력하면 이 비밀번호(B)는 해시함수를 통해 결과 값(B의 해시 값)이 생성되고 최초 등록된 비밀번호의 결과 값(A의 해시 값)과 비교하는 방식으로 인증을 수행하게 된다. 이러한 방식은 시스템 관리자라 하더라도 사용자의 비밀번호를 알 수 없고 해킹을 통해 시스템에 저장된 비밀번호의 결과 값이 유출되더라도 비밀번호를 예측할 수 없기 때문에 정보보안 측면에서 안전하다.

또한 이러한 해시함수는 전자문서 형태로 존재하는 정보가 인터넷 등의 정보통신망을 통해 상대방으로 전달되었을 때 전자문서의 무결성을 확인하는 목적으로 많이 사용된다.

〈그림 Ⅱ-1〉 해시함수를 이용하여 전자 서명을 검증하는 방법



출처: 한국정보통신기술협회 정보통신용어사전[웹사이트],
Retrieved from https://terms.tta.or.kr/main.do

3 블록체인

블록체인은 PKI(공개키기반구조, Public Key Infrastructure) 구조를 토대로 분산ID와 같은 사설인증체계에 활용되고 있다는 점에서 보안인증의 핵심기술의 하나로 볼 수 있다. 블록체인이란 네트워크 참여자가 보관하고자 하는 정보와 이 정보의 해시 값을 저장 · 공유함으로써 정보의 신뢰성을 확보하도록 설계된 분산형 장부로서, 생성된 순서대로 블록(정보 저장 단위)을 연결하는 과정에서 유효성을 검증함으로써 정보의 위 · 변조를 방지할 수 있는 기술이다. 블록체인은 참여제한 여부에 따라 개방형과 폐쇄형으로 구분되며, 개방형은 다수 · 익명의 사용자가 참여하므로 고도의 암호화가 필요(예 가상자산 거래시스템)한 블록체인이고, 폐쇄형은 식별된 사용자 즉, 이해관계자만 참여하고 데이터가 공유되도록 서비스를 구성해야 할 때 적합하다. 폐쇄형은 소수 참여자의 합의로 운영되는 컨소시엄(예 R3CEV)과 하나의 중앙기관이 운영하는 Private 블록체인(예 美 나스닥 비상장주식거래 플랫폼)으로 구분될 수 있다. 블록체인에 대해서는 '제6장 블록체인 개요'에서 상세 내용을 다루고 있다.

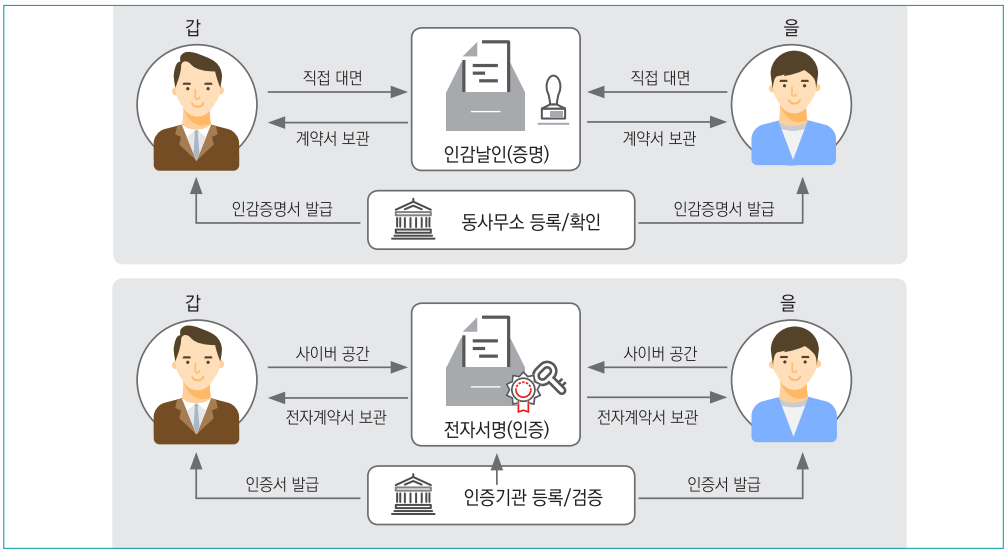
제2절

보안인증기술 사례 (인증서)

1 개요

인증서는 서명이나 인감도장과 같은 역할을 하는 전자서명이 특정인에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 전자적 정보로서 전자서명의 검증에 필요한 공개키에 소유자 정보를 추가하여 만든 일종의 전자 신분증(증명서)으로 인터넷 뱅킹, 전자 민원(G4C; Government for Citizen), 전자 입찰, 인터넷 주택 청약 등에서 신원확인 수단으로 사용되고 있으며, 특정 홈페이지의 로그인 수단으로도 활용되고 있다.[41)]

〈그림 II-2〉 인감과 전자서명의 비교 개념도



출처: 조휘갑 (2002), 전자서명 이용방법 안내, 한국정보보호진흥원

41) 한국정보통신기술협회 정보통신용어사전

2 기술 구성방식

인증서는 PKCS#11(Public Key Cryptography Standards)[42] 인터페이스인 공개키 기반구조(Public Key Infrastructure)로 구성되어 있으며, 이를 PKI구조라고 한다. 이론상으로 PKI구조에서는 공개키와 개인키인 비대칭키 형태로 인증서 발급 시 공개키와 개인키 한 쌍이 생성된 후, 인증기관에는 공개키가, 이용자에게는 개인키와 인증서 파일 형식의 공개키가 발급된다. 이용자는 인증서 파일을 이동식 저장장치(USB 등)에 소지하고 다닐 수 있어 소유기반의 인증 방법이라고 할 수 있으며, 최근에는 클라우드 저장소 등에 저장이 가능하여 별도의 저장매체를 소지하지 않아도 보안인증을 할 수 있다.

인증서 내에는 가입자의 전자서명 검증키, 일련번호, 소유자이름, 유효기간 등의 정보를 포함하고 있어 인증서는 거래 당사자의 신원 확인은 물론 문서의 위 · 변조 방지, 거래사실의 부인 방지 등의 기능을 가진다.

인증서의 대표적인 적용 사례로는 전자서명(Digital Signature)이 있다. 전자서명이란 암호기술과 해시함수 등을 사용하여 정보를 주고받는 양 당사자 사이에서 (i) 상대방에 대한 신원확인, (ii) 정보의 무결성 확인, (iii) 정보 송수신에 대한 증명을 위해 사용되는 개념이다. 핀테크 회사는 고객과 비대면 방식으로 회원가입과 금융서비스를 제공함에 있어 추후 고객과 법적 분쟁, 금융사고, 부인방지 등을 위한 목적으로 전자서명 개념을 적용할 수 있다.

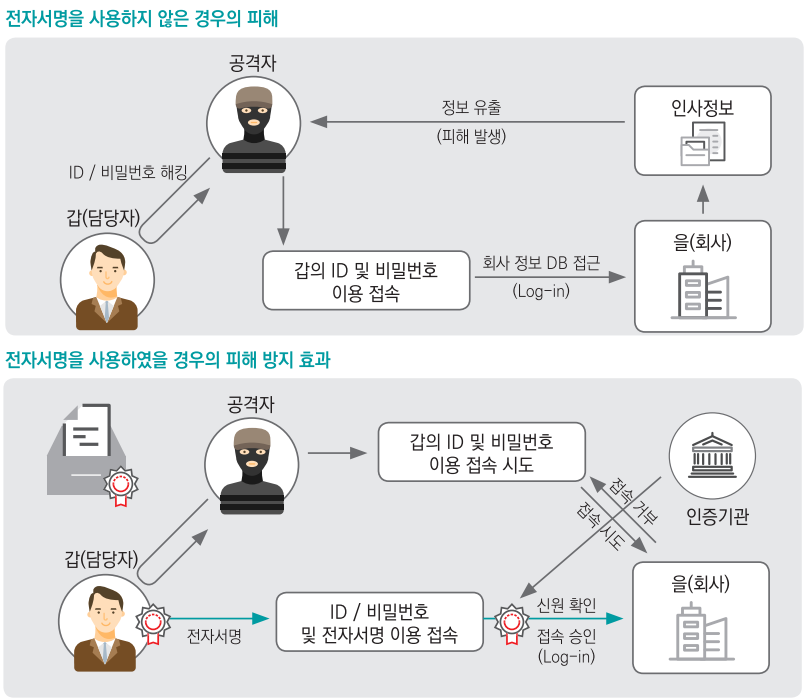
---

42) 미국 기업 RSA가 제시한 공개키 암호 표준의 암호 토큰에 대한 응용프로그램 인터페이스를 정의한 표준으로 보안토큰 API라고도 한다. https://ko.wikipedia.org/wiki/공개_키_암호_표준

2-1 상대방에 의한 신원확인

'갑'이 자신의 개인키를 이용하여 전자서명을 하여 '을'에게 전달하고 '을'은 '갑'의 공개키를 이용한 전자서명 검증으로 '갑'의 신원을 확인할 수 있다.

〈그림 Ⅱ-3〉 신원확인 개념도

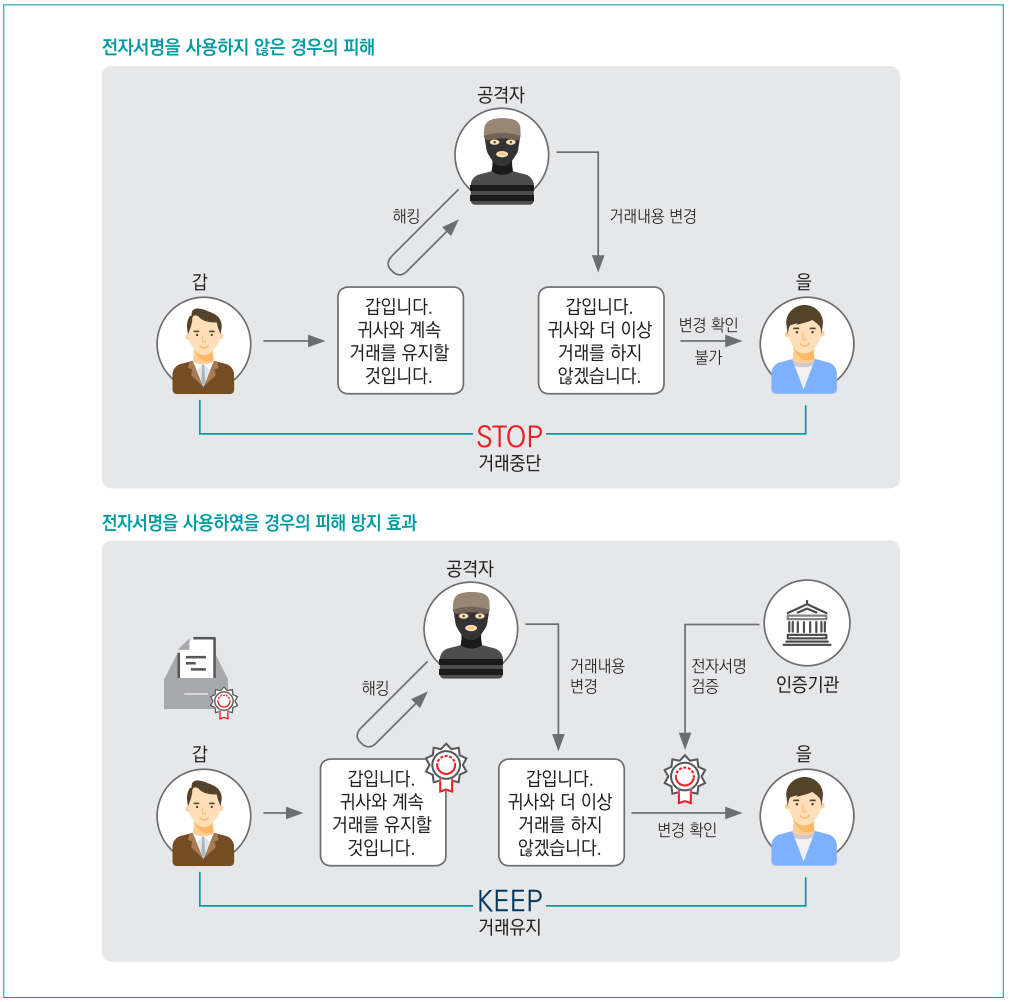


출처: 조휘갑 (2002), 전자서명 이용방법 안내, 한국정보보호진흥원

2-2 정보의 무결성 확인

공격자가 해킹 등을 통해 '갑'의 송신정보를 가로채 내용을 변조하여 '을'에게 보내더라도 '을'은 '갑'의 공개키로 전자서명을 검증하여 정보가 변경된 사실을 쉽게 확인할 수 있다.

〈그림 II-4〉 정보의 변경 확인 개념도

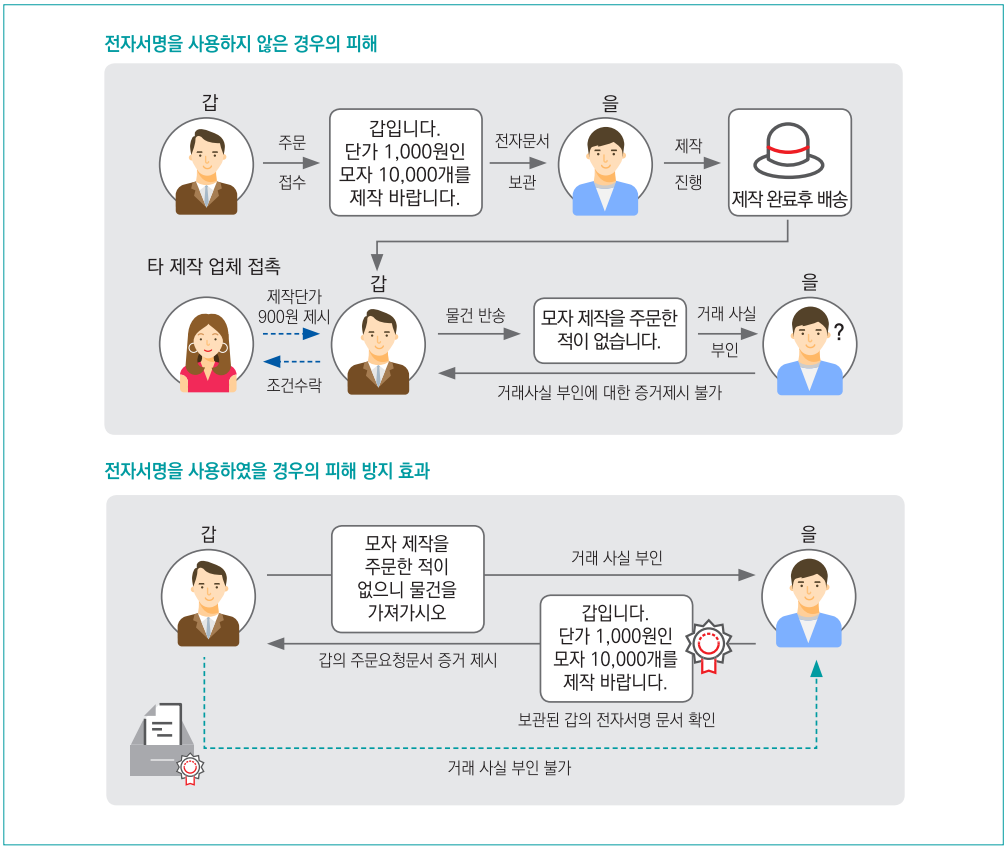


출처: 조휘갑(2002), 전자서명 이용방법 안내, 한국정보보호진흥원

2-3 정보 송수신에 대한 증명

'갑'이 송신한 정보에 대한 부인을 하는 문제가 발생하였을 경우, '을'은 '갑'이 송신한 전자문서를 '갑'의 공개키로 전자서명 검증을 하여 정보 송수신 사실을 증명할 수 있다.

〈그림 Ⅱ-5〉 정보 송수신에 대한 증명 개념도



출처: 조휘갑(2002), 전자서명 이용방법 안내, 한국정보보호진흥원

3 적용사례 등[43)]

대표적인 사례로 국세청홈택스에서 제공하는 로그인 기능 중 '인증서 로그인'이 있다. 국세청홈택스에서는 인증서 로그인으로 (ⅰ) 간편인증 로그인, (ⅱ) 금융인증서 로그인, (ⅲ) 공동인증서 로그인과 같이 3가지 방식을 제공한다.

3-1 간편인증 로그인 방식

카카오, 통신사PASS, 한국정보인증(삼성PASS), KB국민은행, NHN 페이코와 같은 민간전자서명 사업자가 제공하는 전자서명을 이용하여 홈택스에 로그인할 수 있도록 제공하는 방식을 말하며, 주민등록번호로만 로그인 가능하고, 사업자등록번호로는 로그인할 수 없다.

간편인증 방식을 이용한 국세청홈택스 로그인 방법은 '(1) 로그인 화면: 간편인증 로그인 버튼 선택 → (2) 간편인증 로그인: 카카오, 통신사PASS 등 이용하고자 하는 민간전자서명 사업자 선택 → (3) 전자서명 인증: 지문, PIN번호 등 전자서명 비밀번호 확인 → (4) 로그인 완료: 홈택스 로그인 완료' 단계로 진행된다.

〈그림 Ⅱ-6〉 국세청홈택스 '간편인증 로그인' 방식 화면

출처: 국세청홈택스 내 '인증서 로그인 안내' 페이지,
https://www.hometax.go.kr/websquare/websquare.wq?w2xPath=/ui/pp/index_pp.xml

43) 국세청홈택스 내 '인증서 로그인 안내' 페이지, https://www.hometax.go.kr/websquare/websquare.wq?w2xPath=/ui/pp/index_pp.xml

3-2 금융인증서 로그인 방식

은행에서 발급한 금융인증서를 금융결제원(舊 공인인증기관)의 클라우드에 저장하고, 저장된 금융인증서를 이용하여 국세청홈택스에 로그인할 수 있도록 제공하는 방식을 말한다.

금융인증서 로그인 방식을 이용한 국세청홈택스 로그인 방법은 '(1) 로그인 화면: 공동 · 금융인증서 로그인 버튼 선택 → (2) 공동 · 금융인증서 로그인: 인증서 선택창(좌측 상단)에서 "금융인증서" 선택 → (3) 금융인증서 인증: 지문, PIN번호 등 금융인증서 비밀번호 확인 → (4) 로그인 완료: 홈택스 로그인 완료' 단계로 진행된다.

참고로, 금융인증서를 등록하는 방법은 '(1) 인증센터: 인증센터(홈택스 상단) 버튼 선택 → (2) 공동 · 금융인증서 등록: 공동 · 금융인증서 등록메뉴 선택 → (3) 금융인증서 인증: 인증서 선택창(좌측 상단)에서 "금융인증서"를 선택한 후 지문, PIN번호 등 금융인증서 비밀번호 확인 → (4) → 등록 완료: 금융인증서 등록 완료' 단계로 진행된다.

3-3 공동인증서(구 공인인증서) 로그인 방식

전자서명법 시행에 따라 (舊)공인인증서는 공동인증서로 명칭이 변경되었고, 기존에 사용하던 (舊)공인인증서와 동일한 방법으로 홈택스에 로그인할 수 있다.

〈그림 Ⅱ-7〉 국세청홈택스 '공동·금융인증서 로그인' 방식 화면

출처: 국세청홈택스 내 '인증서 로그인 안내' 페이지,
https://www.hometax.go.kr/websquare/websquare.wq?w2xPath=/ui/pp/index_pp.xml

제3절

보안인증기술 사례 (생체정보)

1 개요

「개인정보 보호법」 하위 고시(개인정보처리자) 및 「개인정보 보호법」하위 고시(정보통신서비스 제공자등)에서는 '생체정보 및 생체인식정보'를 정의하고 있으며, 사람의 신체적 또는 행동적 특징을 입력장치를 통해 최초로 수집되어 가공되지 않은 '생체인식정보 원본정보'와 그중 특정 알고리즘을 통해 특징만을 추출하여 생성된 '생체인식정보 특징정보'로 구분하기도 한다고 설명하고 있다.[44)]

[관계법령] 「개인정보 보호법」 하위 고시(개인정보처리자) 제2조 제16호 및 제16의2호

"생체정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

[관계법령] 「개인정보 보호법」 하위 고시(정보통신서비스 제공자등) 제2조 제8호 및 제8의2호

"생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

생체기반 인증방식의 편리성과 생체정보를 통한 인증방식이 탑재된 스마트폰의 대중화로 최근 들어 생체정보를 활용한 보안인증기술이 가장 많이 사용되고 있다.

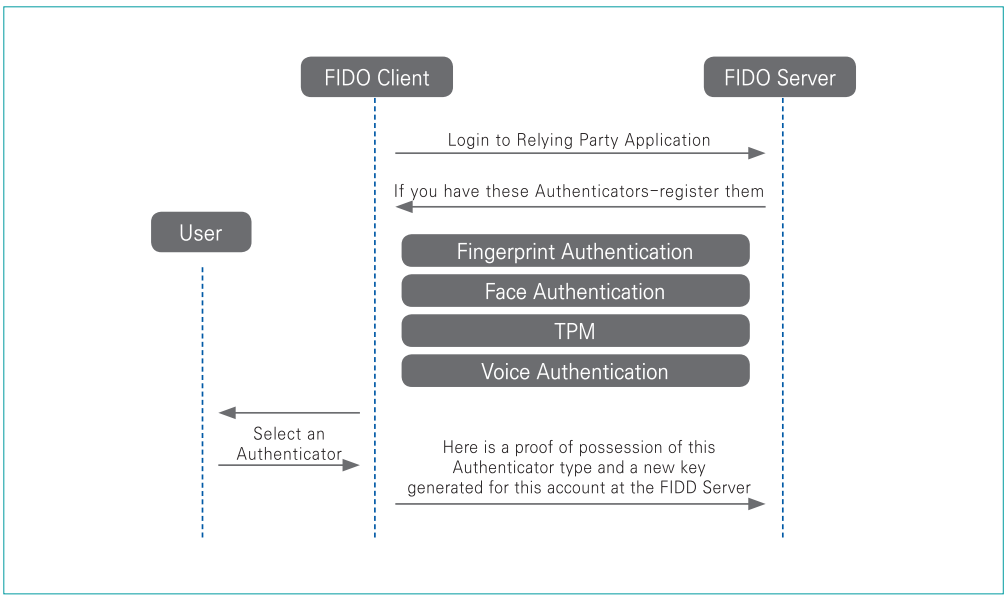
44) 「생체정보 보호 가이드라인」 본문 4면

2 기술 구성방식

생체기반 인증방식의 대표적인 방법으로는 FIDO(Fast IDentity Online)기술이 있으며, 이 FIDO기술은 FIDO Alliance가 발표한 기술로 사실상(De-facto) 기술 표준으로 인정된다.

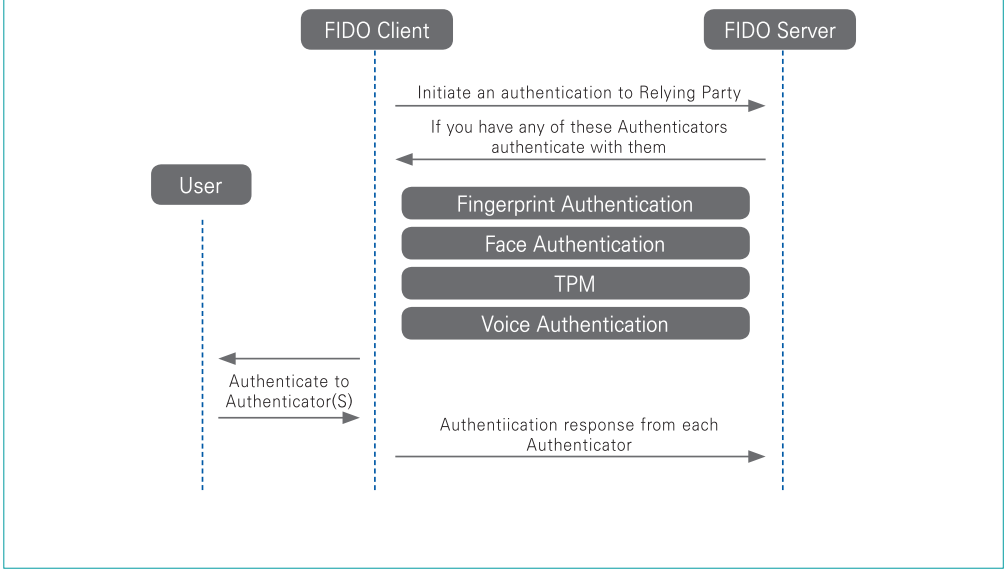
FIDO기술을 이용하는 과정을 간략히 설명하면, 고객은 본인이 소유한 장치(예 스마트폰)를 통해 핀테크 회사의 금융서비스를 이용하기 위한 본인의 정보를 등록한다. 이 등록과정에서 핀테크 회사는 고객에게 고유의 값(또는 인증서)을 부여한다(이 정보는 스마트폰의 안전한 영역에 저장되어 관리됨). 이후 고객이 생체인증을 통해 스마트폰에서 정상 여부가 판단되어 정상일 경우에 한하여 핀테크 회사가 등록과정에서 고객에게 부여한 고유의 값을 핀테크 회사의 시스템에 전달되게 함으로써 고객에 대한 보안인증이 이루어진다.

〈그림 Ⅱ-8〉 FIDO 등록과정



출처: 조상래 외, "패스워드 없는 인증기술-FIDO", 전자통신동향분석, 29권 4호, 2014, 공공누리 제4유형

〈그림 Ⅱ-9〉 FIDO 인증과정



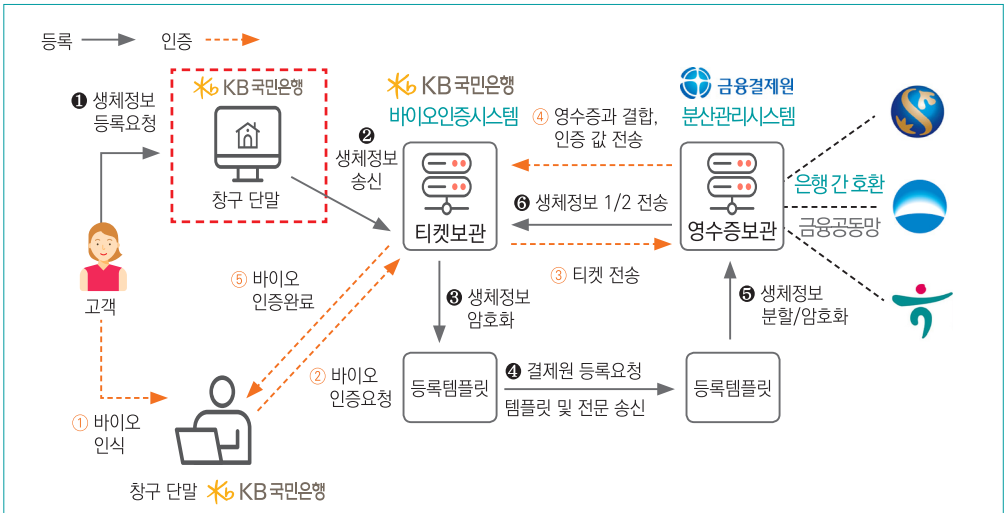
출처: 조상래 외, "패스워드 없는 인증기술-FIDO", 전자통신동향분석, 29권 4호, 2014, 공공누리 제4유형

3 적용 사례 등

2019년 4월 15일 KB국민은행은 금융결제원과 공동으로 정맥인증을 통한 은행거래 서비스를 제공한다고 발표하였다.[45] 이 서비스에서 고객의 생체정보는 개별적으로 사용할 수 없는 2개의 조각으로 정보가 분할되며, 하나는 금융회사, 하나는 금융결제원의 분산관리센터에 분산 보관된다. 2개의 정보로 분할하는 비율은 금융회사마다 상이하게 선택 가능(5:5, 6:4 등)하며, 고객이 실질적인 은행거래를 할 경우에만 분할된 2개의 생체정보를 결합하여 은행거래에 사용되므로 고객의 개인정보를 보호하면서 고객의 생체정보가 안전하게 관리될 수 있다.

45) 금융위원회 보도자료, 정맥인증 서비스로 은행거래가 편리해집니다!-금융위원회의 적극적인 유권해석으로 금융혁신 노력을 뒷받침- (2019.4.15.)

〈그림 Ⅱ-10〉 정맥인증을 통한 은행거래 서비스 사례



- 등록템플릿 : 은행에 등록하는 생체정보에서 특장점을 추출한 암호화 문자파일
- 티켓: 생체정보를 분할하여 은행에 보관되는 1/2 조각
- 영수증: 생체정보를 분할하여 결제원에 보관되는 1/2 조각

출처: 금융위원회 (2019), 정맥인증 서비스로 은행거래

생체기반 인증과 관련하여 최근 「금융혁신지원 특별법」에 따라 혁신금융서비스로 지정된 “얼굴만으로 결제하는 안면인식결제 서비스(신한카드)”,[46] “안면인식기술 활용 비대면 실명확인 서비스(DGB대구은행)”,[47] “안면인식기술을 활용한 비대면 계좌개설 서비스(하나은행)”[48] 사례가 있다.

46) 금융위원회 보도자료, 혁신금융서비스 3건 지정(2021.5.26.)
47) 위 보도자료
48) 금융위원회 보도자료, 혁신금융서비스 3건 지정(2021.4.14.)

제4절 보안인증기술 사례 (분산ID)[49) 50)]

1 개요

분산ID는 프라이버시의 강화와 개인정보 유출 위협 대응, 인증정보 관리의 불편함 등으로 인해 새로운 신원관리체계가 요구되어 등장하게 되었다. 분산ID는 대부분 온라인상에서 컨소시엄/프라이빗 분산원장을 기반으로 사용자 스스로 이름/나이/고유식별정보/인증정보 등 신원에 대한 증명을 관리하고 신원정보 제출 범위 및 제출대상 통제 등을 수행할 수 있도록 하는 신원관리체계를 말한다. 전통적인 신원관리체계와는 다르게 '정보주체'가 자신의 신원정보에 대한 주권(스스로 결정할 수 있는 권리) 행사가 가능하다. 그리고 신뢰된ID저장소를 이용하여 분산ID에 참여하는 참여자는 신원정보의 위·변조 여부 검증이 가능하다.

〈표 II-2〉 분산ID 등장 배경

구 분	설 명
프라이버시 강화	유럽연합(EU)의 GDPR, 미국의 소비자 프라이버시 권리장전 등 개인의 데이터 주권 강화 정책 수립 및 시행 중
개인정보의 유·노출 위협	서비스 제공기관마다 사용자의 신원정보 관리 시 해킹 등 전자적 침해에 따른 대량의 개인정보 유·노출 사고 발생 가능
인증정보 관리 불편	사용자 입장에서 개별 서비스마다 인증정보를 다르게 설정 및 관리하는 것에 대한 한계 (크리덴셜 스터핑 공격 대응)

출처: 전자부품연구원 블록체인사업단 김현식 단장(2019), 지능정보통신 VOL.20, 한국정보통신학회

49) 금융보안원 보안기술연구팀 (2019), 전자금융과 금융보안 제16호, pp.15-36, 금융보안원

50) 중앙등록 메커니즘 없이 신뢰된 분산 프레임워크하에서 활용되는 신원정보 체계(출처: 분산ID를 활용한 금융권 신원관리 프레임워크, 금융보안원)

분산ID의 특징으로는 자신의 신원정보를 지속적으로 사용 가능하다는 '지속성', 기존의 서버-클라이언트 모델과는 달리 신원정보의 발행 및 검증이 특정기관에 종속적이지 않는 피어(PEER) 기반의 '독립성', 신원증명이 필요하면 언제든 스스로 신원정보를 선택 후 제공할 수 있는 '휴대성', 개인의 명시적 동의 없이는 서비스제공자의 개인정보 활용 등이 제한되는 개인정보 보호와 금융권에서 보증하는 신뢰 수준을 요구하는 디지털 신원확인의 확대요구로 다양한 영역에 확대가 가능한 '확장성'이 있다.

〈표 II-3〉 분산ID 특징

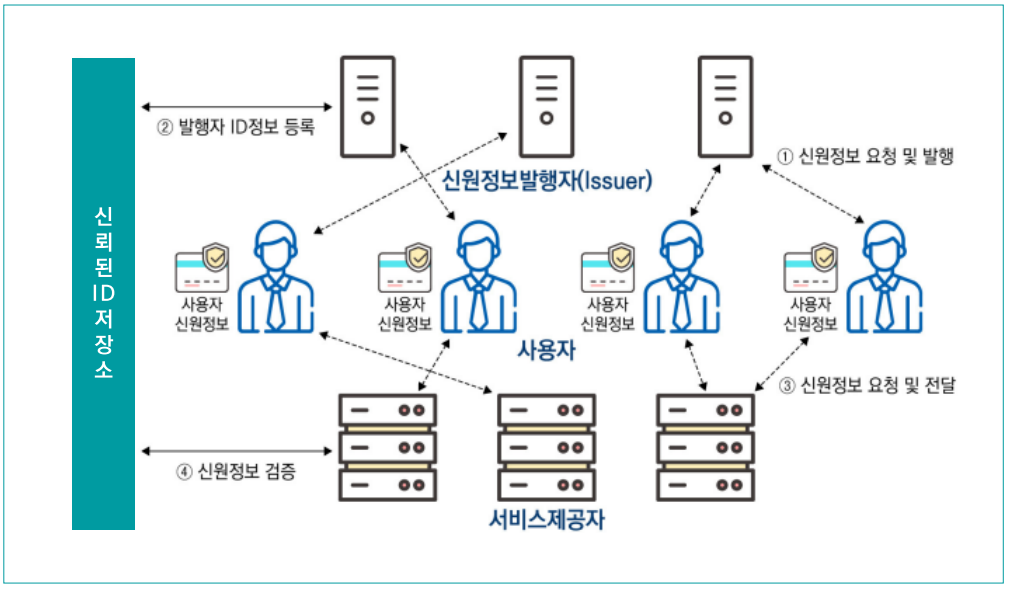
구 분	설 명
지속성	신원정보는 서비스제공자에 의해 관리되지 않으므로 서비스제공자의 서비스 운영 중지 등 외부환경의 변화와 관계없이 사용자는 자신의 신원정보를 지속적으로 사용할 수 있어야 함
독립성	서버-클라이언트 모델과 달리 누구나 필요한 신원정보를 생성·이용하기 위해서 신원정보의 발행·검증은 특정기관에 종속적이지 않고 피어(PEER) 기반으로 독립적으로 운영이 필요함. 다만 사용자의 신원을 최초로 검증할 수 있는 최소한의 신뢰된 기관(Trust Anchor)에 대한 고려는 필요함
휴대성	신원증명이 필요한 경우 언제든 사용자는 스스로 신원정보를 선택 후 제공 가능해야 하므로 사용자의 휴대성을 위해 스마트폰 등을 이용한 모바일ID, 칩이 내장된 실물카드 형태의 ID카드 또는 생체인증(FIDO) 연계 등을 통해 언제든 필요시 신원정보를 선택하여 서비스제공자에게 제공해야 함
개인정보보호	개인의 명시적 동의 없이는 서비스제공자의 개인정보의 활용 등이 제한되도록 분산원장의 암호학적 특성을 기반으로 한 신뢰된ID저장소를 이용하고 제3기관의 통제 없이 분산원장에 참여 가능한 누구나 신원정보의 위·변조 여부 검증이 가능해야 하며, 신뢰된ID저장소 내 개인정보가 포함된 신원정보는 암호화 등의 조치를 수행하거나 분산원장 밖(Off-Chain)에서 저장함
확장성	금융권에서 보증하는 신뢰 수준을 요구하는 디지털 신원확인의 확대요구로 범금융권, 통신/공공/산업 등의 영역으로 적용대상이 확대 가능하도록 표준에 근거한 구현이 필요함

출처: 전자부품연구원 블록체인사업단 김현식 단장(2019), 지능정보통신 VOL.20, 한국정보통신학회

2 기술 구성방식

분산ID를 이용한 본인확인 절차는 4단계로 구성되어 있다. 구체적으로 (i) 사용자가 신원정보 발행을 요청하면 신원정보발행자(Issuer)는 사용자의 신원을 검증한 후 신원정보를 발행(〈그림 II-11〉에서 ①), (ii) 신원정보발행자는 사용자 신원정보를 검증할 수 있는 발행자의 ID정보를 신뢰된ID저장소(분산원장)에 등록(②), (iii) 사용자가 서비스 이용 시, 신원정보를 서비스제공자에게 제출(③), (iv) 서비스제공자는 신뢰된ID저장소에 신원정보에 대한 검증을 요청하여 신원을 확인(④)하는 단계로 구성된다. 위 과정에 대한 구체적인 내용은 다음과 같다.

〈그림 II-11〉 신원확인 절차

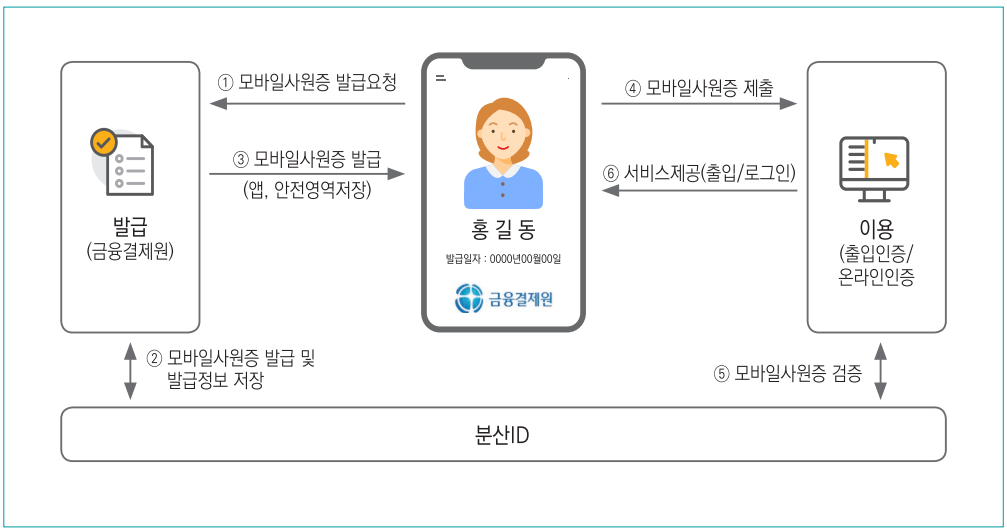


출처: 금융보안원 보안기술연구팀(2019), 전자금융과 금융보안 제16호, 15-36, 금융보안원

3 적용 사례 등

금융권에서는 분산ID 상용화를 위해서 다양한 준비를 하고 있다. 현재 분산ID와 관련된 연합체는 국내에서 총 4개가 운영되고 있다. 금융분산ID 추진협의회는 국내 16개 은행과 금융결제원으로 구성되어 은행권이 공동으로 구축, 운영중인 블록체인 플랫폼을 통해 금융과 연계되는 다양한 분산신원증명을 한곳에서 발급, 관리할 수 있는 정보지갑 서비스 '마이인포'를 제공하고 있다. 이니셜DID연합은 통신 3사(SK텔레콤, KT, LG유플러스)가 주축이 되어 블록체인 기반 모바일 전자증명 서비스 '이니셜'을 개발하고 있다. DID얼라이언스코리아는 분산ID 관련 기업과 기관이 참여할 수 있는 기술의 국제화 및 표준화를 추진한다. 마이아이디 얼라이언스는 컨소시엄을 이끄는 아이콘루프가 개발한 블록체인 기반 비대면 실명확인 플랫폼 '마이아이디'를 중심으로 금융산업에서의 생태계를 확산하겠다는 계획이다.[51] NH농협은행의 '모바일 사원증' 서비스는 '이니셜' 연합에서 제공하는 분산ID 기술을 적용하였으며, 임직원 개인이 모바일로 사원증을 신청 및 발급한 후 출입인증과 출퇴근 관리 기능을 구현하였다.

〈그림 Ⅱ-12〉 금융결제원 분산ID 모바일 신분증 이용절차



금융결제원, 이제 '목걸이 사원증'이 사라집니다(2020.5.14.)

51) 아이콘루프 마이아이디, www.iconloop.com/myid

이처럼 분산ID를 이용할 경우 신원확인에 소요되는 절차가 간소화되고 시간이 절약되는 장점과 도용에 대한 안전성 등 다양한 효율적인 요소들로 인해 정부차원에서도 모바일 신분증에 대한 단계적 도입 계획을 발표하였다. 이에, 2020년부터 디지털 공무원증의 도입 및 향후 복지카드, 운전면허증 등으로 적용범위가 점차 확대되고 있으므로 분산ID에 대한 중요성이 커질 전망이다.

〈그림 Ⅱ-13〉 정부의 모바일 신분증 도입 계획

출처: 행정안전부 인사혁신처, 정부, 모바일 공무원증 도입한다(2020. 04.20.)

분산ID 인증 방식과 관련하여 최근 「금융혁신지원 특별법」에 따라 혁신금융서비스로 지정된 "블록체인 기반 부동산 수익증권 거래 플랫폼",[52] "디지털 실명확인증표 기반 비대면 실명확인 서비스(아이콘루프, 파운트, SK텔레콤, 코인플러그)",[53] "분산ID 기반 신원증명 서비스(파운트)",[54] "분산ID 기반 비대면 실명확인 서비스(파운트)"[55] 사례가 있다.

52) 금융위원회 보도자료, 혁신금융서비스 3건 지정(2021.4.14.)
53) 위 보도자료
54) 금융위원회 보도자료, 혁신금융서비스 5건 지정(2020.9.23.)
55) 금융위원회 보도자료, 혁신금융서비스 4건 지정 및 하반기 금융규제 샌드박스 접수 및 심사일정 안내(2020.7.22.)

핵심정리

1. 보안인증의 핵심기술

- 암호기술(대칭키 vs 공개키)
  - 암호기술은 정보보안의 목적 중 기밀성 또는 무결성을 보장하는 기술로 암호화는 암호 알고리즘과 키를 이용하여 평문을 암호문으로 변환하는 것을 말하고 복호화는 암호문을 암호 알고리즘과 키를 이용하여 평문으로 변환하는 것을 말한다. 이러한 암호기술은 키를 사용하는 방식에 따라 대칭키 암호기술, 비대칭키(또는 공개키) 암호기술로 구분되고 대칭키 암호기술은 하나의 키를 이용하여 암호화와 복호화를 할 수 있는 기술, 공개키는 암호화와 복호화에 사용되는 키가 서로 다른 한 쌍을 이용하는 기술을 말한다.

- 해시함수
  - 해시함수는 입력 메시지의 길이와는 무관하게 출력 메시지는 항상 고정된 길이를 갖는 데이터 변환 함수를 말한다. 해시함수의 특징으로는 단방향으로만 데이터를 변환할 수 있다는 것이고 일반적인 암 · 복호화와는 다르게 키를 이용하지 않는다. 이러한 해시함수를 국내 법규에서는 일방향 암호화라고 명시하고 있다.

2. 보안인증기술 사례 (인증서)

- 인증서는 PKI(공개키 기반구조)로 구성되어 있고 암호기술 중 비대칭키 방식으로 사용된다. 인증서를 이용하여 신원확인, 정보의 무결성 확인, 부인방지 등을 할 수 있게 된다.
- 인증서기술은 대부분 금융회사 전자금융서비스 홈페이지에 적용되어 있으며, ID/PW와 더불어 가장 많이 사용되고 있는 보안인증기술이다.

3. 보안인증기술 사례 (생체정보)

- 생체정보는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 대한 정보와 이를 가공하여 생성된 정보도 포함하는 개념이다. 이 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 '생체인식정보'가 있으며, 가공되지 않은 정보를 '생체인식 원본정보'라고 하고, 가공된 정보를 '생체인식 특징정보'라고 하며 대표적인 생체기반 인증 방법으로 FIDO기술이 있다.
- 생체정보를 이용한 보안인증의 사례로 정맥인증을 이용한 은행거래 서비스가 있고, 고객의 생체정보를 분할해 금융회사와 분산관리센터가 각각 보관하고 실제 거래 시 해당 정보를 결합하여 인증하는 사례도 있다.

4. 보안인증기술 사례 (분산ID)

- 분산ID는 프라이버시의 강화와 개인정보 유출 위협 대응, 인증정보 관리의 불편함 등을 해소하고자 등장하였으며, 사용자 스스로 본인 신원에 대한 증명을 관리하고 통제를 할 수 있는 신원관리체계를 말한다.
- 분산ID 특징으로 신원정보의 지속 사용이 가능한 지속성, 신원정보의 발행 및 검증이 특정기관에 종속적이지 않는 독립성, 언제든 스스로 신원정보를 선택 후 제공할 수 있는 확장성이 있다.

MEMO

헬로, 핀테크!(보안인증 · 블록체인)

3장

핀테크 보안인증기술

제1절 핀테크 보안인증 서비스 배경 및 혁신

제2절 핀테크 보안인증 시장 현황 및 사례

3장 핀테크 보안인증기술

학습목표

1. 전자금융거래, 전자금융업, 전자금융보조업자에 대해 이해하고 설명할 수 있다.
2. 「전자금융거래법」 개정안의 전자금융거래, 전자금융업, 주요수탁자에 대해 이해하고 설명할 수 있다.
3. 핀테크 보안인증 시장의 현황을 확인하고 대표적인 보안인증 사례를 이해하고 설명할 수 있다.

학습개요

「전자금융거래법」에서 전자금융거래란 "금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 고객이 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래"를 말한다. 최근 논의가 되고 있는 「전자금융거래법」 개정안에서는 '전자금융거래' 및 '비대면거래'를 구분하여 규정하고 있다. 또한 「전자금융거래법」의 '전자금융보조업자'는 「전자금융거래법」 개정안에서 '주요수탁자'로 규정되고 있다.

핀테크 회사가 「전자금융거래법」상 “전자금융업을 영위하기 위해서 전자금융업자 자격으로” 허가를 받거나 등록을 하여야 하고, 전자금융업은 7종(① 전자화폐의 발행 및 관리업무, ② 전자자금이체업무, ③ 직불전자지급수단의 발행·관리, ④ 선불전자지급수단의 발행·관리, ⑤ 전자지급결제대행업, ⑥ 결제대금예치업, 그리고 ⑦ 전자고지결제업)으로 구분된다. 「전자금융거래법」 개정안은 전자금융업을 3종{① 자금이체업(송금), ② 대금결제업(결제) 및 ③ 결제대행업(대행)}으로 개편하고, 새로운 전자금융업으로서 ‘지급지시전달업’을 신설한다.

최근 다양한 보안인증 방법을 사용할 수 있는 환경이 마련되었고, 대표적인 보안인증 방법으로는 카카오뱅크, KB모바일 인증서, 오픈패스(OpenPass), PASS 앱, 웹 표준 기반 간편인증 등이 있다.

3장 핀테크 보안인증기술

용어해설

❶ 전자금융거래

「전자금융거래법」 제2조 제1호에 따른, 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다. 「전자금융거래법」 개정안에서는 금융상품 및 서비스를 제공할 때 그 전부 또는 일부가 전자문서 등 전자적 방식으로 처리되는 거래를 말한다.

❷ 비대면거래

「전자금융거래법」 개정안에서는 금융회사 또는 전자금융업자와 이용자 간에 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 하는 전자금융거래를 말한다. 이는 현행 전자금융거래법에서의 전자금융거래와 동일하다.

❸ 전자금융업자

「전자금융거래법」 제2조 제4호에 따른 전자화폐의 발행 및 관리업무, 전자자금이체업무, 직불 · 선불 지급수단의 발행 및 관리, 전자지급결제 대행에 관한 업무 등을 수행하기 위해 금융위원회에 허가를 받거나 등록을 한 자(금융회사는 제외한다)를 말한다. 「전자금융거래법」 개정안에서는 자금이체업(송금), 대금결제업(결제), 결제대행업(대행), 지급지시전달업을 수행하기 위해 금융위원회에 허가를 받거나 등록을 한 자를 말한다.

❹ 전자금융보조업자

「전자금융거래법」 제2조 제5호에 따른 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 금융위원회가 정하는 자를 말한다.

❺ 주요수탁자

「전자금융거래법」 개정안에서는 현행 「전자금융거래법」의 전자금융보조업자에 해당하며 클라우드 컴퓨팅 서비스 제공자, CD VAN사 등이 고려되고 있다.

제1절

핀테크 보안인증 서비스 배경 및 혁신

1 전자금융거래의 개념

법률상 '핀테크'에 대한 정의는 없다. 이에 법률상 핀테크와 유사한 의미로 인식되는 '전자금융거래' 등의 정의를 확인해 본다. '전자금융'라는 단어는 이미 국내 · 외에서 이미 다양한 표현과 정의로 사용되고 있다. 국내 「전자금융거래법」에서는 '전자금융거래'로, 한국은행 금융결제국의 전자금융총람에서는 '전자금융'으로, 국제결제은행(BIS; Bank for International Settlements)은 'Electronic Banking'으로 정의하고 있다.

국내 「전자금융거래법」에서 말하는 '전자금융거래'란, "금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래"로 정의하여 설명한다. 한국은행 금융결제국의 전자금융총람에서의 '전자금융'이란, "금융 업무에 IT기술을 적용하여 자동화, 전산화를 구현한 것으로서, 초기에는 금융회사 업무를 자동화하는 의미였다가, 최근에는 금융과 IT기술이 융합된 금융서비스"를 의미한다고 설명한다. 마지막으로 국제결제은행(BIS; Bank for International Settlements)은 'Electronic Banking'에 대해 "전자적 채널을 통하여 금융상품 및 서비스를 제공하는 것, 예금 · 대출, 계좌관리, 금융자문의 제공, 전자납부서비스, 전자화폐 등의 상품 및 서비스가 포함되는 것"으로 설명한다.

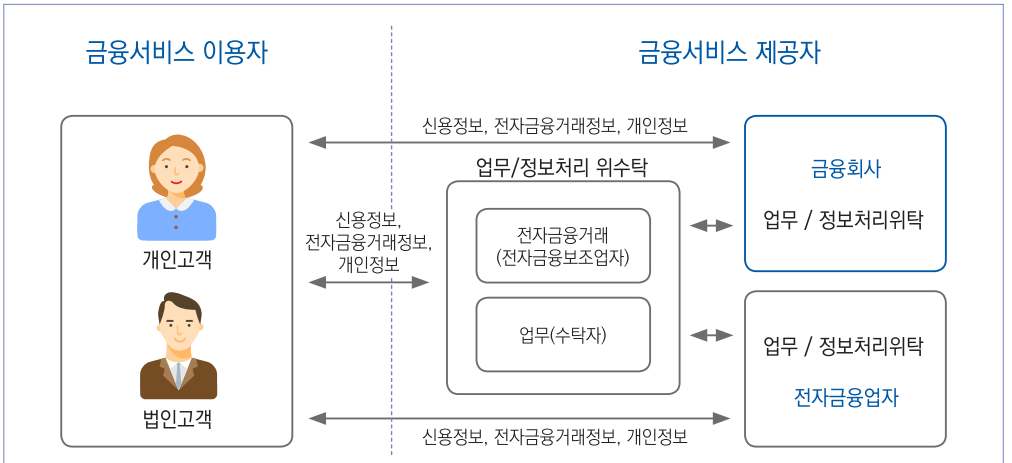
또한 최근 은행 등 금융권을 중심으로 '디지털금융'이라 불리는 새로운 표현이 등장하고 있으나, 금융과 IT기술이 결합되어 기존 금융서비스를 고도화한다는 측면에서는 기존 금융규제 영역에서 법률적인 정의인 '전자금융거래'와 특별히 구분되는 차이는 없다.

[관계법령] 전자금융거래법 제2조 제1호

"전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

핀테크 회사가 '전자금융거래' 관련하여 주의할 사항으로는 「전자금융거래법」상 전자금융업을 영위하기 위해서는 「전자금융거래법」상 전자금융업자로 허가를 받거나 등록을 하여야 하고, 금융관련 법령을 준수하여야 한다. 구체적으로 핀테크 회사가 「전자금융거래법」상 전자금융업으로 명시되어 있는 전자화폐 발행 및 관리, 전자자금이체업무, 직불전자지급수단의 발행 및 관리, 선불전자지급수단의 발행 및 관리, 전자지급결제대행에 관한 업무 등 전자금융업을 하고자 하는 경우는 반드시 법 제28조에서 말한 전자금융업자로 금융위원회의 허가를 받거나 등록을 하여야 하며, 발행규모 및 가맹점 등 제한된 범위 내에서 금융서비스를 제공할 경우에는 등록 없이 할 수 있다.

〈그림 Ⅲ-1〉 전자금융거래법상 전자금융업자 및 전자금융보조업자



〈그림 Ⅲ-1〉에서 보는 바와 같이 핀테크 회사는 '전자금융업자'가 아닌 '전자금융보조업자'의 역할을 수행할 수도 있다. 구체적으로 「전자금융거래법」에서 '전자금융보조업자'는 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자를 말하며, '전자금융업자'와 달리 금융위원회의 허가 또는 등록 절차가 없다.

[관계법령] 전자금융거래법 제2조 제5호

"전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

1-1 「전자금융거래법」 개정안의 전자금융거래

「전자금융거래법」 개정안에서는 현행 비대면거래로 제한되어 있는 전자금융거래의 범위를 전자적 방식으로 처리되는 모든 거래로 확대하고(안 제2조 제1호), 법 적용과 관련하여 적용배제(안 제3조)를 명확히 한다.

[관계법령] 전자금융거래법 개정안 제2조 제1호

"전자금융거래"란 금융상품 및 서비스를 제공할 때 그 전부 또는 일부가 전자문서 등 전자적 방식으로 처리되는 거래를 말한다.

[관계법령] 전자금융거래법 개정안 제2조 제1의2호

"전자금융업무"란 전자금융거래를 처리하는 업무 및 이에 수반되거나 밀접하게 관련이 있는 금융회사 또는 전자금융업자 내부의 업무를 말한다.

[관계법령] 전자금융거래법 개정안 제3조

제3조(전자금융거래 등의 적용배제)

① 다음 각 호의 어느 하나에 해당하는 경우에는 전자금융거래로 보지 아니한다.

1. 금융상품의 제공 과정에 수반되지 않거나 밀접한 관련이 없는 정보의 처리
2. 불특정 다수인을 대상으로 금리, 수수료, 환율 등 금융상품 및 서비스의 내용에 대하여 광고 등의 방법으로 단순히 그 사실을 알리거나 안내하는 경우
3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 통신과금서비스를 이용하는 거래
4. 「어음법」에 따른 어음 또는 「수표법」에 따른 수표를 이용하는 거래로서 전자적 방식으로 처리하지 않는 거래
5. 그 밖에 해당 전자금융거래의 특성 등을 고려하여 전자금융거래에서 제외하더라도 이용자 보호 및 건전한 거래질서를 저해할 우려가 없는 거래로서 대통령령으로 정하는 거래

1-2 「전자금융거래법」 개정안의 비대면거래

「전자금융거래법」 개정안에서는 전자금융거래와 구분하여 비대면거래가 별도 정의된다. 이는 현행 접근매체의 위·변조, 해킹 등으로 획득한 접근매체의 이용 등 특정한 기술적 유형으로 제한되고 있는 금융회사와 전자금융업자의 손해배상책임에 대하여 이용자의 거래지시나 동의가 없거나 그 거래지시에 따라 처리되지 않은 무권한 비대면거래(Unauthorized Transaction) 전반으로 그 책임 범위를 확대하고, 해당 비대면거래가 금융회사 등이 관리·운영하는 영역 외에서 발생하였다는 사실이나 오류 없이 비대면거래를 처리한 사실에 대해서는 금융회사 등이 입증부담을 지도록 하는 등 디지털금융에서 비대면거래 이용자를 두텁게 보호하기 위해서이다(안 제9조 제1항 개정, 제9조의2 신설).[56]

56) 정무위원회 수석전문위원 이용준(2021.2.), 전자금융거래법 일부개정법률안 검토보고

[관계법령] 전자금융거래법 개정안 제2조 제10호 중 일부

10. "접근매체"란 금융회사 또는 전자금융업자가 이용자에게 발급하거나 이용자가 금융회사 또는 전자금융업자에 등록한 조회용매체나 지시용매체 또는 조회용매체와 지시용매체가 복합된 수단 또는 정보로서 다음 각 목의 어느 하나에 해당하는 것을 말한다. 이 경우 **금융회사 또는 전자금융업자와 이용자 간에 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 하는 전자금융거래(이하 "비대면거래"라 한다)**에 사용되는 수단 또는 정보로 한정한다.

1-3 「전자금융거래법」 개정안의 주요수탁자[57]

「전자금융거래법」 개정안에서는 금융의 정보기술부문에 대한 업무위탁 등이 확대됨에 따라 나타날 수 있는 제3자 리스크에 대한 관리·감독을 강화하기 위하여, 현행법은 금융회사·전자금융업자의 외부주문등에 관한 계약에 관하여 금융위원회가 금융회사등에 시정·보완을 지시할 수 있고, 금융감독원장이 금융회사등을 검사하는 경우 수탁자등에 대해서 자료요구를 하거나 조사를 할 수 있도록 하고 있으나(제40조), 개정안은 이에 더하여 수탁자등의 업무가 전자금융거래의 안전성·신뢰성에 중대한 영향을 미치는 "주요수탁자등"에 대해서는 금융위원회가 금융회사등에 대한 검사 시가 아니더라도 그 수탁자등에 대해 직접 자료제출 요구를 하거나, 금융감독원장이 조사를 할 수 있도록 하려고 한다(안 제40조의2 신설). 또한, 전자금융업자가 업무를 위탁할 때 필요한 사항들을 정하고(안 제36조의10), 이를 위반하여 업무를 수행한 주요수탁자에게 과징금을 부과할 수 있도록 하고 있다(안 제46조의2).

또한 전자금융업자는 이용자 보호 등을 위해 대통령령으로 정하는 업무는 제3자에게 위탁해서는 안되고, 업무위탁 시에는 위탁 업무의 범위 및 수탁자의 행위제한에 관한 사항을 포함하는 위탁계약을 체결해야 하는 등의 의무를 이행해야 한다. 그런데 개정안은 업무위탁과 관련하여 의무를 이행해야 하는 주체를 '전자금융업자'로 하면서, 해당 조문 위반 시 과징금은 '주요수탁자'에게 부과할 수 있도록 하고 있다. 과징금이 행정법상 의무 위반에 대해

57) 정무위원회 수석전문위원 이용준(2021.2.), 전자금융거래법 일부개정법률안 검토보고

부과되는 금전적 제재라는 점을 고려하면, 개정안은 의무자인 전자금융업자에게 과징금을 부과하는 것으로 수정하거나, 또는 주요수탁자가 위탁업무와 관련하여 준수하여야 할 사항에 관한 별도의 조문을 규정하고, 해당 규정 위반 시 과징금을 부과할 수 있는 것으로 보완이 필요하다고 본다.

금융위원회는 대통령령에서 정하게 될 "주요수탁자등"으로 클라우드 컴퓨팅 서비스 제공자[58]와 CD VAN[59]사 등을 고려하고 있다고 설명한다. 클라우드 서비스처럼 소수 제공자가 글로벌 시장 지배 시 단일 실패점(a single point of failure)으로 작용하거나[60], 금융안정에 영향을 미칠 우려가 있고, 클라우드 서비스 장애 등으로 인한 서비스 중단, 설정 오류로 인한 데이터 유출, 당국 및 금융회사의 접근·감사 한계, 집중 리스크 등 다수의 리스크 요인이 존재하기 때문에 이에 대한 관리·감독을 강화할 필요가 있다는 것이다.

2 전자금융업의 종류

핀테크 회사가 「전자금융거래법」상 전자금융업을 영위하기 위해서는 전자금융업자로 금융위원회의 허가를 받거나 등록을 하여야 한다. 핀테크 회사가 전자금융업자로서 할 수 있는 전자금융업에 대한 구체적인 설명은 다음과 같다.

---

58) 클라우딩 컴퓨팅은 언제 어디서나 필요한 만큼의 컴퓨팅 자원을 필요한 시간만큼 인터넷을 통하여 활용할 수 있는 컴퓨팅 방식을 의미. 인터넷이 연결되면 PC와 모바일 기기 등 다양한 기기를 통해 클라우드 서비스에 접속할 수 있고, 이용자가 원하는 서비스를 원하는 만큼만 사용하고 비용을 부담한다는 특징을 가짐. 주요 기업으로는 Amazon Web Service가 압도적 시장지위를 유지(전 세계 시장의 34%)하는 가운데 MS, 구글, 알리바바가 빠르게 성장하고 있는 상황이며, 해외 사업자가 시장을 주도하는 가운데 KT, 네이버, SK C&C 등이 경쟁 중임. 강맹수, 「클라우드 컴퓨팅 시장 동향 및 향후 전망」, 2019.1.

59) 부가통신사업자(van, value added network): VAN사란 카드사·가맹점 등과 계약을 맺고 카드 단말기 설치, 신용카드 승인 등 대금 결제 중개 서비스를 제공하는 업체를 말함

60) 일부 서비스제공자의 서비스 장애, 예기치 않은 서비스 중단, 파산 등이 금융안정성에 미치는 부정적 영향을 의미

〈표 Ⅲ-1〉 전자금융업에 대한 구체적인 설명[61)]

구분	설명
전자화폐 발행 및 관리	• 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보 • 발행인 외의 제3자로부터 재화 또는 용역의 대가 지급에 사용 • 2개 이상 광역지방자치단체, 500개 이상 가맹점 이용
선불전자지급 수단 발행 및 관리	• 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 · 정보 • 발행인 외의 제3자로부터 재화 또는 용역의 대가 지급에 사용 • 구입할 수 있는 재화 또는 용역의 범위가 2개 업종 이상
직불전자지급 수단 발행 및 관리	• 이용자와 가맹점 간에 전자적 방법에 따라 금융회사의 계좌에서 자금을 이체하는 등의 방법으로 재화 또는 용역의 제공과 그 대가의 지급을 동시에 이행할 수 있도록 금융회사 또는 전자금융업자가 발행한 증표 또는 그 증표에 관한 정보
전자자금 이체	• 지급이체(지급인의 지시): 계좌이체, 서비스이체, 대량지급 • 거래추심이체(수취인의 지시): 자동계좌이체 [지급인의 출금동의]
전자지급 결제 대행	• 전자적 방법으로 재화의 구입 또는 용역의 이용에 있어 지급결제정보를 송신하거나 수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 것
결제대금 예치	• 「전자상거래 등에서의 소비자보호에 관한 법률」에 따른 거래 일방의 불이행에 따른 거래사고 예방을 위해 결제대금을 예치받는 업무
전자고지 결제	• 수취인을 대행하여 지급인이 수취인에게 지급하여야 할 자금의 내역을 전자적인 방법으로 지급인에게 고지하고, 자금을 직접 수수하며 그 정산을 대행

전자금융업을 하기 위해 핀테크 회사가 허가 및 등록하여야 하는 주요 요건은 다음과 같다.

61) 금융감독원(2009), 전자금융감독규정 해설

〈표 Ⅲ-2〉 전자금융업의 허가 및 등록을 위한 주요 요건[62)]

구분	전자화폐	전자자금이체	직불전자지급수단	선불전자지급수단	지급결제대행	결제대금예치	전자고지결제
1. 허가 및 등록요건	허가	등록	등록	등록	등록	등록	등록
최소자본금	50억원	30억원	20억원		10억원		5억원
					분기별 전자금융거래 총액 30억원 이하인 경우: 3억원		
부채비율	180% 이내	200% 이내					
2. 전문인력	2년 이상 경력 전산전문 5인 이상						
3. 전자금융 사고 대비 보험가입 기준	1억원	2억원	2억원	1억원	1억원 (신용카드등 접근매체 정보 저장 시: 10억)	1억원	1억원
4. 적용범위	5개 업종 이상	-	-	2개 업종 이상	-	-	-
5. 이용지역	2개 이상 광역지자체 500개 이상 가맹점	-					

앞서 설명한 것처럼 핀테크 회사가 전자금융업자로 등록을 하지 않고 전자금융업을 할 수 있는 방법으로는, 핀테크 회사가 발행한 선불전자지급수단이 (ⅰ) 특정한 건물 안의 가맹점 등 일정 기준에 해당하는 가맹점에서만 사용되거나 (ⅱ) 선불전자지급수단의 총 발행잔액이 일정 금액 이하인 경우 등이 해당한다. 또한 전자지급결제대행에 관한 업무를 수행하고자 하는 핀테크 회사가 (ⅲ) 자금이동에 직접 관여하지 아니하고 전자지급거래의 전자적 처리를 위한 정보만을 전달하는 업무를 수행하고자 하는 경우도 등록 없이 전자금융업을 할 수 있다.

62) 금융감독원(2009), 전자금융감독규정 해설

[관계법령] 전자금융거래법 제28조

제28조(전자금융업의 허가와 등록)

③ 제2항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 자는 금융위원회에 등록하지 아니하고 같은 항 각 호의 업무를 행할 수 있다.

1. 다음 각 목의 어느 하나의 경우에 해당하는 선불전자지급수단을 발행하는 자
   가. 특정한 건물 안의 가맹점 등 대통령령이 정하는 기준에 해당하는 가맹점에서만 사용되는 경우
   나. 총 발행잔액이 대통령령이 정하는 금액 이하인 경우
   다. 이용자가 미리 직접 대가를 지불하지 아니한 선불전자지급수단으로서 이용자에게 저장된 금전적 가치에 대한 책임을 이행하기 위하여 대통령령이 정하는 방법에 따라 상환보증보험 등에 가입한 경우
2. 자금이동에 직접 관여하지 아니하고 전자지급거래의 전자적 처리를 위한 정보만을 전달하는 업무 등 대통령령이 정하는 전자지급결제대행에 관한 업무를 수행하는 자

참고로, 「전자금융거래법」 개정안은 현행법령에 따라 7종으로 구분되어 있는 전자금융업을 3종[① 자금이체업(송금), ② 대금결제업(결제) 및 ③ 결제대행업(대행)]으로 개편하고, 새로운 전자금융업으로서 '지급지시전달업'을 신설한다(안 제2조 제2호의2부터 제2호의6까지 등).

제2절

핀테크 보안인증 시장 현황 및 사례

1 보안인증 시장 현황

「전자서명법」 개정에 따른 공인인증서 의무사용 폐지 후 다양한 인증 서비스가 출현하게 되었다. 현재 시장에서 사용되고 있는 인증 서비스의 현황은 다음과 같다.[63]

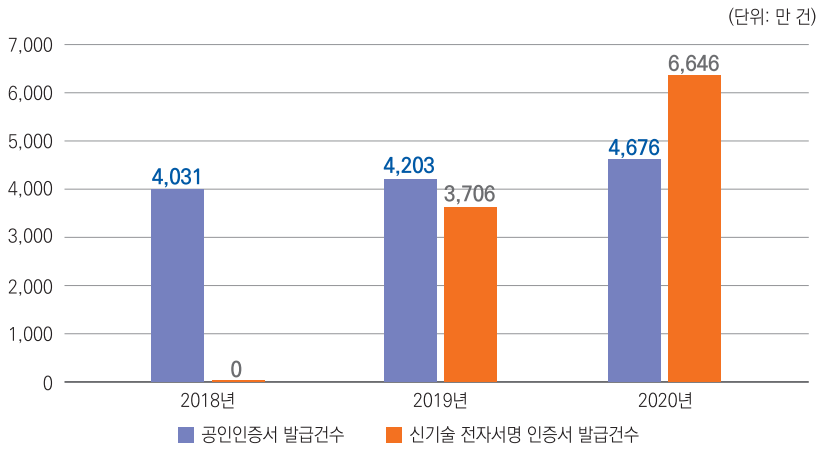
인증서 종류	발급기관	주요특징	출시일자
네이버 인증서	네이버	개별 서비스 앱에서 인증서를 발급하며, 각 플랫폼에 연계된 서비스에서 이용 가능	2019.06.
삼성패스 전자서명 인증서	한국정보인증		2020.12.
카카오페이 인증서	카카오페이		2017.06.
토스 인증서	비바리퍼블리카		2018.11.
페이코 인증서	NHN페이코		2020.09.
PASS 인증서	이동통신 3사		2019.04.
금융인증서비스	금융결제원	별도 프로그램 · 앱 설치 없이 이용할 수 있으며, 인증서 이동 · 복사가 불필요하고, 금융 · 공공 등 모든 전자거래에서 이용 가능	2020.11.
하나원큐 모바일 인증	하나은행	각 은행(모바일뱅킹) 앱을 통해 금융그룹별 서비스에 이용 가능	2020.08.
KB모바일 인증서	KB국민은행		2019.07.
NH원패스	NH농협은행		2020.10.
공동인증서*	금융결제원, 코스콤 등	기존 공인 인증서와 유사한 방식으로 이용가능	–

* 기존 공인인증기관(한국전자인증 등)도 Active X, 보안프로그램 설치 없이 클라우드에 인증서를 발급받아 언제 어디서나 간편하게 이용할 수 있는 방향으로 전자서명서비스를 개선 중

63) 과학기술정보통신부 · 행정안전부 · 국민권익위원회 보도자료, 정부24 · 홈택스 등 주요 공공 누리집에 민간 전자서명 도입 (2021.1.11.)

2020년 11월 말 기준, 민간 전자서명서비스 가입자(6,646만 건)가 공인 전자서명 서비스 가입자(4,676만 건)를 초과하였다.[64]

〈그림 Ⅲ-2〉 전자서명 인증서 발급현황



* 공인인증사업자(금융결제원, 한국정보인증, 한국전자인증, 코스콤, 한국무역정보통신 등 5개사) 및 민간 전자서명사업자(카카오페이, 은행연합회, 비바리퍼블리카, 통신 3사, 네이버, KB국민은행, NHN페이코 등 7개사)가 제출한 가입자 수 기준

출처: 카카오페이

2 보안인증 사례[65]

보안인증 사례로 카카오뱅크, KB모바일 인증서, 오픈패스(OpenPass), PASS, 웹 표준 기반 간편인증 서비스를 간략히 소개한다.

64) 과학기술정보통신부 · 행정안전부 · 금융위원회 보도자료, 12월 10일, 공인전자서명제도 폐지(2020.12.10.)
65) 강효관, 국내 인증 기술 및 서비스 현황, 정보보호학회지 제30권 제3호, 2020.6.

2-1 카카오뱅크

카카오뱅크는 기존 인증서의 경우 사용과 보안을 위해 여러 보안모듈(PKI, 키보드 보안, 방화벽 등)을 설치하던 방식을 일원화하여 자체 개발하고, 보안성 강화를 위해 중요 정보를 모바일 보호 영역에 저장하는 방식을 사용한다. 또한 PKI 방식의 보안 수준을 제공하는 인증서를 사용하면서도 복잡한 UX(User eXperience)를 직관적인 UX로 변경하는 것을 목표로 생체인증, PIN번호 등의 기술을 적용하여 고객 편의성을 극대화하였다.

2-2 KB모바일 인증서

2019년 KB국민은행은 기존 인증서의 불편함을 개선한 인증서 시스템인 "KB모바일 인증서"를 서비스하기 시작했다. 최초 발급 절차의 간소화, 인증서의 안전한 저장과 생체인증, 간편비밀번호를 포함한 편리하고 다양한 인증 방식 제공 등을 주요 특징으로 하고 있다. 특히 매년 갱신해야 하는 인증서의 불편함을 해소하기 위해 인증서를 폐기하거나 장기간 사용하지 않는 경우를 제외하면 계속 사용할 수 있다. 연말정산, 전자정부 민원서류 등과도 연계하여 인증서가 필수였던 서비스에도 사용 가능하다. KB모바일 인증서는 KB국민은행 앱에서만 사용 가능하며, PC나 브라우저 등 범용적인 환경에서는 사용이 불가하다.

2-3 오픈패스(OpenPass)

2019년 안랩과 코스콤은 안랩의 "안랩 V3 모바일 플러스 2.0"에 코스콤의 통합인증기능을 이식한 서비스를 오픈하였다. 약 2,800만 대의 모바일기기에서 이용 중인 앱에 인증기능을 통합하여, 각 사용자의 추가 설치에 대한 부담을 줄였다. 인증서의 안전한 저장과 생체인증, 간편비밀번호 등 편리한 인증 방식 역시 제공하고 있다. 여타 인증 방식과는 다르게 인증서를 통한 인증을 같이 제공하고 있으며, PC에 인증서를 가지고 있지 않은 경우에도 앱을 통해 인증서비스를 사용할 수 있다.

2-4 PASS

2018년 통신 3사는 각각 운영해온 본인확인 서비스(SK텔레콤 'T인증', KT 'KT인증', LG유플러스 'U+인증')를 'PASS'라는 브랜드로 통합하였다. 이후 2019년 PASS 앱 기반의 사설인증서인 '패스 인증서'를 출시했다. 패스 인증서는 보안인증만 제공하던 PASS 앱에 전자서명 기능을 추가하였으며, 인증서를 WBC(White-Box. Cryptography, 화이트박스 암호)를 통해서 보호하고, 백신, 위변조 방지 등의 보안 기술을 적용하였다. 생체인증, 간편비밀번호 등 편리한 인증 방식을 제공한다.

2-5 웹 표준 기반 간편인증 서비스

2019년 인터넷 뱅킹 이용 실적 중 모바일 뱅킹이 차지하는 비중은 건수 및 금액 기준으로 각각 61.9%, 13.1%였다. 모바일의 비중이 높지만, 모바일이 아닌 인터넷 뱅킹에서는 아직도 건수 기준으로는 38.1%, 금액은 86.9%를 차지하고 있다. 이러한 통계를 볼 때 PC웹, 모바일 웹에서 별도의 설치 없이 사용할 수 있는 사설인증 서비스 역시 필요하다고 볼 수 있다. 앱이 반드시 필요한 여타 서비스와 달리 예티소프트와 한컴시큐어(現 한컴위드)는 웹 표준 기반으로 사설인증 서비스를 제공하고 있다. 웹 표준 형태의 서비스는 다른 앱과의 연동이 필요한 경우 In-App 브라우저 등을 통해 별도의 설치나 전환 없이 이용할 수 있다.

핵심정리

1. 핀테크 보안인증서비스 배경 및 혁신

- 전자금융거래의 개념
  - 전자금융거래는 금융회사 또는 전자금융업자가 전자적 장치를 이용해 금융상품 및 서비스를 제공하고 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이용하는 것을 의미한다.
  - 「전자금융거래법」 개정안에서 전자금융거래는 금융상품 및 서비스를 제공할 때 그 전부 또는 일부가 전자문서 등 전자적 방식으로 처리되는 거래를 말하고, 비대면거래는 금융회사 또는 전자금융업자와 이용자 간에 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 하는 전자금융거래를 의미한다.

- 전자금융업의 종류
  - 핀테크 회사가 「전자금융거래법」상 전자금융업을 영위하기 위해서는 전자금융업자로 금융위원회의 허가를 받거나 등록을 하여야 한다.
  - 전자금융업자는 전자화폐의 발행 및 관리, 선불/직불 전자지급수단의 발행 및 관리, 전자자금의 이체, 전자지급결제의 대행, 결제대금 예치, 전자고지 결제 업무를 할 수 있다.
  - 「전자금융거래법」 개정안에서는 자금이체업(송금), 대금결제업(결제), 결제대행업(대행)으로 개편되고, 지급지시전달업이 신설된다.

2. 핀테크 보안인증 사례

- 보안인증 시장 현황
  - 전자금융거래법 및 전자서명법에서 다양한 인증 방법을 사용할 수 있도록 하여, 여러 핀테크 회사에서 다양한 인증 서비스를 출시하였다.
  - 대표적인 사례로는 카카오뱅크, KB모바일 인증서, 오픈패스(OpenPass), PASS, 웹 표준 기반 간편인증 서비스 등이 있다.

- 보안인증 사례
  - 카카오뱅크는 보안을 위해 여러 보안모듈(PKI, 키보드 보안, 방화벽 등)을 설치하던 방식을 일원화하여 자체 개발하고, 보안성 강화를 위해 중요 정보를 모바일 보호 영역에 저장하는 방식을 사용한다. 또한 PKI 방식의 보안 수준을 제공하는 인증서를 사용하면서도 복잡한 UX(User eXperience)를 직관적인 UX로 변경하는 것을 목표로 생체인증, PIN번호 등의 기술을 적용하였다.
  - KB모바일 인증서는 KB국민은행이 제공하는 인증서로 최초 발급 절차의 간소화, 인증서의 안전한 저장과 생체인증, 간편비밀번호를 포함한 편리하고 다양한 인증 방식 제공 등을 주요 특징으로 하고 있다. 특히 매년 갱신해야 하는 인증서의 불편함을 해소하기 위해 인증서를 폐기하거나 장기간 사용하지 않는 경우를 제외하면 계속 사용할 수 있다. 연말정산, 전자정부 민원서류 등과도 연계하여 인증서가 필수였던 서비스에도 사용 가능하다. KB모바일 인증서 또한 KB국민은행 앱에서만 사용 가능하며, PC나 브라우저 등 범용적인 환경에서는 사용이 불가능하다.

- 오픈패스(OpenPass)는 안랩의 “안랩 V3 모바일 플러스 2.0”에 코스콤의 통합인증기능을 이식한 서비스이다. 약 2,800만 대의 모바일기기에서 이용 중인 앱에 인증기능을 통합하여, 각 사용자의 추가 설치에 대한 부담을 줄였다. 인증서의 안전한 저장과 생체인증, 간편비밀번호 등 편리한 인증 방식 역시 제공하고 있다. 여타 인증 방식과는 다르게 공동인증서를 통한 인증을 같이 제공하고 있으며, PC에 인증서를 가지고 있지 않은 경우에도 앱을 통해 인증서비스를 사용할 수 있다.
- PASS는 통신 3사가 각각 운영해온 본인확인 서비스(SK텔레콤 ‘T인증’, KT ‘KT인증’, LG유플러스 ‘U+인증’)가 통합된 브랜드이다. 2019년 PASS 앱 기반의 사설인증서인 ‘패스 인증서’를 출시했다. 패스 인증서는 본인 인증만 제공하던 PASS 앱에 전자서명 기능을 추가하였으며, 인증서를 WBC(White-Box. Cryptography, 화이트박스 암호)를 통해서 보호하고, 백신, 위변조 방지 등의 보안 기술을 적용하였다. 생체인증, 간편비밀번호 등 편리한 인증 방식을 제공한다.
- 웹 표준 기반 간편인증 서비스는 예티소프트와 한컴시큐어(現 한컴위드)가 개발한 웹 표준 기반 인증 서비스이다. 웹 표준 형태의 서비스는 다른 앱과의 연동이 필요한 경우 In-App 브라우저 등을 통해 별도의 설치나 전환 없이 이용할 수 있다.

헬로, 핀테크!(보안인증 · 블록체인)

4장

핀테크 보안인증 관련 규제 및 정책 동향

제1절 국내 규제

제2절 해외 규제

제3절 사고 및 위반 사례

4장 핀테크 보안인증 관련 규제 및 정책 동향

학습목표

❶ 「전자금융거래법」, 「전자금융거래법」 개정안, 「전자서명법」, 「전자문서법」의 규제를 이해할 수 있다.

❷ 국내 · 외 금융규제 동향을 이해할 수 있다.

❸ 보안인증 관련 사고 및 위반 사례를 통해 실무에 적용할 수 있다.

학습개요

핀테크 회사가 금융서비스를 제공함에 있어, 사전에 고려해야 하는 주요 규제는 「전자금융거래법」, 「전자금융거래법」 개정안, 「전자서명법」과 「전자문서법」이 있다. 규제로는 유럽연합 eIDAS, 미국 뉴욕주 23 NYCRR 500, 유럽연합 PDS2, 미국 국립표준기술연구소(NIST; National Institute of Standards and Technology)에서 발표한 사이버보안 로드맵 등이 있다. 추가로, 사고 사례와 위반 사례를 통해 보안인증의 중요성에 대해 개괄적으로 알아본다.

❶ 전자문서법

「전자문서 및 전자거래 기본법*」의 약칭을 의미한다.

* 법률 제17353호, 2020. 6. 9., 일부개정 내용 참고 [시행 2020. 12. 10.]

❷ 접근매체

전자금융거래에 있어서 거래지시를 하거나 고객 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단 또는 정보로서 인증서, 고객의 생체정보 등이 해당한다.

❸ 전자서명

서명자를 확인하고 서명자가 해당 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 해당 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

❹ 다중 인증(Multi-Factor Authentication)

최소 두 가지 이상의 보안인증 방식을 이용하여 본인 여부를 인증하는 것을 말한다.

제1절

국내 규제

핀테크 회사가 금융서비스를 제공함에 있어, 보안인증 관련하여 사전에 고려해야 하는 주요 규제는 「전자금융거래법」, 「전자금융거래법」 개정안, 「전자서명법」, 「전자문서법」이 있다.

1 전자금융거래법

핀테크 회사가 「전자금융거래법」의 전자금융거래에 해당하는 금융서비스를 고객에게 직접 제공할 경우 「전자금융거래법」에서 요구하는 전자금융업 등록을 하여야 한다. 2021년 5월 10일 기준 「전자금융거래법」에 따른 전자금융업 별 전자금융업자 등록 현황은 다음과 같다.

〈표 Ⅳ-1〉 전자금융업 등록 현황 [66]

전자금융업	등록 업체 수
직불전자지급수단의 발행 및 관리	67개
선불전자지급수단의 발행 및 관리	31개
전자지급결제 대행	129개
결제대금예치 업무	39개
전자고지결제 업무	14개
합 계	163개(280개 업종)

66) 금융위원회 · 금융감독원, e-금융민원센터 홈페이지 내 전자금융업등록현황 메뉴, http://www.fcsc.kr/B/fu_b_06.jsp

전자금융업자로 등록한 핀테크 회사는 안전한 전자금융거래를 위해 선량한 관리자로서의 주의를 다하여야 하고, 금융위원회가 정하는 기준인「전자금융감독규정」제8조부터 제37조까지의 기준을 준수하여야 한다. 만약 핀테크 회사가 선량한 관리자로서의 주의를 다하지 않거나, 금융위원회가 정하는 기준을 준수하지 않았을 경우 5천만원 이하의 과태료를 부과받을 수 있다. 따라서 아래의 규제 항목 준수를 위한 노력을 해야 한다.

[관계법령] 전자금융거래법 제21조 제1항, 제2항 및 제51조

제21조(안전성의 확보의무)

① 금융회사 · 전자금융업자 및 전자금융보조업자(이하 "금융회사등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

② 금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및「전자서명법」에 의한 인증서의 사용 등 인증 방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.

제51조(과태료)

① 다음 각 호의 어느 하나에 해당하는 자(제3호의 경우에는 제28조 제4항 단서에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 5천만원 이하의 과태료를 부과한다.

1. 제21조 제1항 또는 제2항을 위반하여 선량한 관리자로서의 주의를 다하지 아니하거나 금융위원회가 정하는 기준을 준수하지 아니한 자

[관계법령] 전자금융감독규정 제7조

제7조(전자금융거래 종류별 안전성 기준) 법 제21조 제2항의 "금융위원회가 정하는 기준"이라 함은 다음 각 호의 내용에 관하여 제8조부터 제37조에서 정하는 기준을 말한다.

1. 인력, 조직 및 예산 부문
2. 건물, 설비, 전산실 등 시설 부문
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술 부문
4. 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항

최근 일부 핀테크 회사는 네트워크 보안을 위한 통신망에 대한 분리 의무[(전자금융감독규정 제15조 제1항 제3호 및 제5호)] 를 준수하지 않아 과태료를 처분받은 경우가 있다.

[관계법령] 전자금융감독규정 제15조

제15조(해킹 등 방지대책)

① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립 · 운용하여야 한다.

3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리 · 차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

전자금융업자로 등록한 핀테크 회사는 고객과 전자금융거래의 계약 체결 시 이용 약관을 명시하여야 하고, 사본을 교부하고 그 약관의 내용을 설명하여야 한다.

[관계법령] 전자금융거래법 제24조

제24조(약관의 명시와 변경통지 등)

① 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어서 약관을 명시하여야 하고, 이용자의 요청이 있는 경우에는 금융위원회가 정하는 방법에 따라 그 약관의 사본을 교부하고 그 약관의 내용을 설명하여야 한다.

② 금융회사 또는 전자금융업자는 제1항의 규정을 위반하여 계약을 체결한 때에는 당해 약관의 내용을 계약의 내용으로 주장할 수 없다.

③ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 변경되는 약관의 시행일 1월 전에 금융위원회가 정하는 방법에 따라 이를 게시하고 이용자에게 알려야 한다. 다만, 법령의 개정으로 인하여 긴급하게 약관을 변경하는 때에는 금융위원회가 정하는 방법에 따라 이를 즉시 게시하고 이용자에게 알려야 한다.

④ 이용자는 제3항의 규정에 따른 약관의 변경내용이 게시되거나 통지된 후부터 변경되는 약관의 시행일 전의 영업일까지 전자금융거래의 계약을 해지할 수 있다. 전단의 기간 안에 이용자가 약관의 변경내용에 대하여 이의를 제기하지 아니하는 경우에는 약관의 변경을 승인한 것으로 본다.

핀테크 회사가 전자금융거래에 관한 약관을 제정하거나 변경(개정)하고자 하는 경우에는 약관의 시행일 1개월 전에 금융위원회에 사전보고하여야 한다.

[관계법령] 전자금융거래법 제25조

제25조(약관의 제정 및 변경)

① 금융회사 또는 전자금융업자가 전자금융거래에 관한 약관을 제정하거나 변경하고자 하는 경우에는 미리 금융위원회에 보고하여야 한다. 다만, 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융위원회가 정하는 경우에는 약관의 제정 또는 변경 후 10일 이내에 금융위원회에 보고할 수 있다.

② 금융위원회는 건전한 전자금융거래질서를 유지하기 위하여 필요한 경우에는 금융회사 또는 전자금융업자에 대하여 제1항의 규정에 따른 약관의 변경을 권고할 수 있다.

핀테크 회사는 전자금융거래를 위하여 접근매체를 선정하여 사용 및 관리하고 고객의 신원, 권한 및 거래지시의 내용 등을 확인하여야 하며, 접근매체를 발급할 때에는 고객의 신청이 있는 경우에 한하여 본인임을 확인한 후에 발급하여야 한다. 여기서 '본인임을 확인'한다는 것은 「금융실명법」상 실명확인을 의미한다.

[관계법령] 전자금융거래법 제6조, 전자금융감독규정 제37조

법 제6조(접근매체의 선정과 사용 및 관리)

① 금융회사 또는 전자금융업자는 전자금융거래를 위하여 접근매체를 선정하여 사용 및 관리하고 이용자의 신원, 권한 및 거래지시의 내용 등을 확인하여야 한다.

② 금융회사 또는 전자금융업자가 접근매체를 발급할 때에는 이용자의 신청이 있는 경우에 한하여 본인임을 확인한 후에 발급하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 이용자의 신청이나 본인의 확인이 없는 때에도 발급할 수 있다. (각 호 생략)

1. 선불전자지급수단 또는 제16조 제1항 단서의 규정에 따른 전자화폐인 경우
2. 접근매체의 갱신 또는 대체발급 등을 위하여 대통령령이 정하는 바에 따라 이용자의 동의를 얻은 경우

③ 누구든지 접근매체를 사용 및 관리함에 있어서 다른 법률에 특별한 규정이 없는 한 다음 각 호의 행위를 하여서는 아니 된다. 다만, 제18조에 따른 선불전자지급수단이나 전자화폐의 양도 또는 담보제공을 위하여 필요한 경우(제3호의 행위 및 이를 알선하는 행위는 제외한다)에는 그러하지 아니하다. (각 호 생략)

규정 제37조(인증 방법 사용기준)

금융회사 또는 전자금융업자는 전자금융거래의 종류 · 성격 · 위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.

접근매체란 전자금융거래에 있어서 거래지시를 하거나 고객 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단 또는 정보로서 인증서, 고객의 생체정보 등이 해당한다.

[관계법령] 전자금융거래법 제2조 제10호

10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
    가. 전자식 카드 및 이에 준하는 전자적 정보
    나. 「전자서명법」 제2조 제4호의 전자서명생성정보 및 같은 조 제7호의 인증서
    다. 금융회사 또는 전자금융업자에 등록된 이용자번호
    라. 이용자의 생체정보
    마. 가목 또는 나목의 수단이나 정보를 사용하는 데 필요한 비밀번호

2 「전자금융거래법」개정안[67)]

최근 유럽연합의 「지급결제산업지침(PSD2: The revised Payment Services Directive)」, 「전자적 신원확인 및 인증 등에 관한 법률(eIDAS: Regulation on electronic Identification, Authentication and Trust Services)」, 영국의 「지급결제산업법(Payment Services Regulations)」, 싱가포르의 「지급결제산업법(Payment Services Acts)」, 일본의 「자금결제에 관한 법률」 등의 제 · 개정에 이르기까지 해외 유수의 국가가 디지털금융의 중요성을 인식하고 디지털금융 분야에서의 경쟁과 혁신을 장려하기 위해 앞다투어 관련 법 · 제도를 정비하고 있다.

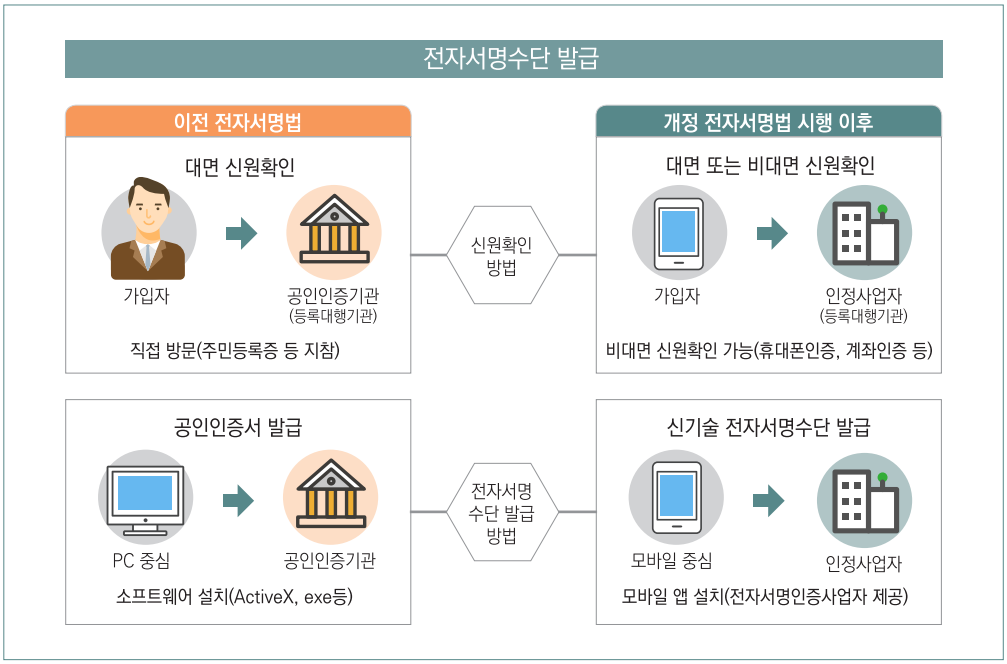
지급지시전달업과 종합지급결제사업자 제도의 도입, 현행 전자금융업의 기능별 통합 · 간소화, 최소자본금 등 진입규제와 후불결제업무 도입 등 영업행위규제의 합리화 등을 통해 디지털금융에서 경쟁과 혁신을 촉진하고 관련 산업을 건전하게 육성하며, 전자금융업자가 보유한 이용자예탁금에 대한 별도관리, 금융플랫폼 운영에 관한 영업행위 규율체계의 마련, 이용자가 허용하지 아니한 비대면거래에 대한 금융회사와 전자금융업자의 책임 확대 등을 추구하고 있다. 이를 통하여 국민들이 믿고 편리하게 디지털금융을 이용할 수 있도록 이용자 보호를 강화하고자 한다. 또한 오픈뱅킹과 전자지급거래청산업의 제도화, 비대면거래의 인증수단인 접근매체와 전자적 방식의 신원확인 관련 제도의 정비, 국내외 빅테크의 금융산업 진출에 대한 관리감독체계 마련 등으로 안전한 전자금융거래의 기반을 조성하고, 금융회사와 전자금융업자 등의 금융보안 거버넌스 강화, 전자금융업자 등의 업무위탁에 관한 규율체계 정비, 보안지원전담기관의 제도화 등을 통해 금융보안을 강화함으로써 인터넷전문은행, 금융규제샌드박스, 데이터 3법에 이어 디지털금융의 혁신과 안정을 위한 법 · 제도의 정비를 완결하도록 하였다. 한편, 현재의 전자금융거래의 범위를 확대하고 정부로 하여금 전자금융발전계획을 수립하고 디지털금융협의회를 설치 · 운영하도록 하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선 · 보완하려는 방향으로 「전자금융거래법」 개정안이 마련된다.

67) 정무위원회 수석전문위원 이용준(2021.2.), 전자금융거래법 일부개정법률안 검토보고

3 전자서명법[68)]

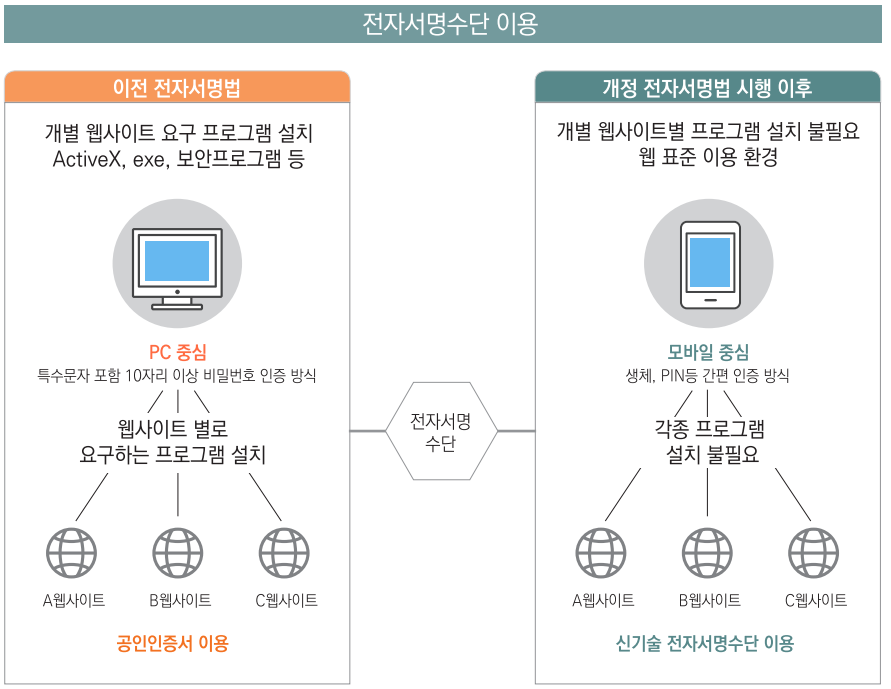
핀테크 회사는 인터넷 등 온라인에서 고객과 전자적 형태로 작성되어 송신 또는 수신되는 전자문서에 대해 (i) 신원확인, (ii) 거래내용의 변경 확인, (iii) 거래 사실에 대한 증명 등이 필요할 경우 「전자서명법」에 명시된 전자서명 관련 사항을 준수할 필요가 있다.

〈그림 Ⅳ-1〉「전자서명법」 개정 前과 後 전자서명수단 발급 안내자료



68) 과학기술정보통신부 보도자료, 전자서명법 시행령 개정안 국무회의 의결(2020.12.1.)

〈그림 Ⅳ-2 〉「전자서명법」 개정 前과 後 전자서명수단 발급 안내자료



[관계법령] 전자서명법 제2조 제2호

"전자서명"이란 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

가. 서명자의 신원

나. 서명자가 해당 전자문서에 서명하였다는 사실

[관계법령] 전자서명법 제3조 및 제6조

제3조(전자서명의 효력)

① 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다.

② 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.

제6조(다양한 전자서명수단의 이용 활성화)

① 국가는 생체인증, 블록체인 등 다양한 전자서명수단의 이용 활성화를 위하여 노력하여야 한다.

② 국가는 법률, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙, 대통령령 또는 감사원규칙에서 전자서명수단을 특정한 경우를 제외하고는 특정한 전자서명수단만을 이용하도록 제한하여서는 아니 된다.

우선, 공공분야는 행정안전부를 중심으로 민간 전자서명의 도입을 추진하고 있다. 특히, 전자서명법 개정에 따른 변화를 국민들이 조기에 체감할 수 있도록 2021년 1월부터 "홈택스 연말정산 간소화서비스(국세청), 정부24 연말정산용 주민등록등본 발급서비스(행안부), 국민신문고(국민권익위원회)" 등 주요 공공웹사이트에 민간 전자서명 도입을 적용하였다. 이를 위해 지난 2020년 9월 "공공분야 전자서명 확대 도입을 위한 시범사업"에 착수하여 카카오(카카오인증), KB국민은행(KB스타뱅킹), NHN페이코(페이코), 한국정보인증(삼성PASS), 통신3사(PASS) 등 5개 사업자를 후보 사업자로 선정하고 물리적 · 기술적 · 관리적 보안사항을 점검한 후, 사업자를 최종 확정하였다.[69]

69) 과학기술정보통신부 · 행정안전부 · 국민권익위원회 보도자료, 정부24 · 홈택스 등 주요 공공 누리집에 민간 전자서명 도입 (2021.1.11.)

〈그림 Ⅳ-3〉 연말정산용 주민등록등본 발급 서비스에 민간 전자서명 이용 예시

〈그림 Ⅳ-4〉 연말정산 간소화 서비스에 민간 전자서명 이용 예시

〈그림 Ⅳ-5〉 연말정산 간소화 서비스에 민간 전자서명 이용 예시

과학기술정보통신부는 국민들이 다양한 전자서명을 선택하는 데 도움을 주기 위해 전자서명인증의 안전성, 신뢰성 및 보안성 등을 확인해 주는 전자서명 평가·인정제도를 도입하여 운영하고 있다. 이를 위하여 2020년 12월 18일 과학기술정보통신부는 한국정보통신기술협회(TTA), 금융보안원, 딜로이트 안진회계법인 등 3개 기관을 전자서명인증사업자 평가기관으로 신규 선정한 바 있다. 전자서명인증사업자는 평가기관으로부터 전자서명의 운영기준[70] 준수 여부를 평가받고 인정기관(한국인터넷진흥원)의 승인을 받아 '전자서명인증업무 운영기준 준수사실 인정 증명서'를 발급받을 수 있다.[71]

70) 전자서명의 안전성·신뢰성 확보 및 가입자·이용자 보호를 위해 인증사업자가 지켜야 할 물리적·관리적·기술적 보안, 개인정보보호 등의 사항을 규정한 기준

71) 과학기술정보통신부·행정안전부·국민권익위원회 보도자료, 정부24·홈택스 등 주요 공공 누리집에 민간 전자서명 도입 (2021.1.11.)

4 전자문서법[72)]

2020년 12월 10일「전자문서법」개정으로, 전자문서의 법적 효력 및 서면요건 명확화, 종이문서 폐기 근거, 온라인 등기우편 활성화를 위한 공인전자문서중계자 제도가 개선되었다. 주요 내용은 다음과 같다.

첫째, 전자문서가 법적효력이 있음을 명시하고, 서면은 종이문서라는 고정관념에서 벗어나 전자문서도 일정한 요건[73)]을 갖추면 서면으로 볼 수 있게 되었다. 다만, 다른 법령에 특별한 규정이 있거나 성질상 전자적 형태가 허용되지 않는 경우는 제외된다. 이에 따라 다른 특별한 규정이 없는 한 각종 법령에서 요구되는 서면 · 문서에 의한 행위[74)]도 전자문서로 인정 받는다.

[관계법령] 전자적 형태를 허용하지 않는 경우

> 민법 제428조의2(보증의 방식)
> ① 보증은 그 의사가 보증인의 기명날인 또는 서명이 있는 서면으로 표시되어야 효력이 발생한다. 다만, 보증의 의사가 전자적 형태로 표시된 경우에는 효력이 없다.

둘째, 종이문서를 스캔하여 변환한 전자문서를 공인전자문서센터[75)]에 보관하는 경우, 해당 종이문서를 폐기할 수 있다.

셋째, 공인전자문서중계자(온라인 등기우편 사업자) 진입요건을 완화[76)]하여 신기술을 갖춘 혁신 중소기업들도 시장에 진입이 가능해짐에 따라 모바일 전자고지와 같은 국민 실생활에 편리성을 제공하는 新서비스가 다수 창출될 수 있게 되었다. 모바일 전자고지는 모바일앱, MMS 등으로 세금, 민방위 통지 등에 대한 정보를 받아볼 수 있는 서비스이다.

---

72) 과학기술정보통신부 · 법무부 보도자료,「전자문서 및 전자거래 기본법」, 12월 10일 시행(2020.12.10.)
73) 전자문서의 내용을 열람할 수 있고 전자문서가 작성 · 변환되거나 송신 · 수신 또는 저장된 때의 형태 또는 그와 같이 재현될 수 있는 형태로 보존되어 있을 것
74) 2018년 기준으로 3천여 개 법령의 2만여 개 조항에서 서면, 문서 등을 요구
75) 전자문서의 안전한 보관 및 증명 등의 업무를 수행하기 위해 과학기술정통부 장관으로부터 지정받은 전문기관
76) 진입요건 중 인력 · 재정기준을 폐지하고, 전자문서 유통에 필요한 설비 · 기술요건만 규정

5 금융위원회 — 금융분야 인증·신원확인 제도혁신 T/F[77]

최근 정보통신기술의 발전과 스마트폰의 대중화 추세 등은 인터넷 · 모바일뱅킹 등 온라인 · 비대면 전자금융거래를 보편화하였으며, 대면 거래에서도 태블릿PC 등 다양한 전자적 장치를 이용하는 사례가 급속도로 확산되고 있다. 이에 더해, 공인인증서의 지위를 폐지하는 「전자서명법」 개정안이 국회를 통과(2020.5.20.)하여 간편비밀번호, 지문 · 홍채 등을 활용한 생체인증 등 다양한 인증수단 간 경쟁이 기대되며, 국제적으로도 전자서명 · 인증 관련 법제도를 정비 중[78]이다.

금융위원회도 편리하면서도 안전한 다양한 인증 · 신원확인 수단이 경쟁할 수 있도록 제도를 지속적으로 개선해왔다.

① (2010.6월) 공인인증서 외에도 공인인증서와 동등한 수준의 안전성이 인정되는 인증 방법을 허용(「전자금융감독규정」 개정)
② (2015.3월) 전자금융거래에서 안전한 인증 방법을 자율적으로 채택할 수 있도록 공인인증서 사용 의무 폐지(「전자금융감독규정」 개정)
③ (2015.12월) 대면 확인이 원칙이었던 실명확인을 비대면 방식*으로 수행할 수 있도록 허용(「비대면 실명확인 가이드라인」 마련)
* 비대면 실명확인 시 아래 5가지 실명확인 방법 중 2개 이상을 중첩하여 적용
① 실명확인증표 사본 제출, ② 영상통화, ③ 위탁기관 등을 통하여 실명확인증표 확인, ④ 기 개설된 계좌를 이용한 소액 이체 등, ⑤ 기타 ①~④에 준하는 방식(생체인증 등)

그러나 현행 전자금융거래 시 인증 관련 규정이 다양한 디지털 신기술을 반영하기에는 여전히 한계가 있다. 또한, 오프라인 · 대면 확인을 전제로 하는 신원확인도 전자적 장치를 활용하는 대면거래, 디지털 신기술이 활용되는 비대면 거래의 현실을 충분히 반영하지 못한다는 지적이 제기되고 있다.

77) 금융위원회 보도자료, 전자금융거래의 편리성 · 안전성 확보를 위한 「금융분야 인증 · 신원확인 제도혁신 T/F」 1차 회의를 개최하였습니다(2020.6.3.)
78) 유럽연합은 「전자신원확인 및 인증 등에 관한 규정(eIDAS)」을 제정(2014년)하여 기술발전에 따른 다양한 인증 기술을 포용

이에 「금융혁신지원 특별법」에 따른 금융규제 샌드박스를 통하여 인증 · 신원확인 관련 규제에 대해 특례를 부여하여 다양한 서비스를 테스트 중이며, 테스트 진행상황 등을 감안하여 관련된 규정을 신속하게 정비하는 방안도 논의 중이다.

[참고자료] 규제샌드박스를 통해 테스트 중인 인증·신원확인 방식(총 14건)

① 신분증 없이 은행에 내방 시 은행 앱을 통한 본인인증, 기제출한 신분증 스캔 이미지를 이용한 신분증 진위 확인, 신분증 스캔 이미지와 실물 대조를 통해 실명확인(중소기업은행)
② 분산ID를 이용하여 실명확인 절차를 간소화하는 서비스(아이콘루프, 파운트, SKT)
③ 안면인식기술을 이용하여 실명확인증표의 사진과 고객이 직접 촬영한 얼굴 사진을 대조하는 방식을 비대면 실명확인 방법 중 한 가지(영상통화 대체)로 활용하는 서비스(한화투자증권, KB증권, DGB대구은행)
④ 얼굴 결제(FacePay)를 위하여 생체정보 등록 시 실명확인 절차 대신 신한카드가 정한 본인확인 절차를 거칠 수 있는 서비스(신한카드)
⑤ SMS/1원송금/USIM을 활용하여 추심이체 출금동의가 가능한 서비스(페이플, 세틀뱅크, 쿠팡, 삼성카드/케이에스넷/엘핀)

[참고자료] 비대면 실명확인 관련 혁신금융심사위원회(5.26.) 논의사항

① (혁신위 위원) 비대면 실명확인 관련 다양한 샌드박스 사례가 축적되고 있는 만큼, 테스트 경과 등을 바탕으로 관련 제도 개선을 검토할 필요
② (금융위원장) 코로나 이후 비대면 거래의 중요성이 부각되고 있으며, 비대면 실명확인과 관련한 샌드박스 역시 이러한 측면에서 의미가 있다고 생각
– 앞으로 비대면 실명확인 서비스의 안전성, 편리성 등 테스트 진행상황을 감안하여 제도개선을 고민 · 검토해 나가겠음

한편, 전자금융거래는 국민의 재산을 안전하게 관리하여야 하므로 인증에도 편리성과 보안성을 종합적으로 고려할 필요가 있다. 이러한 환경적 · 제도적 변화를 반영하여 인증 · 신원확인에 대한 새로운 규율체계 마련을 위해 T/F를 구성 · 운영하게 되었다.

T/F에서는 인증 · 신원확인 분야의 기술중립성, 독자적 산업 육성, 금융안정이라는 3가지 정책방향하에 앞으로 전자금융거래의 편의성 · 안전성 · 보안성을 확보할 수 있는 다양한 혁신적 인증수단이 개발 · 활용될 수 있도록 지원 · 검증가능한 체계를 구축하고 전자금융거래의 중요도 · 난이도 등 수준에 상응하는 신원확인방식을 구축하여 전자금융거래의 안전성과 실효성을 확보할 방안에 대해 논의해 나갈 계획이다.

참고로, 2021년 5월 20일 현재 기준 '금융분야 인증 · 신원확인 제도 혁신 T/F' 운영결과는 발표되지 않았다.

6 금융위원회 — 디지털금융 관련 정책 방향[79]

실명확인증표 중심[80]의 거래 관행이 디지털 新기술이 활용되는 대면 · 비대면 금융거래의 원활한 발전을 저해하고, 위조 신분증 등을 이용한 금융사기 등을 방지하기 위해서는 발전된 디지털 신기술을 활용한 신원확인 절차의 보완이 필요하게 되었다.

이를 위하여 비대면 · 전자적 장치를 통한 금융거래의 특성에 맞는 합리적인 신원확인 방식을 통해 제도의 실효성을 확보하고자 한다. 다만, 국민 재산 보호와 건전한 금융거래질서의 확립이라는 신원확인의 기본 원칙은 견지하여 제도의 안전성을 유지하고자 기존 실명확인증표 확인 외에 안전 · 보안성이 확보되는 디지털 新기술 기반의 신원확인 방식을 확대 허용하고, 신기술 활용 시 국민의 수용가능성 등을 고려하여 단계적으로 접근한다. 업종별(종합 · 이체 · 결제), 고객별(신규 · 기존)로 그에 따른 거래행위별 금융리스크 수준이 상이한 점 등을 종합 고려하여 신원확인 수준을 합리적으로 차등화한다. 현행 유권해석 · 가이드라인에 기반한 전자금융거래의 신원확인 제도를 법제화하여 명확성을 제고한다.

---

79) 금융위원회 보도자료 내 첨부, 4차 산업혁명 시대의 디지털금융 종합혁신방안 〈전자금융거래법령 등 개정방향〉(2020.7.24.)

80) 2015년부터 비대면 실명확인 허용(① 신분증 사본, ② 영상통화, ③ 접근매체 전달시 확인, ④ 기존계좌 활용, ⑤ 기타 중 2가지 확인) → 대부분 금융회사가 신분증 사본을 요구

제2절

해외 규제

핀테크 회사가 금융서비스를 제공하는 데 참고할 만한 해외 규제로는 유럽연합의 「전자인증규정(eIDAS)」, 미국 뉴욕주 「23 NYCRR 500」, 유럽연합 「지급결제산업지침(PSD2: The revised Payment Services Directive)」, 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)에서 발표한 사이버보안 로드맵 등이 있다.

1 유럽연합 — eIDAS[81)]

유럽연합의 「전자인증규정(eIDAS)」에서는 특정 요건을 만족하는 전자서명을 '적격 · 고급전자서명'으로 규정하여 민간의 다양한 전자서명기술이 통용 가능하도록 하였다.[82)]

eIDAS는 기존의 전자서명 지침(eSignature Directive (1999/93/EC)을 대체하고, 유럽 시민, 기업, 공공기관의 원활한 전자적 상호작용 및 새로 정의된 전자 '트러스트 서비스'의 범위에 대한 EU 차원의 법적 체계를 수립하는 것을 목적으로 한다. 구체적으로 이용자들이 각각 거래하는 나라마다 여러 개의 서명을 만들어야 하는 문제점을 해결하기 위해, "통일된 한 가지 수단(eIDAS)"으로 안전한 거래를 하기 위한 목적으로 제정되었다. (i) 개인과 기업이 자국의 eID(전자신원확인, electronic identification, eID)를 이용해 타 EU 국가들의 공공 서비스에 접근할 수 있도록 하고, (ii) 전자서명, 전자문서, 웹사이트 인증 등 전자 트러스트 서비스(electronic trust services)를 위한 유럽의 내부 시장을 조성해 기존의 서면(書面) 기반 프로세스와 동일한 법적 지위를 확보할 수 있도록 하기 위해서이다.

81) 한국인터넷진흥원, 해외 개인정보보호 동향 보고서(2018년 4월 4주)
82) 금융위원회 보도자료 내 첨부, 4차 산업혁명 시대의 디지털금융 종합혁신방안 〈전자금융거래법령 등 개정방향〉 (2020.7.24.)

2 미국 뉴욕주 – 23 NYCRR 500

미국 뉴욕주 금융청(Department of Financial Services)이 은행업 또는 보험업 인가를 받은 금융회사가 준수하여야 할 요구사항으로, 사이버안전규정(23 NYCRR 500)[83]에서 다중인증(Multi-Factor Authentication)[84]과 위험기반인증(Risk-Based Authentication)에 대해 규정하고 있다.

[관계법령] NYCRR 500 Section 500.01 Definitions

(f) Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(l) Risk-Based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's

구체적으로 금융회사는 위험평가를 기반으로 비공개정보 또는 정보처리시스템에 대해 권한 없는 자의 접근을 차단하기 위하여 다중 인증을 포함한 효과적인 제어방안을 사용하여야 한다.

83) NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES 23 NYCRR 500 (Title: CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES)

84) 최소 두 가지 이상의 인증 요소를 이용하여 본인 여부를 인증하는 것(출처: 한국정보통신기술협회 정보통신용어사전)

[관계법령] NYCRR 500 Section 500.12 Multi-Factor Authentication

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

특히, 금융회사는 제3의 서비스제공자에 대한 보안정책을 수립함에 있어, 다중 인증을 포함한 접근제어 정책과 절차를 마련하여야 한다.

[관계법령] NYCRR 500 Section 500.11 Third Party Service Provider Security Policy

Section 500.11 Third Party Service Provider Security Policy.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

3 유럽연합 — PSD2

유럽연합은 지급결제서비스를 제공자가 준수해야 하는 지침을 통해 '인증, 강화된 고객인증(Strong Customer Authentication), 개인화된 보안인증서(Personalised Security Credentials)'에 대해 정의하고 있다. 여기서 인증이란 서비스제공자가 개인화된 보안인증서 사용 등을 통해 지급결제서비스 이용자의 신원확인, 지급수단의 사용에 대한 유효성 등을 하는 것을 의미하고, 강화된 고객인증이란 지식기반, 소유기반, 존재기반(또는 생체기반) 인증 방법 중 2개 이상의 요소를 결합하여 인증하는 것을 의미한다.

[관계법령] Payment Services 2 (PSD 2) – Directive (EU) 2015/2366, Article 4 Definitions

(29) 'authentication' means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;

(30) 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

(31) 'personalised security credentials' means personalised features provided by the payment service provider to a payment service user for the purposes of authentication;

4 미국 NIST – 사이버보안 로드맵

미국 국립표준기술연구소인 NIST는 사이버보안 프레임워크(Cybersecurity Framework) 관련하여 3가지 주요 개정내용을 발표하였고, 이 중 하나로 '인증(Authentication)'이라는 용어를 권한부여(또는 인가, Authorization)와 신원증명(Identity Proofing)과 같은 중요한 기술적 주제의 광범위한 범위를 설명하기 위해 '식별 및 접근(Identity and Access Management)' 용어로 변경하는 것이다.

이 내용의 의미는 비대면 업무방식이 확대되면서 사이버보안을 위하여 인증이라는 단순한 기술적인 기준이 아닌 생체인증을 통한 권한부여와 신원증명이라는 개념의 적용이 필요하다는 것으로, 핀테크 회사가 금융서비스를 제공함에 있어 본인인증 또는 보안인증이라는 기술 및 절차만을 고려하지 말고 권한부여와 신원증명이라는 기술 및 절차도 함께 고려하여야 한다는 점이다.

[참고자료] NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 (April 25, 2019)

Identity and Access Management solutions have continued to evolve and improve since the Framework's initial release, with both the public and private sectors making progress toward developing and implementing stronger standards, processes, technologies, and protocols. In particular, multi-factor authentication (MFA) solutions are increasingly used to augment passwords. New protocols are aimed at bringing easy-to-use and cost-effective MFA solutions to the consumer masses, with support by nearly every major browser and mobile manufacturer. These technologies are also being paired with biometric technology to make strong authentication more common and user-friendly, and increasingly, password-less. While adoption is trending in the right direction, the rate falls short of what is needed to best protect against cybersecurity threats, especially with a report that "81% of hacking-related breaches [leveraging] either stolen and/or weak passwords."

제3절

사고 및 위반 사례

1 (#1) 사고 사례

업무 성격상 불필요하다고 판단되는 업무에 접속 가능한 ID/PW를 부여하였고, 퇴직자가 재직 시 사용한 ID/PW를 그대로 유지한 상황에서 해커가 위 ID/PW를 습득하여 약 175만 명의 고객정보를 탈취한 사건이다.

[참고자료] 2011년 5월 17일 자 금융감독원 보도자료 중 일부 발췌

'11.3.6~4.7 기간 중 해커가 업무관리자의 ID/PW[85]를 습득한 후, 보조서버인 광고메일발송서버와 정비내역조회서버에 침입하여 화면복사 또는 해킹프로그램 설치/다운로드 방식으로 약 175만 명의 고객정보를 해킹한 것으로 드러났음

사고발생원인 (인증관련 내용만 일부 발췌)

- 업무 성격상 불필요한 ID/PW 부여[86] 및 담당직원 퇴직(1명) 후 ID/PW 미삭제[87]
- 해킹사고 발생 시 정보유출을 최소화할 수 있는 고객 비밀번호 암호화[88] 및 업무관리자의 화면 조회 시 주민번호 뒷자리 숨김표시[88] 미조치 등

출처: 금융감독원, 현대캐피탈 해킹사고 검사결과 중간발표(2011.05.18), http://www.fss.or.kr

85) 외부에서 광고메일 발송 서버에 접속한 ID/PW 2개 및 퇴직자의 ID/PW 1개
86) 외부에서 광고메일서버에 접속 가능한 ID/PW(5개) 부여.
87) 퇴직자가 재직 시 사용하던 ID/PW로 정비내역조회서버에 총 7회 무단 접속
88) DB서버(메인시스템)내에 보관 중인 고객 비밀번호는 암호화하고 있으나, 고객정보 조회・생성・변경사실 등이 기록되는 로그파일에 남아 있는 고객 비밀번호 암호화는 미실시

[관련법령] 전자금융감독규정 제13조 제1항 제1호, 2호, 14호 및 제17조 제1항 제2호

제13조(전산자료 보호대책)

① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.

1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것

14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

제17조(홈페이지 등 공개용 웹서버 관리대책)

① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것

출처: 방송통신위원회, 방통위, KT 개인정보 유출 사고 관련 조사(2012.7.31), https://kcc.go.kr

2 (#2) 사고 사례

해커가 해킹프로그램을 이용하여 통신사의 고객정보를 저장한 데이터베이스에 침입하여 2012.2.20.부터 2012.7.13.까지의 고객의 개인정보(주민등록번호, 휴대전화번호, 주소 등) 1,000만 건 이상을 위법하게 탈취한 사건이다.

[참고자료] 2012년 7월 31일자 보도자료 내용 중 일부 발췌

방송통신위원회(이하 방통위)는 KT 개인정보 유출 사건과 관련하여 해당 사업자가 개인정보보호의 기술적 · 관리적 보호조치 기준 등 개인정보보호 관련 법규를 준수했는지 여부를 면밀히 조사중이라고 밝혔다.

이에 앞서 지난 30일 경찰청은 해킹 프로그램을 제작하여 자신이 운영하는 TM사업에 이용하거나 타 TM 업체에 제공 · 판매할 목적으로 KT의 휴대전화 고객정보를 유출 · 판매한 해커 등 9명을 검거하고, 유출한 고객정보와 해킹한 KT 고객정보를 전송받아 총괄 저장하고 있는 모든 DB서버를 압수 · 회수 조치했다고 발표한 바 있다.

이와 같은 조치에도 불구하고 발생할 수 있는 추가적인 피해를 방지하기 위하여 방통위는 해당 사업자로 하여금 개인정보가 유출된 이용자에게 즉각 해당 사실을 알리도록 하고, 홈페이지를 통해 유출 사실을 공개하도록 하였다.

또한, 개인정보 침해대응 핫라인(109개 인터넷사업자)를 통해 이러한 사실을 전파하여 개인정보의 불법 유출로 인한 2, 3차 추가 피해를 방지하도록 조치하였다.

출처: 방송통신위원회, 방통위, KT 개인정보 유출 사고 관련 조사(2012.7.31)
https://kcc.go.kr

3 (#3) 사고 사례

해커가 다른 사람의 ID/PW로 통신사 홈페이지에 접속하여 약 1,200만 명의 개인정보의 탈취한 사건으로, 홈페이지 구축 당시부터 본인인증 또는 보안인증 절차를 제대로 검증하지 않은 것이 원인인 사건이다.

[참고자료] 2014년 3월 7일자 공지사항 중 일부 발췌

[원인]

- 고객 개인정보 요청 시 인증 절차 미흡
  - KT 고객센터 홈페이지는 요금 명세서 조회 시 명세서 계정번호를 서버에 전송하여 해당 사용자의 정보를 수신하고 있음
  - 이때 KT 서버에 전달하는 명세서 계정번호가 로그인한 사용자의 것인지 확인하는 인증 절차가 없음
  - 따라서 로그인 후, 해킹도구(파로스)로 명세서 계정번호를 변조하여 타인의 개인정보를 수집

[대책]

- 명세서 계정번호에 대한 사용자 일치 확인
  - 로그인한 사용자로부터 전송받은 데이터(명세서 계정번호 등의 특수 고유식별 데이터)가 해당 사용자의 데이터인지에 대한 일치여부 확인 과정 추가 필요
- 특정 IP에서 비정상적으로 과도한 명세서 등의 조회 시도 모니터링 및 차단 정책 필요

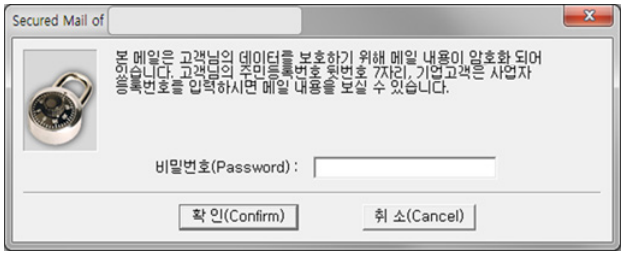
출처: (사)한국침해사고대응팀협의회, KT 개인정보 유출 사고 관련 조사(2014.3.7)
https://concert.or.kr/

4 (#1) 위반 사례

고객에게 고지서, 명세서 등을 보안메일로 발송하여 해당 보안메일을 열람하기 위해 입력하는 정보를 주민번호 뒷자리(7자)가 입력되도록 할 경우 주민등록번호 처리 제한에 대한 위반으로 「개인정보 보호법」상 3천만원 이하의 과태료 대상이 된다.

〈그림 Ⅳ-6〉 주민번호 앞자리(6자)를 입력하는 보안메일

〈그림 Ⅳ-7〉 주민번호 뒷자리(7자)를 입력하는 보안메일



[관계법령] 개인정보 보호법 제24조, 제24조의2 및 제75조

제24조(고유식별정보의 처리 제한)

① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조 제2항 각 호 또는 제17조 제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

제24조의2(주민등록번호 처리의 제한)

① 제24조 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우

제71조(벌칙)

다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

4. 제24조 제1항을 위반하여 고유식별정보를 처리한 자

제75조(과태료)

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

4의2. 제24조의2 제1항을 위반하여 주민등록번호를 처리한 자

2014년 1월 안전행정부(現 행정안전부)가 공개한 주민등록번호 수집금지 제도 가이드라인의 주민번호 수집금지 정책에 관련하여 다음의 Q&A에서도 주민번호 앞자리(생년월일)의 경우 고객의 동의를 받아 수집 · 이용이 가능하지만, 주민번호 뒷자리의 경우는 법령상 구체적인 수집 근거가 없다면 수집 · 이용할 수 없다고 설명하고 있다.

[Q&A] 주민번호 앞자리(생년월일) 사용 가능 여부

[Q] 주민번호 앞자리(생년월일)는 사용 가능한가요?

[A] 주민번호 앞자리의 생년월일은 주민번호의 체계에 따라 생성되는 것이 아니라, 출생신고 시 국민이 공공기관에 신고한 날짜를 토대로 정의되는 숫자 열입니다. 따라서, 생년월일은 주민번호를 이용한 숫자열이라 보기 어려우며, 이용자의 동의를 받아 수집 · 이용이 가능합니다.

[Q&A] 주민번호 뒷자리 사용 가능 여부

[Q] 주민번호 뒷자리만 사용하는 것은 괜찮은가요?

[A] 주민번호의 뒷자리를 수집 · 이용하여 회원의 유일성과 식별성을 확보하는 것은 주민번호의 체계를 활용하여 주민번호의 고유한 특성을 이용하는 것이므로 주민번호를 수집 · 이용하는 경우에 해당한다고 볼 수 있습니다. 따라서, 법령상 주민번호를 수집할 수 있는 구체적 근거가 없다면 주민번호의 뒷자리를 수집 · 이용할 수 없습니다.

5 (#2) 위반 사례

「신용정보법」 제19조, 제20조 등에 따라 신용정보회사등은 취급중인 개인신용정보 유출 등을 방지하기 위한 기술적 · 관리적 보안대책을 수립 · 시행하여야 한다. 그럼에도 개인신용정보 관리 불철저로 인한 개인신용정보의 유출로 제재받은 건이다.

[관련자료] 금융감독원 제재결과 내용

신용회복위원회는 사이버지부 홈페이지의 개인신용정보 조회서비스를 제공하는 과정에서 보안대책을 제대로 이행하지 않은 결과, 2013.6.1.~2017.4.5. 기간 중 공인인증서 및 휴대폰 본인인증 없이 27,935명(53,680건)의 개인신용정보가 유출되는 결과를 초래하였음

구체적으로, 2011년 3월 홈페이지에 '나의신용정보조회' 메뉴를 신설하면서 기술적 보안성에 대한 검수·확인을 적절히 이행하지 않아 개인신용정보 조회를 위한 본인인증 절차가 우회되는 등 기술적 보안대책을 소홀히 하였고, 2016년 12월경부터 휴대폰 본인인증 실패율이 급증(9.74%→14.85%)하는 등 본인인증 관련 이상 징후가 나타나고 있었음에도 약 3개월간 원인점검 등 신용정보 유출을 방지하기 위한 적절한 활동이 없는 등 관리적 보안대책을 소홀히 함

출처: 금융감독원, 검사결과제재(제재조치일: 2018.1.19.),
Retrieved from https://www.fss.or.kr

6 (#3) 위반 사례

「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제17조 제1항 제2호 및 제4호에 따라 금융회사는 공개용 웹서버에 접근할 수 있는 사용자 계정은 아이디·비밀번호 이외에 추가 인증수단을 적용하여야 하고, DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니하여야 하는데도 홈페이지 등 공개용 웹서버 관리 소홀로 제재받은 건이다.

[관련자료] 금융감독원 제재결과 내용

SCI평가정보는 여러 홈페이지를 관리하는 데 담당 직원이 사용자 계정으로 접속할 때 아이디·비밀번호만을 사용하고 추가 인증수단을 적용하지 않았음

2017.12.19. DMZ구간에서 운영하는 2개 홈페이지의 웹서버의 거래로그를 점검한 결과 해당 로그에 이름, 전화번호, 주소 등 총 116건의 이용자 정보를 암호화하지 않고 저장한 사실이 있음

출처: 금융감독원, 검사결과제재(제재조치일: 2018.10.16.),
Retrieved from https://www.fss.or.kr

7 (#4) 위반 사례

「금융실명법」 제3조 및 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제5조의2 등에 의하면, 금융회사 등은 거래자의 실지명의를 확인한 후 계좌를 개설하여야 한다. 만약 대리인이 본인의 가족으로서 계좌 개설을 신청하는 경우 대리인의 실명확인증표, 발급일로부터 3개월 이내의 유효한 가족관계확인서류를 징구하여야 하고 가족이 아닌 대리인이 계좌 개설을 신청하는 경우 본인 및 대리인의 실명확인증표, 인감증명서 또는 본인서명사실확인서, 인감날인 또는 서명이 기재된 위임장을 징구하여야한다. 그럼에도 금융거래 실명확인 의무 및 고객확인 의무 위반으로 제재받은 건이다.

[관련자료] 금융감독원 제재결과 내용

2017.1.16. □□□(2011.10.22. 사망) 명의의 정기예금계좌 1건 (90백만 원), 2017.1.17. 청약저축계좌 1건(15백만 원), 2017.4.4. 정기예금계좌 1건(50백만 원)을 대리인 △△△(□□□의 모)의 신청에 따라 개설할 때 대리인의 실명확인증표를 징구하면서 가족관계확인서류로 인정되지 않는 서류(제적등본)를 징구하여 실명확인을 함으로써 금융거래 실명확인 의무 및 고객확인 의무를 위반하였음

2016.7.27. ㉥㉥㉥명의의 증권계좌 1건(0원)을 본인의 신청에 따라 개설할 때 거래자의 실명확인증표를 징구하였으나 전산조작 실수로 동명이인인 ㉥㉥㉥(2010.3.26. 사망) 명의로 계좌를 개설하여 금융거래 실명확인 의무 및 고객확인 의무를 위반하였음

출처: 금융감독원, 검사결과제재(제재조치일: 2019.6.12.),
Retrieved from https://www.fss.or.kr

핵심정리

1. 국내 규제

- **전자금융거래법**
  - 「전자금융거래법」은 전자금융업을 함에 있어서 가장 중요한 규제 중 하나이며, 금융회사, 전자금융업자, 전자금융보조업자 등 전자금융서비스를 제공하는 회사가 준수해야 하는 내용을 포함하고 있다.
  - 동법 하위 규정으로 「전자금융감독규정」이 있으며, 전자금융업을 영위하는 회사는 해당 규정에서 말하는 선량한 관리자로서의 주의 노력을 해야 하며, 해당 규정을 위반하거나 주의 의무를 다하지 않을 경우 5천만원 이하의 과태료 부과 등 제재가 발생할 수 있다.
  - 최근 이슈로는 네트워크 보안 관점에서의 망분리가 있으며, 핀테크 회사의 경우 유연근무, 스마트워크 등 근무환경의 편의성이 있으나 망분리 의무에 소홀한 경우가 있어 이를 주의해야 한다. (과태료 처분 사례 발생)

- **「전자금융거래법」개정안**
  - 지급지시전달업과 종합지급결제사업자 제도의 도입, 현행 전자금융업의 기능별 통합 · 간소화, 최소자본금 등 진입규제와 후불결제업무 도입 등 영업행위규제의 합리화 등을 통해 디지털금융에서 경쟁과 혁신을 촉진하고 관련 산업을 건전하게 육성하며, 전자금융업자가 보유한 이용자예탁금에 대한 별도관리, 금융플랫폼 운영에 관한 영업행위 규율체계의 마련, 이용자가 허용하지 아니한 비대면거래에 대한 금융회사와 전자금융업자의 책임 확대 등을 추구하고 있다. 이를 통하여 국민들께서 믿고 편리하게 디지털금융을 이용할 수 있도록 이용자 보호를 강화하고자 한다. 오픈뱅킹과 전자지급거래청산업의 제도화, 비대면거래의

인증수단인 접근매체와 전자적 방식의 신원확인 관련 제도의 정비, 국내외 빅테크의 금융산업 진출에 대한 관리감독체계 마련 등으로 안전한 전자금융거래의 기반을 조성하고, 금융회사와 전자금융업자 등의 금융보안 거버넌스 강화, 전자금융업자 등의 업무위탁에 관한 규율체계 정비, 보안지원전담기관의 제도화 등을 통해 금융보안을 강화함으로써 인터넷전문은행, 금융규제샌드박스, 데이터 3법에 이어 디지털금융의 혁신과 안정을 위한 법·제도의 정비를 완결하도록 하였다. 한편, 현재의 전자금융거래의 범위를 확대하고 정부로 하여금 전자금융발전계획을 수립하고 디지털금융협의회를 설치·운영하도록 하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하려는 방향으로 「전자금융거래법」 개정안이 마련된다.

- **전자서명법**
  - 핀테크 회사는 인터넷 등 온라인에서 고객과 전자적 형태로 작성되어 송신 또는 수신되는 전자문서에 대해 (i) 신원확인, (ii) 거래내용의 변경 확인, (iii) 거래 사실에 대한 증명 등이 필요할 경우 「전자서명법」에 명시된 전자서명 관련 사항을 준수할 필요가 있다.

- **전자문서법**
  - 2020년 12월 10일 「전자문서법」 개정으로, 전자문서의 법적 효력 및 서면요건 명확화, 종이문서 폐기 근거 마련, 온라인 등기우편 활성화를 위한 공인전자문서중계자 제도 개선사항을 반영하고 있다.

2. 해외 규제

- 유럽연합 eIDAS
  - 유럽연합의 「전자인증규정(eIDAS」에서는 특정 요건을 만족하는 전자서명을 '적격 · 고급전자서명'으로 규정하여 민간의 다양한 전자서명기술이 통용 가능하도록 하였다.[89)]
  - eIDAS는 기존의 전자서명 지침(eSignature Directive (1999/93/EC)을 대체하고, 유럽 시민, 기업, 공공기관의 원활한 전자적 상호작용 및 새로 정의된 전자 '트러스트 서비스'의 범위에 대한 EU 차원의 법적 체계를 수립하는 것을 목적으로 한다.

- 미국 뉴욕주 23 NYCRR 500
  - 23 NYCRR 500은 미국 뉴욕주 금융청(금융감독원)에서 은행업이나 보험업을 인가받은 금융회사가 준수해야하는 규제를 정의하고 있으며, 보안인증과 관련해서는 다중 인증과 위험기반 인증의 내용이 포함되어 있다.
  - 다중 인증은 하나의 인증수단이 아니라 서로 다른 인증방식을 두가지 이상 적용하여 인증하는 것을 말하고, 위험기반인증은 위험평가를 기반으로 비공개정보나 정보처리시스템에 권한이 없는 자의 접근을 차단하는 것을 말한다.

89) 금융위원회 보도자료 내 첨부, 4차 산업혁명 시대의 디지털금융 종합혁신방안 〈전자금융거래법령 등 개정방향〉(2020.7.24.)

- 유럽연합 PSD2
  - PSD2는 지급결제서비스제공자가 준수해야하는 지침으로 인증, 강화된 고객인증, 개인화된 보안인증서 개념이 포함되어 있다. 이 지침에서의 인증은 서비스제공자가 개인화된 보안인증서로 신원확인, 지급수단의 유효성을 검증하는 것을 의미하고 강화된 고객인증은 다중인증과 같은 2개 이상의 인증을 이용하는 것을 말한다.

- 미국 NIST
  - NIST는 미국 국립표준기술연구소이나 현실적으로 국제적 표준을 제안하는 기관이라 할 수 있다. NIST에서는 다양한 보안기술 가이드라인을 배포하고 있으며, 일부 가이드라인에는 인증과 신원증명의 개념, 해당 기술의 안전성 등급 등이 포함되어 있다.

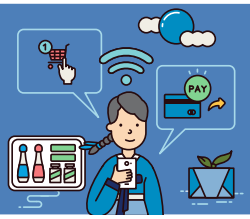
MEMO

헬로, 핀테크!(보안인증 · 블록체인)

5장

보안인증 관련 고려사항

5장 보안인증 관련 고려사항



학습목표

1. 보안인증의 기본원칙을 이해하고 설명할 수 있다.
2. 인증서, 생체정보, API 및 스크래핑, 마이데이터 관련 사례를 통해 보안인증을 실무에 적용할 때 고려하여야 사항을 확인할 수 있다.

학습개요

핀테크 회사는 자율에 따라 보안인증 관련 기술과 절차를 도입하여 사용할 수 있다. 전자문서 및 전자서명의 경우 (i) 전자문서의 효력, (ii) 전자서명 방식의 개선에 대해 고려할 필요가 있고, 생체정보의 경우, (iii) 「전자금융거래법」상 전자금융보조업자의 역할과 책임, (iv) 생체정보 처리에 따른 역할과 책임에 대한 고려, API 및 스크래핑의 경우 (v) 스크래핑 사용가능 여부, (vi) 이용약관 위반의 주체에 대해서도 고려할 필요가 있다. 마지막으로 마이데이터의 경우, (vii) 본인인증의 목적, (viii) 인증수단에 대해 고려할 필요가 있다.

용어해설

❶ API(Application Programming Interface)

"특정 프로그램의 기능이나 데이터를 다른 프로그램이 접근할 수 있도록 미리 정한 규칙" 또는 "네트워크상으로 서로 다른 프로그램 간 기능 · 데이터를 연결하는 매개체의 역할"을 의미한다.

❷ 스크래핑

인터넷 웹사이트 화면에서 보이는 데이터 중 필요한 데이터를 자동적으로 수집 · 저장하는 기술을 의미한다.

❸ 마이데이터 서비스 가이드라인

금융위원회 및 한국신용정보원이 발행한 '금융분야 마이데이터 서비스 가이드라인 (2021.2.)'을 의미한다.

❹ 마이데이터 기술 가이드라인

금융위원회 및 금융보안원이 발행한 '금융분야 마이데이터 기술 가이드라인 (2021.2.)'을 의미한다.

제1절

기본 원칙

핀테크 회사는 자율에 따라 보안인증 관련 기술과 절차를 도입하여 사용할 수 있고, 금융규제를 직접 적용받은 핀테크 회사의 경우도 기존보다는 완화된 금융규제를 적용받고 있다.

1 안전성의 확보의무

「전자금융거래법」은 전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전성과 신뢰성을 확보함과 아울러 전자금융업의 건전한 발전을 위한 기반조성을 함으로써 국민의 금융편의를 꾀하고 국민경제의 발전에 이바지함을 목적으로 한다(법 제1조).

이에 안전성의 확보의무에 따라 핀테크 회사가 전자금융업자 또는 전자금융보조업자로서의 역할을 수행할 경우 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 하며(법 제21조 제1항), 기본 원칙은 제2항 및 제3항과 같다.

[관계법령] 전자금융거래법 제21조 제2항 및 제3항

법 제21조(안전성의 확보의무)

② 금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증 방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.

③ 금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.

제2절

전자문서 및 전자서명 사례

1 전자문서의 효력

「민법」에 따르면 보증은 그 의사가 보증인의 기명날인 또는 서명이 있는 서면으로 표시되어야 효력이 발생하며, 보증의 의사가 전자적 형태로 표시된 경우에는 효력이 없다(민법 제428조의2 제1항). 그러나 「전자서명법」에서는 전자서명이 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 않으며(전자서명법 제3조 제1항), 「전자문서법」에서는 전자문서가 전자적 형태로 되어 있다는 이유만으로 법적 효력이 부인되지 아니하고(전자문서법 제4조 제1항), 보증인이 자기의 영업 또는 사업으로 작성한 보증의 의사가 표시된 전자문서는 「민법」 제428조의2 제1항 단서에도 불구하고 같은 항 본문에 따른 서면으로 본다고 규정되어 있다. 따라서 보증인이 자기의 영업 또는 사업으로 작성한 보증의 의사가 표시된 전자문서 및 전자서명의 경우 효력이 없다고 해석될 가능성이 없다고 볼 수 있다.

[관계법령] 민법 제428조의2 제1, 제2, 제3항

법 제428조의2(보증의 방식)

① 보증은 그 의사가 보증인의 기명날인 또는 서명이 있는 서면으로 표시되어야 효력이 발생한다. 다만, 보증의 의사가 전자적 형태로 표시된 경우에는 효력이 없다.

② 보증채무를 보증인에게 불리하게 변경하는 경우에도 제1항과 같다.

③ 보증인이 보증채무를 이행한 경우에는 그 한도에서 제1항과 제2항에 따른 방식의 하자를 이유로 보증의 무효를 주장할 수 없다.

[관계법령] 전자서명법 제3조

제3조(전자서명의 효력)

① 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다.

② 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.

[관계법령] 전자문서법 제4조

제4조(전자문서의 효력)

① 전자문서는 전자적 형태로 되어 있다는 이유만으로 법적 효력이 부인되지 아니한다.

② 보증인이 자기의 영업 또는 사업으로 작성한 보증의 의사가 표시된 전자문서는 「민법」 제428조의2제1항 단서에도 불구하고 같은 항 본문에 따른 서면으로 본다.

2 전자서명 방식의 개선

2021년 5월 17일 금융위원회는 모바일 청약 시 반복서명 절차를 폐지한다는 내용의 보험 대면모집 관련 개선방안을 발표하였다.[90] 구체적으로 이 개선방안에는 기존 설계사가 계약자를 만나서 중요사항을 설명하면, 보험계약 서류작성 등 청약절차는 모바일로 진행할 수 있으나 이 과정에서 소비자는 작은 휴대폰 화면 등에서 모든 서류에 반복해서 전자서명을 해야 해서 불편을 겪었다. 이를 개선하고자 전자서명 입력은 청약절차 시작 시 1회만 하고, 소비자가 계약 중요사항 및 각각의 서류내용을 꼼꼼하게 확인하여 서명란을 클릭 확인하도록 개선[91]하였다.

90) 금융위원회 · 금융감독원 · 생명보험협회 · 손해보험협회, 소비자 보호의 실효성은 높이고 보험모집의 비효율은 낮출 수 있도록「비대면 디지털 모집 규제」를 개선하겠습니다[보험업법 시행령 및 감독규정 등 입법예고](2021.5.17.)

91) 전체 일괄동의 또는 일괄서명 방식은 금지되며, 각 항목별로 별도 페이지(팝업) 등에서 "확인"하도록 조치하고 전자서명법상 전자서명에 부합되도록 시스템 구현 필요

〈그림 Ⅴ-1〉 청약서류 서명방법(예시)

출처: 금융위원회(2021) 보험업법 시행령 및 감독규정 등 입법예고

제3절

생체정보 사례

1 전자금융거래법상 전자금융보조업자의 역할과 책임

핀테크 회사가 금융회사 또는 전자금융업자를 위하여 「전자금융거래법」의 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 경우「전자금융거래법」상 전자금융보조업자의 역할을 수행한다고 할 수 있다. 핀테크 회사가 전자금융업자일 경우 전자금융보조업자의 고의나 과실로 인한 손해 발생 시에는 그 손해배상에 대한 구상권을 전자금융보조업자에게 청구할 수 있으나, 핀테크 회사가 전자금융보조업자일 경우 금융회사 또는 전자금융업자로부터 구상권을 청구 받을 수 있다.

[관계법령] 전자금융거래법 제2조 제5호 및 제11조 및 전자금융감독규정 제3조

법 제2조(정의)

5. "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

법 제11조(전자금융보조업자의 지위)

① 전자금융거래와 관련하여 전자금융보조업자(전자채권관리기관을 포함한다. 이하 이 장에서 같다)의 고의나 과실은 금융회사 또는 전자금융업자의 고의나 과실로 본다.

② 금융회사 또는 전자금융업자는 전자금융보조업자의 고의나 과실로 인하여 발생한 손해에 대하여 이용자에게 그 손해를 배상한 경우에는 그 전자금융보조업자에게 구상할 수 있다.

③ 이용자는 금융회사 또는 전자금융업자와의 약정에 따라 금융회사 또는 전자금융업자에게 행하는 각종 통지를 전자금융보조업자에게 할 수 있다. 이 경우 전자금융보조업자에게 한 통지는 금융회사 또는 전자금융업자에게 한 것으로 본다.

규정 제3조(전자금융보조업자의 범위) 법 제2조 제5호에서 "금융위원회가 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 정보처리시스템을 통하여 「여신전문금융업법」상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
2. 정보처리시스템을 통하여 은행업을 영위하는 자의 자금인출업무, 환업무 및 그 밖의 업무를 지원하는 사업자
3. 전자금융업무와 관련된 정보처리시스템을 해당 금융회사 또는 전자금융업자를 위하여 운영하는 사업자
4. 제1호부터 제3호의 사업자와 제휴, 위탁 또는 외부주문(이하 "외부주문등"이라 한다)에 관한 계약을 체결하고 정보처리시스템을 운영하는 사업자

2 생체정보 처리에 따른 역할과 책임

생체정보를 처리하는 방식에 따라 서버검증형과 단말검증형으로 구분된다. 서버검증형의 경우, 최초 스마트폰 등 생체인식단말을 통해 고객의 생체정보를 수집하여 특징정보를 추출한 후 특징정보를 핀테크 회사의 인증서버로 전송하여 등록 및 저장한다. 이후 고객의 인증절차 수행이 필요한 경우 고객의 지문정보를 수집하여 핀테크 회사의 인증서버에 등록된 정보와 비교하는 방식이다. 이외에도 적용 사례(2장 3절)와 같이 고객의 생체 정보를 분할하여 핀테크 회사와 분산관리센터가 각각 보관하고 실제 거래 시 해당 정보를 결합하여 인증하는 방식도 있다.

단말검증형의 경우, 본 교재 본문 58~59면에서 설명된 기술 구성방식의 '〈그림 II-8〉 FIDO 등록과정'과 '〈그림 II-9〉 FIDO 인증과정'을 참고하면 된다. 단말검증형 방식을 사용할 경우 스마트폰 등 생체인식단말에 단말검증형 기술을 제공한 회사는 핀테크 회사를 위해 생체정보를 처리하는 방식으로 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자에 해당하는 전자금융보조업자가 될 수 있고, 전자금융보조업자의 고의나 과실로 인하여 발생한 손해에 대하여 핀테크 회사가 이용자에게 그 손해를 배상한 경우에는 그 전자금융보조업자에게 구상할 수 있다.

따라서 핀테크 회사가 어떤 방식으로 생체정보를 처리하느냐에 따라 생체정보 처리에 따른 역할과 책임이 달라질 수 있다. 이용자 손해에 대하여 서버검증형의 경우 핀테크 회사가 책임을, 단말검증형의 경우 핀테크 회사와 전자금융보조업자가 공동책임을 질 수 있다.

제4절

API 및 스크래핑 사례

API(Application Programming Interface)란 "특정 프로그램의 기능이나 데이터를 다른 프로그램이 접근할 수 있도록 미리 정한 규칙" 또는 "네트워크상으로 서로 다른 프로그램 간 기능 · 데이터를 연결하는 매개체의 역할"을 의미한다. API에 접속할 수 있는 권한을 가진 자의 범위에 따라 '폐쇄형(Closed API)'과 '공개형(Open API)'으로 구분될 수 있다. 폐쇄형은 해당 회사 · 기관 내부에서만 API를 통한 프로그램 접근이 가능하고, 공개형은 · 회사 · 기관 외의 제3자에게도 API를 통한 프로그램 접근이 허용된 것으로 제3자의 범위에 따라 Partner(상호협의에 따른 파트너만 접근 가능), Member(자격요건 등을 정하고 있는 커뮤니티에 속하는 멤버만 접근 가능), Acquaintance(일정한 요건을 갖출 경우 누구나 접근 가능)로 구분하기도 한다.[92)]

대표적으로 금융결제원이 제공하는 금융결제망을 통해 제공하는 금융회사들의 '오픈뱅킹 서비스' 사례가 있다. '오픈뱅킹 서비스'란 고객이 여러 금융회사 앱(App)을 설치할 필요 없이 하나의 은행, 상호금융, 증권사, 핀테크 앱(오픈뱅킹 참여기관 앱)만으로 모든 본인계좌를 조회하고 자금을 이체할 수 있는 서비스를 의미한다. 보안에 취약한 스크래핑 대신 본인 직접인증 및 안전한 전송방식을 활용할 수 있도록 하는 기술이다.[93), 94)]

스크래핑 기술은 API 미제공 등으로 데이터를 별도로 수집 가능한 채널이 없는 경우 API의 대체 수단으로 활용 가능한 기술이다. 핀테크 회사는 ① 고객을 대신하여 고객의 인증정보로 인증을 수행한 후, ② 스크래핑으로 화면에 표시된 개인(신용)정보를 수집하는 방식을 많이 이용한다. 이때 사용되는 인증정보는 비밀번호, 인증서 등이다.

92) 금융위원회, [알기 쉬운 핀테크] 금융권 Open API [참고5] (본문 12면)(2019.2.21.)
93) 금융위원회 보도자료, 저축은행 이용자들도 보다 편리하게 조회 · 이체 서비스를 이용할 수 있습니다(2021.4.28.)
94) 금융위원회 보도자료, 본인신용정보관리업(마이데이터) 운영 가이드라인 발간 및 마이데이터 지원센터 개소(2021.2.23.)

일부 핀테크 회사는 고객의 인증정보(ID/PW, 인증서 등)를 보관 및 사용하여 스크래핑함에 따라 고객 인증정보 보호에 취약할 수 있고, API를 이용하거나 금융회사와의 계약 등을 통한 수집이 아닌 고객 인증정보를 이용한 수집이므로 데이터 확보의 안정성이 낮으며, 고객은 핀테크 회사가 실제 수집 및 저장하는 데이터의 범위를 확인하거나 통제할 수 없어 개인정보에 대한 자기결정권 실현에 한계가 있다.

「신용정보법」에 따른 개인신용정보 이동권[95] 행사로 정보제공 의무가 부여되는 금융회사, 통신사 등에 「데이터 표준 API」 구축이 의무화됨에 따라 마이데이터 사업자는 ①데이터 표준 API」을 통해 통합조회 등의 서비스 제공을 위한 정보를 충분히 제공받게 된다.

표준 API를 사용하도록 하는 것은 보다 안전한 데이터 수집 · 제공을 위한 정보보호 · 보안 관련 조치이며, 스크래핑 기술 자체를 금지하는 것이 아니다. ① 웹사이트에서 링크하고 있는 다른 웹사이트의 정보를 수집하는 등(이른바 Crawling) 고객 인증정보를 사용하지 않는 데이터 수집은 가능하고, ② 증권사 호가 정보, 금융상품 설명정보 등 개인신용정보가 아닌 데이터를 수집하는 경우와 업무자동화 등을 위해 기업 · 기관의 자체 전산시스템에서 내부통제 절차에 따라 데이터를 처리할 때(이른바 B2B) 스크레이핑 기술 사용할 수 있다. 또한 기업 인증정보를 사용 · 보관하여 기업의 정보를 수집하는 것도 가능하다.

1 스크래핑 사용가능 여부

2022년 1월 1일부터 본인신용정보관리회사(일명, 마이데이터사업자)는 「전자금융거래법」 제2조 제10호에 따른 접근매체를 사용 · 보관함으로써 신용정보주체에게 교부할 신용정보를 수집할 수 없다. 다시 말하면 인증서, ID/PW 등을 통하여 고객의 신용정보를 스크래핑

95) 정보주체가 본인 정보를 보유한 기관(금융회사 등)에게 본인정보(사본)를 본인 또는 본인이 지정한 제3자에게 이동시키도록 할 수 있는 권리

방식으로 수집할 수 없다는 것을 의미한다. 참고로, 최근 금융위원회 보도참고자료에 따르면 API 의무화시기는 2021년 12월 31일까지 유예되었다.[96]

다만, 「신용정보법」에서는 주어가 '본인신용정보관리회사'로만 규정되어 있어 '본인신용정보관리회사'만 스크래핑 사용이 금지되고 본인신용정보관리회사를 제외한 다른 회사들은 사용할 수 있는 것인지 법률 상 명확하지 않다고 생각할 수 있다. 그러나, 허가를 받은 본인신용정보관리회사만이 마이데이터 관련 업무를 수행할 수 있다는 점을 명심할 필요가 있다.

[관계법령] 신용정보법 제22조의9 제3항 및 부칙 제1조 제2호

제22조의9(본인신용정보관리회사의 행위규칙)

③ 본인신용정보관리회사는 다음 각 호의 수단을 대통령령으로 정하는 방식으로 사용 · 보관함으로써 신용정보주체에게 교부할 신용정보를 수집하여서는 아니 된다.

1. 대통령령으로 정하는 신용정보제공 · 이용자나 「개인정보 보호법」에 따른 공공기관으로서 대통령령으로 정하는 공공기관 또는 본인신용정보관리회사(이하 이 조 및 제33조의2에서 "신용정보제공 · 이용자등"이라 한다)가 선정하여 사용 · 관리하는 신용정보주체 본인에 관한 수단으로서 「전자금융거래법」 제2조제10호에 따른 접근매체
2. 본인임을 확인 받는 수단으로서 본인의 신분을 나타내는 증표 제시 또는 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법

부칙 〈법률 제16957호, 2020. 2. 4.〉

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 다음 각 호의 구분에 따른 개정규정은 각각 해당 호에서 정하는 날부터 시행한다.

2. 제22조의9제3항부터 제7항까지 및 제52조제2항제4호의2 · 제4호의3의 개정규정: 이 법 공포 후 1년 6개월을 넘지 아니하는 범위에서 대통령령으로 정하는 날

96) 금융위원회.금융감독원.신용정보원.금융보안원 보도참고자료, 본인신용정보관리업(마이데이터) 운영 가이드라인 개정 (2021.7.29.)

[관계법령] 신용정보법 시행령 제18조의6

제18조의6(본인신용정보관리회사의 행위규칙 등)

③ 법 제22조의9제3항 각 호 외의 부분에서 "대통령령으로 정하는 방식"이란 같은 항 각 호의 수단(이하 "접근수단"이라 한다)을 다음 각 호의 어느 하나에 해당하는 방법을 통해 위임 · 대리 · 대행, 그 밖에 이와 유사한 방식으로 신용정보주체의 이름으로 열람하는 것을 말한다.

1. 접근수단을 직접 보관하는 방법
2. 개인인 신용정보주체의 접근수단에 접근할 수 있는 권한을 확보하는 방법
3. 접근수단에 대한 지배권, 이용권 또는 접근권 등을 사실상 확보하는 방법
4. 그 밖에 제1호부터 제3호까지의 규정에 따른 방법과 유사한 방법으로서 금융위원회가 정하여 고시하는 방법

⑥ 법 제22조의9제3항제2호에서 "대통령령으로 정하는 방법"이란 신용정보주체가 신용정보회사등에 본인의 신분을 나타내는 증표를 내보이거나, 전화 또는 인터넷 홈페이지 등을 이용하여 본인임을 확인받은 경우를 말한다.

[시행일 : 2021. 8. 4.] 제18조의6제3항, 제18조의6제6항

2 이용약관 위반의 주체

신용정보원의 '본인신용정보열람서비스' 이용약관에서는 (i) 다른 사람의 개인정보, 인증서의 정보를 부정 사용하거나 자신의 개인정보, 인증서 등을 제3자에게 이용하게 하는 행위, (ii) 신용정보원의 사전승낙 없이 기술적 수단(스크래핑,[97] 캡처, 크롤러, 미러링 등 데이터 추출 프로그램 및 기타 자동화 수단)을 사용하여 신용정보원이 제공하는 서비스의 콘텐츠를 가져가거나 제3자가 가져가도록 허용하는 행위, (iii) 신용정보원의 인프라에 부당하게 또는 통상적인 수준 이상의 부담을 주거나 줄 수 있는 조치를 하는 행위, (iv) 신용정보원 서비스 사이트의 접속을 금지하거나 제한하기 위해 신용정보원이 취할 수 있는 조치를 회피하거나 회피를 시도하는 행위, (v) 회원 이외 제3자의 제1호 내지 제12호의

97) 이용약관에서는 '스크레이핑'으로 표기되어 있으나 본 교재에서는 용어통일을 위하여 '스크래핑'으로 수정함

행위에 대한 협력 행위 등에 대하여 회원의 의무를 부여하고 있다.

이는 '본인신용정보열람서비스' 이용자인 고객이 스크래핑 서비스를 제공하는 제3자와 협력하여 신용정보원이 제공하는 서비스의 콘텐츠를 가져가도록 하는 행위, 제3자가 이용하게 하는 행위 등은 이용약관 위반이 될 가능성이 있고, 이용약관 위반에 따른 서비스 이용제한은 제3자가 아닌 고객이 받게 될 수 있다. 이러한 점에서 이용약관 위반에 따른 피해를 받는 주체가 누구인지를 명확히 이해할 필요가 있다.

[참고자료] 신용정보원의 '본인신용정보열람서비스' 이용약관 제2조 및 제10조

제 2 조 (정의)

① 이 약관에서 사용하는 용어의 정의는 다음 각 호와 같습니다.

2. "회원"이란 신용정보원의 서비스에 접속하여 이 약관에 따라 신용정보원의 가입절차를 통해 아이디를 부여받은 자를 의미합니다.

제 10 조 (회원의 의무)

회원은 서비스 이용과 관련하여 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 안 됩니다.

1. 다른 사람의 개인정보, 인증서의 정보를 부정 사용하거나 자신의 개인정보, 인증서 등을 제3자에게 이용하게 하는 행위
7. 신용정보원의 사전승낙 없이 기술적 수단(스크레이핑, 캡처, 크롤러, 미러링 등 데이터 추출 프로그램 및 기타 자동화 수단)을 사용하여 신용정보원이 제공하는 서비스의 콘텐츠를 가져가거나 제3자가 가져가도록 허용하는 행위
10. 신용정보원의 인프라에 부당하게 또는 통상적인 수준 이상의 부담을 주거나 줄 수 있는 조치를 하는 행위
12. 신용정보원 서비스 사이트의 접속을 금지하거나 제한하기 위해 신용정보원이 취할 수 있는 조치를 회피하거나 회피를 시도하는 행위
13. 회원 이외 제3자의 제1호 내지 제12호의 행위에 대한 협력 행위

제5절

마이데이터 사례

1 본인인증의 목적

'마이데이터 서비스 가이드라인'과 '마이데이터 기술 가이드라인'에서 본인인증의 정의는 유사하지만 목적은 다소 다르다. 구체적으로 '마이데이터 서비스 가이드라인'에서는 본인인증의 목적으로 '정보제공자가 고객이 (i) 해당 정보의 정보주체이며, (ii) 전송요구를 하였는지 확인'하는 것으로 설명하고, '마이데이터 기술 가이드라인'에서는 '고객이 해당 개인신용정보의 소유자임을 정보제공자가 확인'하는 것으로 설명하고 있다.

그러나 핀테크 회사가 마이데이터 서비스 제공자 또는 정보제공자인 경우 위 두 가지 가이드라인을 준수할 필요가 있고, 핀테크 회사가 정보제공자인 경우는 고객이 (i) 해당 정보의 정보주체이고, (ii) 전송요구를 하였는지를 모두 확인하여야 할 의무가 있다는 점을 명심할 필요가 있다.

[참고자료] 마이데이터 서비스 가이드라인(본문 4면)

(본인인증) 고객이 정보제공자에게 정보의 전송을 요구할 때, **정보제공자가 고객이 해당 정보의 정보주체이며 전송요구를 하였는지 확인**하는 방법

[참고자료] 마이데이터 기술 가이드라인(본문 5면)

(본인인증) 고객이 정보제공자에게 개인신용정보 전송을 요구할 때, **고객이 해당 개인신용정보의 소유자임을 정보제공자가 확인**하기 위한 방법

2 인증수단[98)]

정보제공자인 금융회사등은 다중인증, 다중요소 공개키인증서, 비대면 실명확인 방식 등과 같이 신뢰성 및 안전성이 확보된 인증수단을 사용하여 고객에 대한 본인인증을 수행하여야 한다. 핀테크 회사가 정보제공자인 경우 본인인증에서 허용하는 방식과 절차를 이해하고 가이드라인에서 요구하는 기술 또는 절차를 본인의 서비스에 적용할 필요가 있다.

여기서 '다중인증'이란 지식 · 소유 · 특징 기반 인증수단 중 소유기반 인증수단을 포함하여 2가지 이상의 인증수단을 동시에 적용하되, 각 인증정보는 서로 분리된 환경에서 생성 및 전송되는 방식을 의미하고, '다중요소 공개키인증서'란 안전하게 생성 · 보호된 개인키 및 공개키 인증서로서 인증요구를 위한 전자서명을 생성하기 위해 개인키 인증정보(비밀번호, 생체정보 등)를 요구하는 방식을 의미한다. 마지막 '비대면 실명확인 방식 활용'이란 「금융실명법」상 비대면 실명확인 방식 7가지 중 2가지 이상을 중첩확인하는 방식을 말한다. 이때 사용되는 비대면 실명확인 방식은 금융거래가 아니므로 방식만 동일할 뿐 「금융실명법」의 실명확인에 따라 금융회사등이 의무적으로 수행하여야 하는 방식과는 구분될 필요가 있다.

그리고 마이데이터 정보전송 요구시 정보제공자인 금융회사등의 '개별인증'을 반복해야 하는 방식을 개선하고자 '통합인증'을 도입하였다.[99)] '마이데이터 서비스 가이드라인'과 '마이데이터 기술 가이드라인'에서 모두 '개별인증(또는 개별 본인인증)'과 '통합인증(또는 통합 본인인증)'에 대하여 설명하고 있으나, '마이데이터 기술 가이드라인'의 '제4장.

98) 마이데이터 기술 가이드라인
99) 금융위원회 보도자료, 「제6차 디지털금융 협의회」 개최(2021.2.9.)

본인인증'에서 보다 상세 내용을 다루고 있다. '개별인증'과 '통합인증' 간 인증 수행주체, 인증수단 제공자, 인증수단, 인증회수(고객관점)에서의 차이는 〈표 Ⅰ-1〉과 같다.

〈표 Ⅰ-1〉 보안인증 유형 비교

비교기준	개별 본인 인증	통합 본인 인증
인증 수행주체	정보제공자	정보 제공자
인증 수행제공자	정보제공자, 제3의 인증기관 등	통합 인증기관
인증수단	다중 인증 등*(정보제공자별 상이) *'나. 인증수단' 참고	다중요소 공개키 인증서(PKI) *CI 제공 필요
인증 횟수 (고객 관점)	전송요구 대상 정보제공자의 수만큼 반복적 인증 수행	전송요구 대상 정보제공자의 수와 무관하게 1회 수행

출처: 마이데이터 기술 가이드라인, 본문 56면

[참고자료] 마이데이터 서비스 가이드라인(본문 4면)

(개별인증) 각각의 정보제공자가 일반적으로 제공되는 인증수단을 이용하여 개별적으로 고객이 본인임을 인증하는 방식의 본인인증(마이데이터사업자를 통하여 고객이 정보를 전송 요구할 때마다 정보제공자의 수만큼 인증이 이루어짐)

(통합인증) 다수의 정보제공자가 공통의 인증수단을 이용하여 고객을 동시에 인증하는 방식의 본인인증

[참고자료] 마이데이터 기술 가이드라인(본문 5면)

(개별인증) 정보제공자가 자율적으로 제공하는 인증수단을 이용한 본인인증 방법으로 고객이 개인신용정보 전송을 요구하는 정보제공자의 수만큼 인증이 이루어지는 방식

(통합인증) 고객이 공용의 인증수단을 이용하여 인증행위를 1회 수행함으로써 다수의 정보제공자에 인증이 가능한 방식

핵심정리

1. 기본 원칙

핀테크 회사가 전자금융업자 또는 전자금융보조업자로서의 역할을 수행할 경우 전자금융과 관련된 법규를 준수하고 전자금융거래의 안전성 및 신뢰성을 확보할 수 있어야 한다. 자율에 따라 보안인증 관련 기술과 절차를 도입할 수 있으나, 구축 및 도입하려는 보안인증에 대한보안성은 충분히 검토해야 한다.

2. 전자문서 및 전자서명 사례

- 전자문서의 효력
  - 「민법」에 따르면 보증은 그 의사가 보증인의 기명날인 또는 서명이 있는 서면으로 표시되어야 효력이 발생하며, 보증의 의사가 전자적 형태로 표시된 경우에는 효력이 없다(민법 제428조의2 제1항). 그러나 「전자서명법」에서는 전자서명이 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 않으며(전자서명법 제3조 제1항), 「전자문서법」에서는 전자문서가 전자적 형태로 되어 있다는 이유만으로 법적 효력이 부인되지 아니하고(전자문서법 제4조 제1항), 보증인이 자기의 영업 또는 사업으로 작성한 보증의 의사가 표시된 전자문서는 「민법」 제428조의2 제1항 단서에도 불구하고 같은 항 본문에 따른 서면으로 본다고 규정되어 있다. 따라서 보증인이 자기의 영업 또는 사업으로 작성한 보증의 의사가 표시된 전자문서 및 전자서명의 경우 효력이 없다고 해석될 가능성이 없다고 볼 수 있다.

- 전자서명 방식의 개선
  - 2021년 5월 17일 금융위원회는 모바일 청약 시 반복서명 절차를 폐지한다는 내용의 보험 대면모집 관련 개선방안을 발표하였다. 구체적으로 이 개선방안에는 기존 설계사가 계약자를 만나서 중요사항을 설명하면, 보험계약 서류작성 등 청약절차는 모바일로 진행할 수 있으나 이 과정에서 소비자는 작은 휴대폰 화면 등에서 모든 서류에 반복해서 전자서명을 해야 해서 불편을 겪었다. 이를 개선하고자 전자서명

입력은 청약절차 시작 시 1회만 하고, 소비자가 계약 중요사항 및 각각의 서류내용을 꼼꼼하게 확인하여 서명란을 클릭 확인하도록 개선하였다.

3. 생체정보 사례

- 「전자금융거래법」상 전자금융보조업자의 역할과 책임
  - 핀테크 회사가 금융회사 또는 전자금융업자를 위하여 「전자금융거래법」의 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 경우「전자금융거래법」상 전자금융보조업자의 역할을 수행한다 할 수 있다. 핀테크 회사가 전자금융업자일 경우 전자금융보조업자의 고의나 과실로 인한 손해 발생 시에는 그 손해배상에 대한 구상권을 전자금융보조업자에게 청구할 수 있으나, 핀테크 회사가 전자금융보조업자일 경우 금융회사 또는 전자금융업자로부터 구상권을 청구 받을 수 있다.

- 생체정보 처리에 따른 역할과 책임
  - 생체정보 처리 방식으로는 서버검증형과 단말검증형으로 구분된다.
  - 서버검증형은 스마트폰을 통해 생성한 지문 특징정보를 핀테크 회사의 서버에 저장·등록하고 인증 시 스마트폰에서 전달된 특징정보와 회사 서버에 저장된 특징정보와 비교하는 방식을 말한다.
  - 단말검증형은 지문정보는 스마트폰에 저장되고, 해당 지문에 대한 토큰값을 발생시켜 스마트폰과 핀테크 회사의 서버에 각각 저장·등록한다. 이후 인증 시 스마트폰에서 사용자 인증이 완료되면, 토큰값이 서버로 전달되고 그 토큰정보와 서버에 저장된 토큰정보가 일치하는지 검증한다.

4. API 및 스크래핑 사례

- 스크래핑 사용가능 여부
  - 2022년 1월 1일부터 본인신용정보관리회사(일명, 마이데이터사업자)는 「전자금융거래법」 제2조 제10호에 따른 접근매체를 사용·보관함으로써

신용정보주체에게 교부할 신용정보를 수집할 수 없다. 다시 말하면 인증서, ID/PW 등을 통하여 고객의 신용정보를 스크래핑 방식으로 수집할 수 없다는 것을 의미한다.

- 다만, 「신용정보법」에서는 주어가 '본인신용정보관리회사'로만 규정되어 있어 '본인신용정보관리회사'만 스크래핑 사용이 금지되고 본인신용정보관리회사를 제외한 다른 회사들은 사용할 수 있는 것인지 법률상 명확하지 않다고 생각할 수 있다. 그러나, 허가를 받은 본인신용정보관리회사만이 마이데이터 관련 업무를 수행할 수 있다는 점을 명심할 필요가 있다.

• 이용약관 위반의 주체

- 신용정보원의 '본인신용정보열람서비스' 이용자인 고객이 스크래핑 서비스를 제공하는 제3자와 협력하여 신용정보원이 제공하는 서비스의 콘텐츠를 가져가도록 하는 행위, 제3자가 이용하게 하는 행위 등은 이용약관 위반이 될 가능성이 있고, 이용약관 위반에 따른 서비스 이용제한은 제3자가 아닌 고객이 받게 될 수 있다. 이러한 점에서 이용약관 위반에 따른 피해를 받는 주체가 누구인지를 명확히 이해할 필요가 있다.

5. 마이데이터 사례

• 본인인증의 목적

- '마이데이터 서비스 가이드라인'과 '마이데이터 기술 가이드라인'에서 본인인증의 정의는 유사하지만 목적은 다소 다르다. 구체적으로 '마이데이터 서비스 가이드라인'에서는 본인인증의 목적으로 '정보제공자가 고객이 (ⅰ) 해당 정보의 정보주체이며, (ⅱ) 전송요구를 하였는지 확인'하는 것으로 설명하고, '마이데이터 기술 가이드라인'에서는 '고객이 해당 개인신용정보의 소유자임을 정보제공자가 확인'하는 것으로 설명하고 있다.
- 그러나 핀테크 회사가 마이데이터 서비스 제공자 또는 정보제공자인 경우 위 두 가지 가이드라인을 준수할 필요가 있고, 핀테크 회사가 정보제공자인 경우는 고객이 (ⅰ) 해당 정보의 정보주체이고, (ⅱ) 전송요구를 하였는지를 모두 확인하여야 할 의무가 있다는 점을 명시할 필요가 있다.

• 인증수단

– 정보제공자인 금융회사등은 다중인증, 다중요소 공개키인증서, 비대면 실명확인 방식 등과 같이 신뢰성 및 안전성이 확보된 인증수단을 사용하여 고객에 대한 본인인증을 수행하여야 한다. 핀테크 회사가 정보제공자인 경우 본인인증에서 허용하는 방식과 절차를 이해하고 가이드라인에서 요구하는 기술 또는 절차를 본인의 서비스에 적용할 필요가 있다.

헬로, 핀테크!(보안인증 · 블록체인)

6장

블록체인 개요

6장 블록체인 개요

학습목표

1. 블록체인이 등장한 역사적 배경을 설명할 수 있다.
2. 블록체인을 만든 목적을 이해하고 설명할 수 있다.
3. 블록체인을 이루고 있는 기반기술을 설명할 수 있다.

학습개요

비트코인은 이전 25년에 걸친 프라이버시 보호운동이 결집되어 2008년 개발되었으며, 2009년 1월 3일 실제로 구현된다. 그러나 금융기관과의 제휴에 기반한 그 이전의 방법과 달리 비트코인은 금융기관을 배제하는 방법을 통해 프라이버시 보호를 꾀했다.

이 장에서는 비트코인의 등장배경과 함께 블록체인의 구조와 그 특징 그리고 블록체인이 사용하고 있는 해시함수와 비대칭 암호화 기법 등의 기반기술을 살펴보도록 한다.

아울러 블록체인의 원형인 비트코인의 작동원리와 기반기술에 대해 자세히 알아봄으로써 그로부터 파생된 여러 변형을 쉽게 이해할 수 있도록 학습한다.

용어해설

❶ 슈도니머스

가명을 의미하며, 필요시 실명을 특정할 수 있는 경우를 의미한다.

❷ 어노니머스

익명을 의미하여, 어떤 경우에도 실명을 특정할 수 없다는 것을 의미한다.

❸ 작업증명

네트워크 오남용을 막기 위해, 특정 과제 수행을 위해서 의도적으로 일정 이상의 에너지를 소모하게 만드는 일을 말한다.

❹ 채굴

블록체인에서 기록을 위해 작업증명을 수행하는 일. 채굴이 완성되어야 블록에 기록할 수 있는 자격이 주어진다.

❺ 블록체인

블록체인의 정의는 제7장 제2절 참고. 제7장 제1절까지는, 블록체인은 비트코인과 동의어로 생각하면 된다. 제7장 제2절부터는 문맥에 따라 혼용하여 사용되지만 정의에 따라 구분이 가능하다.

❻ ICO(Initial Coin Offering)

IPO(Initial Public Offering)에 빗대어 만든 신조어로서 증권 대신 새로운 코인을 발행하고 판매 대금으로 기존 코인을 수령하는 방식을 말한다.

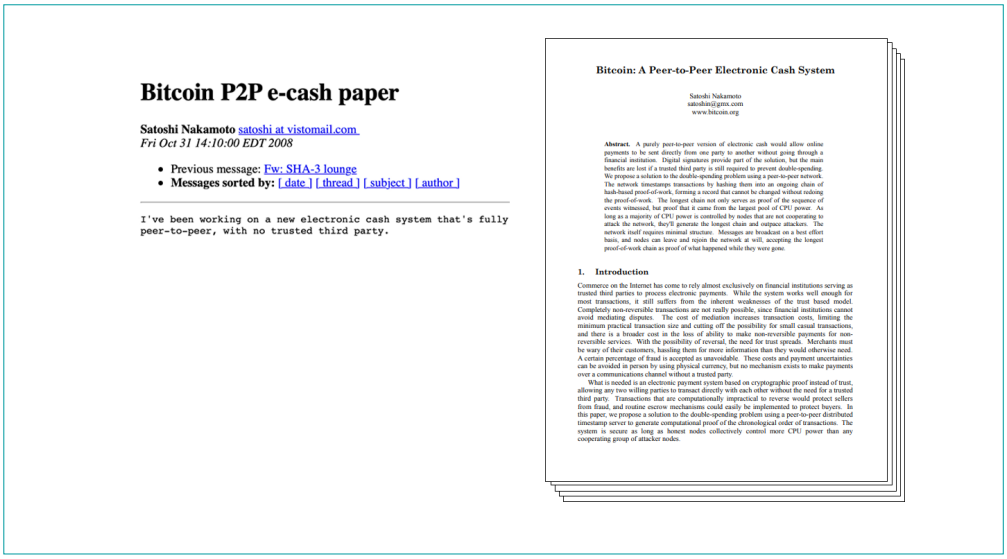
제1절

블록체인의 등장 배경

블록체인은 2008년 사토시 나카모토(Satoshi Nakamoto)라는 가명을 사용한 어느 집단이 프라이버시 보호가 되는 거래 시스템에 관한 자신들의 구상이 담긴 9쪽짜리 논문인 『Bitcoin: A Peer-to-Peer Electronic Cash System』[100]을 암호학 커뮤니티의 메일링 리스트에 첨부하여 발송하면서 세상에 알려졌다.

블록체인에 대한 평가는 극명하게 나뉘는데, 블록체인을 4차 산업혁명의 기반기술이라고 치켜세우는 사람이 있는가 하면 노벨 경제학상을 수상한 뉴욕대학의 누리엘 루니비(Nouriel Roubini) 교수는 블록체인은 무용지물이며, 모든 ICO는 사기라고 주장한다.[101]

〈그림 VI-1〉 비트코인을 소개한 메일과 그 첨부파일 [100]



Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

100) Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf
101) 형사정책연구원, 제4차 산업혁명시대의 형사사법적 대응 및 발전방안(II) – IoT와 블록체인, 2019, p. 156

과연 블록체인은 무엇을 위한 '기술'일까? 특히 '4차 산업혁명의 기반기술'이라는 문장은 블록체인이라는 모호한 개념의 설명을 위해 4차 산업혁명이라는 모호한 개념을 동원한 것으로 그다지 유용한 정보를 주지 못한다. 블록체인을 온전히 이해하려면 먼저 데이비드 차움(David Chaum)의 'e-캐시'와 '사이퍼펑크(CypherPunk)라는 행동주의자들을 살펴볼 필요가 있다. 이 둘이 바로 블록체인의 효시인 비트코인 등장의 개념적 · 이론적 배경은 물론 대부분의 기술적 바탕을 제공했기 때문이다. 이제 각각을 살펴보도록 한다.

1 데이비드 차움과 e-캐시

1975년 미국 표준국(NIST)의 요청으로 IBM은 DES(Data Encryption Standard)라는 새로운 암호화 체계를 연구하였고 이 기술은 곧 민간에도 공개된다. 당시 암호화 기술은 군이나 정부가 독점한 상태였으므로 DES는 사실상 민간이 접하게 된 최초의 고급 암호화 기술이었던 셈이다. 평소 개인정보를 악용한 무분별한 스팸 메일의 난립과 정부기관에 의한 개인의 프라이버시 침해에 대해 환멸을 느끼던 많은 사람들에게 있어 이러한 고급 암호화 기술을 사용할 수 있게 되었다는 사실은 매우 큰 의미였고, 이러한 암호화 기법을 적극적으로 활용하여 개인의 프라이버시를 보호하고자 하는 움직임이 서서히 싹트기 시작하였다.

[정부에 대한 불신] DES에 관한 의혹

미국 정부 주도로 개발된 DES는 발표 당시부터 많은 의혹이 따랐다. 특히 DES가 IBM의 원안대로 공개되지 않고 마지막에 정부기관에 의해 일부 수정된 것이 알려지면서 의혹은 더 커졌고 백도어(Back Door)가 설치돼 있어 특수한 방법으로 정부기관이 쉽게 복호화할 수 있다는 소문도 파다했다. 또 전체 64비트 길이의 키(Key) 중 56비트만 암호화에 사용하므로 안전성이 약한 것도 문제점 중 하나였다. 이 알고리즘은 이후 보다 강력한 AES(Advanced Encryption Standard)로 대체된다.

출처: 블록체인 해설서, 이병욱, 에이콘 출판사, 2019, p. 42

[정부의 프라이버시 침해] 합법적 감청

미국 정부에 의한 프라이버시 침해 사례는 상당히 많은데 클리퍼(Clipper) 칩도 그 대표적 사례이다. 1993년 클린턴 행정부는 미국 국가안전 보장국(NSA)이 개발한 백도어인 LEAF(Law Enforcement Access Filed) 코드가 심어진 칩인 클리퍼를 모든 통신장비에 설치하도록 각 통신사에 권고하였다. 이 칩이 설치되면 정부가 모든 국민의 통화 내용을 감청할 수 있게 된다. 명분은 테러방지 등을 통한 국가안보 제고였다. 이 계획은 칩 자체의 결함과 수정헌법에 반하는 위헌성 때문에 격렬한 논란 끝에 1996년 완전히 폐기된다.

출처: 블록체인 해설서, 이병욱, 에이콘 출판사, 2019, p. 44

1-1 추적이 불가능한 거래 시스템

1983년 데이비드 차움(David Chaum)은 'e-캐시'라는 이름의 새로운 캐시시스템을 구상하게 된다. e-캐시는 금융기관과의 제휴를 통해 모든 거래 내용을 암호화함으로써 제3자가 그 내역을 추적할 수 없도록 프라이버시를 보호하는 것이 목적이었다.[102] 데이비드 차움이 1985년에 발표한 논문 제목이 『신분노출이 없는 보안: 빅브라더를 무용지물로 만들 수 있는 거래시스템』이라는 점에서 그가 추구한 '통제 권력으로부터의 자유'라는 목적을 짐작할 수 있다.[103]

데이비드 차움은 그의 구상을 실현하기 위해 1990년 디지캐시(DigiCash)라는 회사를 직접 설립하여 서비스를 시작했지만 실제 그와 제휴한 은행은 단 한 군데뿐이었고 그는 1999년 회사를 떠나게 된다.

1-2 익명의 거래 시스템이 갖춰야 할 조건

데이비드 차움은 프라이버시 보호를 최우선으로 고려했지만 익명의 금융 거래가 가진

102) David Chaum, "Blind Signature for untraceable payments", Advances in cryptology Proceedings. 82(3): pp. 199-203

103) David Chaum, "Security without identification: Transaction system to make big brothers obsolete", Communications of ACM, pp. 1030-1044

위험성을 잘 이해하고 있었으므로, 프라이버시 보호를 목적으로 한 익명의 결제 수단이 갖춰야 할 3가지 기본 성질을 다음과 같이 정의했다.[104)]

첫째, 각 개인이 행한 결제에 대해 그 수취인, 결제 시간, 금액은 제3자가 알 수 없어야 한다.
둘째, 예외적 상황 하에서는 각 결제에 대한 증명 또는 수취인의 신원에 대한 자료를 제공할 수 있어야 한다.
셋째, 도난당한 것으로 보고된 결제 수단은 사용을 중지할 수 있어야 한다.

그러나 2009년 구현된 비트코인은 e-캐시를 그 기술적 효시로 승계하고 있지만, 오직 첫 번째만 만족한다. e-캐시가 프라이버시를 보호하려던 방식은 금융기관과 제휴하여 암호화라는 도구를 사용하는 것이었지만, 비트코인은 프라이버시 보호를 위해 금융기관 자체를 배제하려 한 점에서 이 둘은 크게 차이가 난다. 즉, 둘 다 익명성을 가지지만, 유사시에 금융기관을 통해 신원 특정이 가능한 슈도니머스(Pseudonymous)와 달리 비트코인은 그 어떤 경우도 신원을 특정할 수 없도록 금융기관 자체를 배제한 어노니머스(Anonymous)로 설계된 것이다. 이 두 개념의 차이는 제2절에서 좀 더 자세히 알아보기로 한다.

2 사이퍼펑크

암호화를 사용해 프라이버시를 보호하려던 개별 움직임은 1980년대 말이 되면서 조금씩 세력화되기 시작한다. 이들 중 주드 미혼(Jude Mihon)은 스스로를 지칭하기 위한 신조어를 만드는데, 암호화를 의미하는 Cipher와 인터넷 악동을 뜻하는 부르스 배스케(Bruce Bethke)의 소설 제목 사이버펑크(Cyberpunk)를 조합한 신조어 사이퍼펑크(Cypherpunk)가 바로 그것이다. 장난스레 만든 이 단어는 2006년 옥스퍼드 사전에 정식으로 등재되었는데 다음과 같이 정의돼 있다.

104) 각주 103)과 동일하다.

> 컴퓨터 네트워크를 사용할 때 특히 정부기관으로부터 프라이버시를 보호하기 위해
>
> 암호화 기술을 사용하는 사람
>
> – Oxford Dictionary –

즉, 사이퍼펑크란 암호화 기술을 사용해 프라이버시를 보호하려던 행동주의자를 일컫던 말이다. 1980년대 초 데이비드 차움을 그 기술적 효시로 하여 수많은 사이퍼펑크들이 활동하였는데 비트코인이 등장하는 2008년까지의 약 25년 사이 (i) 웨이 다이(Wei Dai)는 1998년 익명의 분산 전자 캐시 시스템인 B-머니를 제안하였는데 이는 암호화 퍼즐에 기반하여 새로운 화폐를 생성한다는 아이디어였다. (ii) 닉 사보(Nick Szabo)는 비트코인의 채굴 모델의 기본 개념이 된 비트골드(Bitgold)를 제안하였으며 (iii) 아담 백(Adam Back)은 작업증명에 기반한 해시캐시(Hash Cash)를 구상하였다. (iv) 할 피니(Hal Finney)는 재사용이 가능한 작업증명이라는 개념의 R-POW를 2004년에 제안하는 등 비트코인의 원형이 된 다양한 거래 시스템이 제안되었다.

결국 비트코인의 핵심 작동 기저인 해시, 작업증명, 연쇄 해시와 머클트리[105] 등의 모든 기술적 개념은 이미 훨씬 전에 체계적으로 정립이 된 셈이다. 특히 연쇄 해시(Hash Chain; 해시체인)는 블록체인의 '체인'이라 단어가 유래한 배경이기도 하다. 그러나 비트코인 이전의 이들 기술의 공통점은 모두 여전히 '슈도미너스'였다는 것이다. 한편 비트코인을 최초로 건네받은 인물로 알려진 할 피니를 비롯한 이들 사이퍼펑크 대부분은 비트코인은 물론 이더리움 등 여러 가상자산이 만들어지는 데 직간접적으로 관여하게 된다. 데이비드 차움 역시 현재 엘릭서(Elixxir)라는 이름의 새로운 가상자산을 개발 중인데 양자 컴퓨터가 현실화되더라도 견딜 수 있는 암호화 체계를 탑재하는 것이 목표라고 주장하고 있다.

105) 이 개념들은 모두 제4절에서 자세히 설명한다.

[디지털 기록의 가치] 닉 사보의 비트골드

닉 사보는 1998년 비트골드(Bitgold)라는 개념을 구상한다. 그는 금이 가치를 가지는 이유는 채굴이 힘들기 때문이라고 생각했고, 동일한 이유로 어떤 디지털 정보가 생성하기 무지 힘들면 디지털 정보 자체가 어떤 가치를 가질 수 있을 것으로 생각했다. 예컨대 아주 어려운 수학문제가 있다면, 그 수학문제의 정답을 디지털화해서 서로 주고받는다면 그 정답 자체가 금과 같이 어떤 가치를 가질 수도 있을 것으로 생각한 것이다. 그는 이런 개념을 비트골드라고 표현했는데, 이는 비트코인이 해시퍼즐의 정답을 알아내기 위해 엄청난 에너지를 소비하며 계산을 되풀이하는 과정과 개념상으로 일치한다. 이 때문에 많은 사람들은 비트골드를 비트코인의 전신이라 주장하기도 한다. 물론 단순히 에너지를 소비했다고 해서 가치가 생긴다는 주장은 당연히 그 근거가 약하지만 이 논리는 현재 비트코인이 가치를 가지게 된 당위성을 옹호하기 위한 주요 근거로 이용되기도 한다.

그러나 실상은 많이 다르다. 대부분의 가상자산 개발자들은 소위 채굴과정이 없는 선채굴이라는 편법을 사용해 자신들의 가상자산을 손쉽게 미리 확보했다. 이더리움의 경우 7,200만 이더를 선채굴했으니, 이더리움 총량의 무려 70%는 선채굴로 시중에 뿌려진 비탈릭 부테린[106]의 불로소득인 셈이다!

출처: 블록체인 해설서, 이병욱, 에이콘 출판사, 2019, p. 46

106) 비탈릭 부테린(Vitalic Buterin)은 이더리움을 만든 코인 개발자이다.

제2절

블록체인의 목적

1 슈도니머스 vs. 어노니머스

비트코인이 만들어진 배경을 2008년 금융위기와 연결시켜 명목화폐의 문제점을 해결하기 위한 것이라 주장하는 사람도 있지만 이는 그다지 합리적인 설명이 아니다. 사토시 나카모토가 명목화폐에 환멸을 느꼈을 수도 있고, 실제로 비슷한 메모도 남겼지만 이는 당시 많은 이들의 보편적 정서일 뿐이다.

비트코인은 어느 순간 갑자기 만들어진 것이 아니라 무려 25여 년 가까이 기술과 개념이 집약되면서 등장했고 원 논문에는 명목화폐에 대한 언급조차 없다. 또한 제도와 규정이 핵심인 금융시스템을 소프트웨어 하나로 변혁한다는 것도 비논리적이다.

비트코인을 만든 명백한 목적은 '프라이버시 보호'이며 이를 위해 '금융기관을 배제'한 어노니머스 방식을 선택한 것이다. 단순히 프라이버시를 보호하는 슈도니머스와 달리 어노니머스는 금융의 건전성에 정면으로 반하는 속성으로서 자금세탁 등 각종 검은돈을 위한 도구로 사용될 수 있다. 비트코인이 가진 어노니머스 성질로 인해 비트코인은 그 소유자를 특정하기 어렵다. 학문적 용어는 아니지만 본서에서는 이 둘을 구분하기 위해서 지금부터 슈도니머스는 '가명'으로 어노니머스는 '절대 익명'으로 줄여 쓰도록 한다.

2 비트코인과 고객확인제도

1993년 8월 12일 저녁 김영삼 대통령은 민주화시대 이후 최초이자 유일했던 긴급명령을 통해 금융실명제를 전격 발표한다. 그 익일부터 모든 금융계좌는 신분증을 통한 실명확인 없이는 개설이 금지되었다. 금융실명제는 건전한 금융의 가장 기본이 되는 제도이지만 이웃 일본조차 아직 온전히 시행하고 있지 못할 정도로 전 세계적으로 기득권의 반발이 적지 않은 제도이다.

금융거래에 사용하는 계좌번호는 금융기관이 발행하고 이는 실명제를 통해 그 소유자를 특정할 수 있다. 그러나 비트코인에서 사용되는 비트코인 주소는 금융기관이 발급하는 것이 아니라 각 개인이 임의로 (무한대로) 만들어서 사용한다. 이 때문에 그 소유주를 특정하는 것은 사실상 불가능하며 이것이 비트코인이 절대 익명으로 거래되는 근본 원인이다.

현재 비트코인 거래 당사자를 확인할 수 있는 거의 유일한 통로는 소위 중개소를 통해서이다. 중개소를 통해 비트코인을 구매한 경우에는 연계 은행의 실명 확인된 가상계좌를 통해 그 소유자를 특정할 수 있다. 그러나 일단 비트코인 구매자가 임의의 비트코인 주소로 이전하면 더 이상의 추적이 불가능해 질 수 있다. 이 점은 제8장에서 다시 자세히 살펴보겠지만 이는 비트코인의 개발 목적이 '추적이 불가능한' 지급시스템이었으므로 당연한 귀결이라고 하겠다.

현재 금융권에서는 금융거래 또는 서비스가 자금세탁 등의 불법행위에 이용되지 않도록 고객확인 및 검증, 거래관계의 목적 확인 및 실소유자 확인 등을 실시하고 있으며 금융감독원과 금융정보분석원이 이를 관리하고 있다. 하지만 비트코인의 직거래는 고객확인의 첫 단계인 소유자 특정이 불가능해짐으로써 이 제도가 무력화된다.

〈표 Ⅵ-1〉 e-캐시와 비트코인 방식 비교

구 분	e-캐시	비트코인
개발자	데이비드 차움	사토시 나카모토(가명)
구현 방식	금융기관과 제휴 및 암호화	금융기관을 배제한 익명성
고객확인 제도 가능 유무	가능 (슈도니머스)	불가능 (어노니머스)
목적	프라이버시 보호	프라이버시 보호
개발 시기	1983	2008

제3절

블록체인의 구조 및 특징

지금까지 비트코인이 만들어지기 전 25여 년간에 걸친 프라이버시 보호 운동의 전개와 함께 비트코인을 만든 목적 그리고 절대 익명성에 대해 알아보았다. 이제 제3절과 제4절에 걸쳐 절대 익명이란 목적을 달성하기 위해 비트코인이 사용하고 있는 기술과 구조를 자세히 알아보도록 한다.

1 비트코인과 블록

1-1 블록의 크기

전산학에서 블록(Block)이란 통상 한꺼번에 처리하는 논리적 데이터 단위를 일컫는 용어이다. 대개 바이트(Byte, 8bit) 단위 또는 워드(Word, 32bit)를 그 최소단위로 하며 과제에 따라 그 크기는 달라진다. 이는 우리가 일상생활에서 승강기를 이용할 때 통상 한 명씩만 타지 않고 정원이 허용하는 범위 내까지 동시에 사용하는 것이 훨씬 더 효율적인 것에 비유할 수 있다. 이때 승강기 정원이 클수록 동시에 이용 가능한 사람은 많아질 것이고, 특정 시간의 이용객이 적다면 정원이 아무리 크더라도 승강기는 거의 빈 채로 운행될 수도 있을 것이다.

비트코인에서의 블록이란 정원이 1메가바이트이고, 대기 시간이 약 10분[107]인 승강기에 비유할 수 있다. 즉 블록이란 10분 동안 네트워크에 제출된 모든 거래 요청서들을 1메가바이트가 넘지 않는 범위 내에서 한꺼번에 모아 처리하고 그 결과를 저장하는 논리적 단위인 셈이다. 우리가 문서를 파일 단위로 저장하는 것처럼 비트코인은 블록 단위로 데이터를 저장한다고 이해하면 된다.

107) 이 시간은 정확히 10분이 아니라 평균적으로 10여 분이 되도록 시스템이 계속 조정해 나간다.

블록체인에서는 다양한 형태로 자신만의 블록을 정의할 수 있다. 예컨대 비트코인 캐시는 단순히 비트코인의 블록 용량을 8메가바이트로 크기만 조정한 아류 블록체인이며 이더리움은 개스(Gas)라 불리는 메타 단위에 의해 블록 크기가 동적으로 좌우되는데 대개 하나의 블록은 20~30k바이트를 유지하고 있다. 그러나 그 평균 대기시간이 불과 15초여서 비트코인 블록이 하나 생성되는 10여 분 동안 이더리움 블록은 무려 40개 정도 생성되므로 10여 분간 생성되는 데이터 크기는 800K~1,200K로서 비트코인과 유사하다[108)]

1-2 트랜잭션

트랜잭션(Transaction)은 금융에서는 폭넓게 금융 거래를 의미하고, 전산학에서는 보통 업무처리 단위를 말하는데 특히 데이터베이스에서는 더 이상 쪼갤 수 없는(혹은 더 쪼개면 심각한 오류가 발생할 수 있는) 최소한의 업무 처리 단위를 뜻한다.

비트코인에서의 트랜잭션은 비트코인을 주고받는 거래를 의미한다. 블록체인은 단순히 가상자산을 주고받는 것 이외에 다른 용도로 구현할 수 있으며 그에 따라 트랜잭션을 다양하게 정의할 수 있다. 따라서 블록체인의 트랜잭션이란 업무처리의 단위이며 비트코인의 경우는 비트코인을 주고받은 거래 내역을 기록하는 것이 업무처리 단위가 된다. 그러므로 트랜잭션은 그 응용 분야에 따라 다양한 의미를 가지는 포괄적인 용어이며 비트코인의 트랜잭션인 '거래 내역의 기록'은 지급결제 시스템과 관련된 특수한 경우의 예이다.

1-3 블록의 생성속도

비트코인에서 블록이 생성되는 속도는 이 절 마지막에서 설명할 채굴과 관계된다. 비트코인은 소위 채굴과정을 거쳐야 블록이 생성되는데, 그 평균 생성 시간이 10여 분이 되도록 채굴 난이도를 동적으로 조절하므로 약 10여분 간격으로 데이터가 처리되는 셈이다.

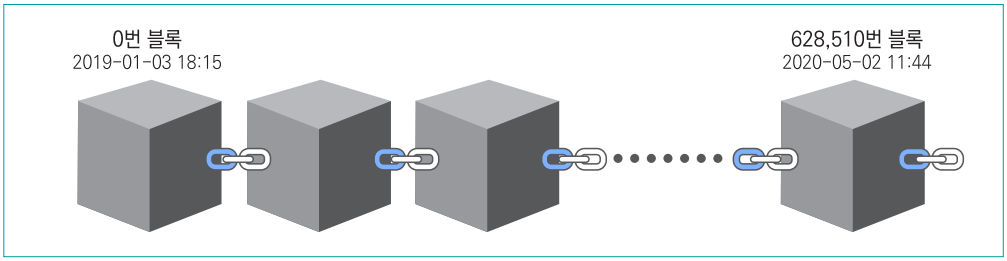
108) 엄밀히 말하면 이더리움은 데이터가 블록 외부에 저장되는 방식을 사용하고 있어서 약간 다르다.

2009년 1월 3일[109] 오후 6시 15분에 최초의 블록 즉, 0번 블록(이를 제네시스 블록라고 부른다)이 만들어 졌고 그로부터 6일 뒤인 2009년 1월 9일 오전 2시 45분 25초에 첫 번째 채굴을 통해[110] 1번 블록이 생성된 후 약 평균 10여 분에 하나씩 끊임없이 블록이 생성되어 저장되고 있다. 2020년 5월 2일 오전 11시 31분에는 628,509번 블록이 생성되었고 그로부터 13분 뒤인 오전 11시 44분에는 628,510번 블록이 생성되었다. 이더리움은 비트코인보다 6년 뒤인 2015년 7월 30일에 런칭되었지만 약 15초에 하나씩 블록이 생성되므로 앞서와 동일한 2020년 5월 2일 오전 11시 44분 기준으로 이미 9,984,171개의 블록이 생성되어 비트코인보다 약 16배나 더 많다.

1-4 순서대로 배열된 블록

생성된 블록은 순서대로 보관된다. 이 순서는 대단히 중요해서 절대로 변경돼서는 안 된다.

〈그림 Ⅵ-2〉 블록이 논리적인 긴 사슬에 묶여 순서대로 늘어선 모습



〈그림 Ⅵ-2〉는 생성된 블록들이 그 순서에 따라 마치 하나의 긴 논리적 사슬(Chain)에 묶인 것처럼 길게 늘어선 개념도를 보여준다. 블록체인 내에 존재하는 트랜잭션들은 자신들이 기록된 블록에 의해 그 시간 순서가 정해지는데 m ＜ n일 때 m번 블록에 기록된 트랜잭션은 항상 n번 블록의 트랜잭션보다 시간적으로 먼저라는 의미다.

109) 시각은 모두 대한민국 표준시(GMT+9)로 표기한다.
110) 제네시스 블록(0번 블록)은 별도의 채굴과정 없이 그냥 만들어진다.

[사건의 순서] 타임스탬프 기계

블록체인은 타임스탬프(Time Stamp) 기계이다. 블록체인을 전산학의 네트워크 관점에서 보면 익명의 비동기화 네트워크에서 발생한 일련의 사건들을 일관성 있게 순서를 정하는 방법에 관한 연구라고 할 수 있다.
내가 돈을 쓰려면 그 전에 그 돈을 얻게 된 다른 사건이 반드시 존재해야만 한다. 이 두 사건의 순서가 바뀌면 돈을 쓸 수가 없다. 지급결제 시스템 역시 전체 거래의 순서가 대단히 중요하며 비트코인은 익명의 비동기화 네트워크에서 신뢰받는 서버 없이도 이러한 순서를 정할 수 있는 방법에 대한 연구라고 할 수 있다. 즉 발생된 모든 사건에 대해 공식적인 시점 처리(Time Stamping)를 하여 그 발생 순서에 대한 시비를 차단하는 시스템이다. 이런 관점에서 블록체인은 금융결제원의 공인 시점확인 서비스인 TSA(Time Stamping Authority)의 비동기화 익명 네트워크 버전이라고 비유할 수 있다.

1-5 블록에 저장되는 내용

비트코인의 각 블록에는 대략 10여 분 동안에 수집된 트랜잭션(=거래 내역)이 저장된다. 트랜잭션을 구성하는 내용은 매우 간단한데, 각각 송신자와 수신자의 비트코인 주소, 비트코인 이전 금액, 전자서명 데이터 등으로 이루어져 있다. 비트코인 주소는 은행의 계좌번호에 비유할 수 있는데 이 주소에는 상대방 공개키의 해시 값 정보가 들어 있어 적절한 암호화 키를 보유하고 있는 사람만이 사용할 수 있도록 보호하고 있다.[111)]

하나의 트랜잭션 데이터를 저장하려면 최소 200여 바이트가 필요하다. 따라서 최소 바이트로 구성된 트랜잭션으로만 블록을 가득 채운다면 단순 수치상으로는 5,000여 개까지 저장 가능하다. 그러나 블록에는 트랜잭션 이외에도 다른 부가적인 요약 데이터 등도 저장돼야 하고 또한 하나의 거래에서 다수의 상대에게 비트코인을 이전할 경우에는 그 대상자 수에 비례하여 트랜잭션의 크기가 증가하는 등 그 크기는 유동적이며 평균적으로 하나의 블록에는 대략 2,000 ~ 2,500여 개 내외의 트랜잭션이 저장된다.

111) 공개키와 해시 값에 대한 상세한 설명은 제4절에서 기술한다.

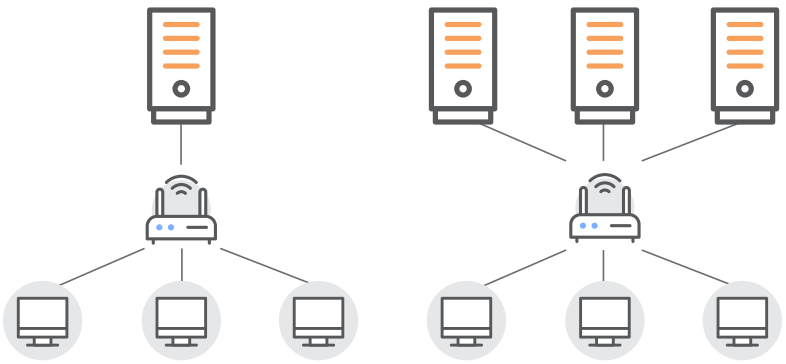
[블록과 거래 내역] 블록에 기록된 거래 내역 개수

블록 하나에 저장된 평균 트랜잭션 개수를 계산해 보면 2020년 1월 ~ 4월은 약 2092개, 2019년 전체 평균은 약 2240개이다. 전체적으로는 2009년 1월 3일 0번 블록부터 2020년 5월 1일의 628424번 블록에 이르기까지 저장된 총 발생 트랜잭션을 모두 세어보면 약 5억 2568만 건 정도가 된다.

2 분산 vs. 중복

2-1 중앙화 시스템과 분산 시스템

〈그림 Ⅵ-3〉 중앙집중 시스템과 분산 시스템



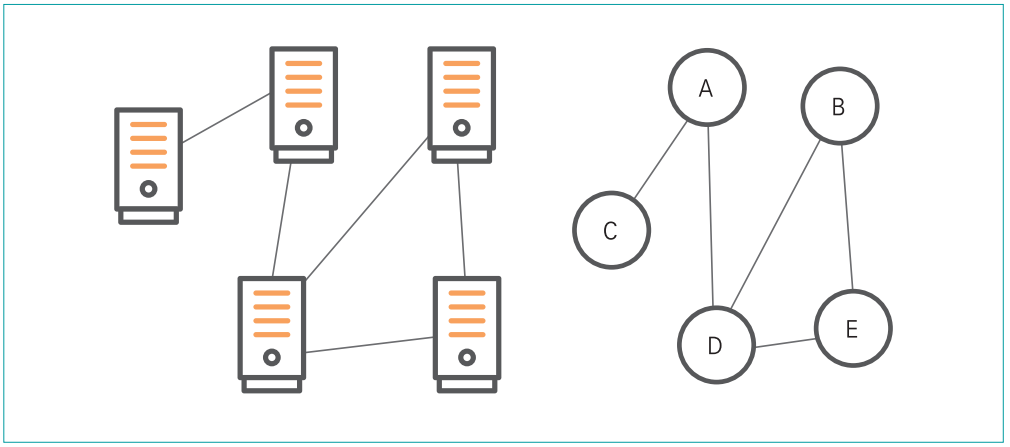
(a) 중앙집중 시스템 (b) 분산 시스템

하나의 서버가 전체 서비스를 실행하는 네트워크 시스템을 통상 중앙집중 시스템[〈그림 Ⅵ-3〉의 (a)]이라 부르고 여러 개의 서버가 작업을 나눠 처리하는 시스템을 분산 시스템[〈그림 Ⅵ-3〉의 (b)]이라 부른다. 중앙집중 시스템에서의 모든 사용자는 중앙 서버와 직접 연결되고 중앙 서버는 사용자의 모든 요청을 처리하고 서비스한다.

분산 시스템에서는 사용자의 처리를 여러 서버가 나누어 처리하게 된다. 분산처리는 크게 두 가지 목적에서 활용된다. 하나는 처리속도의 향상을 위한 배분 및 병렬처리이며 다른 하나는 안정성 향상을 위한 중복 보관 또는 처리이다. 특히 서버를 여러 군데 복제해 두면 어느 하나가 고장 나더라도 나머지 서버가 일을 대신하여 서비스의 안정성을 크게 높일 수 있고, 트래픽이 몰릴 경우 이를 분산하여 여러 대의 서버가 나눠 처리함으로써 전체 반응속도를 향상시킬 수 있다. 분산 구성은 비용을 어느 정도 증가시키지만 현대의 네트워크 시스템은 소규모를 제외하고는 중앙집중 시스템이라 하더라도 대개 어느 정도의 분산과 중복을 사용해 그 안정성을 높이고 있다.

2-2 노드와 피어

〈그림 Ⅵ-4〉 네트워크 구성도



〈그림 Ⅵ-4〉는 컴퓨터 네트워크 구성도를 보여준다. 그림의 왼편은 서버 및 이들 사이를 연결하는 네트워크 선을 그림으로 그린 것인데 보통은 보다 간결하고 쉬운 표현을 위해 그림의 우측처럼 그래프로 나타낸다. 그래프 표현에서는 컴퓨터 서버는 꼭짓점으로 표시하고 두 서버를 연결한 네트워크 선은 선분으로 표시한다. 그래프의 꼭짓점은 통상 노드(Node)라 부른다. 따라서 노드란 네트워크에 참여하고 있는(=연결된) 모든 컴퓨터를 지칭한다고 생각할 수 있다. 한편, 각 꼭짓점의 관점에서 자신과 직접적인 연결 관계를 유지하고 있는 꼭짓점은

특별히 피어(Peer)라고 부른다. 이에 기반하여 다시 〈그림 Ⅵ-4〉를 살펴보면, 우측의 그래프에서 노드의 개수는 5개로 고정이지만 피어의 개수는 꼭짓점마다 다르다. 꼭짓점 A의 피어는 두 개(C와 D)이고 꼭짓점 D의 피어는 세 개(A, B, E)이며 꼭짓점 C의 경우는 피어가 단 하나(A)뿐이다.

블록체인은 참여자 모두가 서버이자 동시에 사용자 역할을 수행하는 네트워크이다. 블록체인의 각 노드는 오로지 자신의 피어를 통해서 전달받은 정보에만 의존해 판단하게 된다.

[피어 IP 찾기] DNS 하드코딩

비트코인의 프로그램 소스와 운영은 bitcoin.org 도메인을 소유하고 있는 사적 단체가 관리하고 있다. 비트코인 네트워크에 처음 접속하면 이들이 운영하는 네임서버(Name Server)에 가장 먼저 접속한 다음 현재 운영 중인 IP 주소 목록 정보를 얻게 되고 이 정보를 기반으로 나의 피어를 형성하기 위한 접속을 시도하게 된다. 이 네임서버들의 IP 주소는 비트코인 클라이언트 프로그램에 하드코딩되어 있다. 이처럼 블록체인이라 하더라도 최소한의 기능을 하는 서버가 반드시 필요하다.

출처: 블록체인 해설서, 이병욱, 에이콘 출판사, 2019, p. 56

[피어의 중요성] 정직한 피어와 거짓된 피어

비트코인 네트워크에서의 모든 정보는 오로지 나의 피어를 통해서만 얻게 된다. 중앙 서버가 없기 때문이다. 이때 운이 나빠 거짓된 피어를 만나면 지속적으로 잘못된 정보를 얻을 수 있다. 특히, 많은 피어를 가진 거짓 노드가 존재한다면 쉽게 네트워크의 건전성이 훼손될 수 있다. 이처럼 많은 피어를 가진 소수의 거짓 노드가 규합하여 비교적 손쉽게 다수의 노드를 속이는 공격을 이클립스(Eclipse) 공격이라고 한다. 개기일식으로 달이 태양을 완전히 가려버리는 것처럼 거짓 노드에 연결된 피어들은 모두 거짓 정보만 받게 되는 상황을 비유한 것이다.

2-3 분산 시스템과 블록체인

흔히 블록체인을 분산원장으로 설명하지만 이는 부정확한 설명이다. 분산원장은 보편적인 저장기술일 뿐 블록체인만의 속성이 아니므로 하나의 속성을 전체 부류로 일반화한 오류라 할 수 있다. 또한 블록체인은 분산보다는 극단적인 중복 시스템에 더 가깝다.

블록체인의 모든 노드는 동일한 권리와 의무를 가지며 그 어떤 노드도 더 많은 권한이나 데이터를 가지고 있지 않다. 또한 블록체인의 모든 노드는 동일한 데이터를 중복 저장한다. 그러나 그 이유는 앞서 설명한 분산 시스템의 처리속도나 안정성 향상과는 거리가 멀다.

블록체인에서 모든 노드가 데이터를 중복 저장해야 하는 결정적인 이유는 그 어떤 노드도 '신뢰할 수 없기' 때문이다. 결국 모든 노드가 반복해서 작업을 수행하는 극단적 비효율은 신뢰받는 서버를 제거했기 때문에 치러야 할 대가이자 고육지책인 셈이다. 이 부분의 기술적 관점은 제7장 제1절에서 보다 자세히 설명하겠지만 블록체인은 분산 시스템이 아닌 극단적 중복 시스템에 가깝다는 점을 기억하도록 한다.

[신뢰할 수 없는 사회] 전 사원의 중복

김 대리를 못 믿으면 같은 일을 서 대리에게도 시켜야 한다. 서 대리도 못 믿으면 박 과장도 같은 일을 시켜야 한다. 그러다 결국 전 직원에게 같은 일을 시키게 된다. 이러한 방법은 전 직원을 못 믿을 때의 고육지책으로 비용 때문에 안 하는 것이지 몰라서 안 하는 것이 아니다. 신뢰는 곧 돈이다. 블록체인은 효율을 위한 분산 시스템이 아니라 신뢰를 할 수 없어서 전 사원이 같은 일을 반복해야 하는 중복 시스템이라는 사실을 기억하자.

[노드의 역할] 완전노드와 SPV 노드

사실 블록체인의 모든 노드가 동등하지는 않다. 블록체인의 노드는 크게 3가지로 구분되는데 첫째, 채굴과 검증을 모두 하는 노드. 둘째, 검증만 하는 노드. 셋째, 단순 사용자 노드이다. 이 중 첫째, 둘째를 완전노드(Full Node)라고 하고 단순 사용자 노드를 SPV(Simple Payment Verification)라 부른다. SPV는 데이터를 저장하지 않고 요약 정보만 갖고 있다. 비트코인의 경우 약 1,500만 정도의 SPV가 있는 것으로 알려져 있는데 완전노드는 단 10,000여 개에 불과하다. 하지만 이 중에서 채굴까지 겸하는 노드는 극히 드물며 전체 채굴의 90% 이상은 단 10개 노드가 독점하고 있다. 2020년 5월 기준으로 완전노드가 되려면 최소 250기가바이트의 블록체인 데이터를 다운로드 받아야 한다. 비록 노드 형태는 다양하지만 자신이 어떤 형태의 노드로 네트워크에 참여할지는 스스로 결정할 수 있다. 여기서는 모든 노드가 완전노드라는 관점에서 설명한다. 채굴에 대한 자세한 설명은 제3절 마지막에서 다시 언급한다.

3 프라이버시 보호를 위한 극단적 비효율

앞서 비트코인은 프라이버시 보호가 되는 지급시스템을 구성하기 위해 '금융기관을 배제'시키는 방법을 선택했다고 설명했다. 그로 인해 비트코인에는 극단적인 비효율 두 가지가 필요하게 되었는데 그중 하나는 앞서 잠시 언급한 '모두에 의한 저장과 검증'이며 또 다른 하나는 작업증명을 통한 기록의 비가역성이다. 이제 각각을 자세히 살펴보기로 한다.

3-1 모두에 의한 저장과 검증

비트코인은 지급결제 시스템이다. 즉 비트코인을 서로 주고받은 거래를 기록하는 것이 그 핵심 기능이다. 따라서 발생한 모든 거래 내역을 빠짐없이 기록해야 하는 것은 물론 그 기록이 정확한 것인지에 대한 검증도 필요하다. 우리나라는 금융결제원이 금융공동망을 운영하며 기록의 검증을 통해 청산(Clearing) 기능을 수행하고, 한국은행은 금융결제원의 청산 데이터를 신뢰하고 그에 기반해 최종 결제(Settlement) 기능을 수행한다. 미국도 지급결제망으로 Fed-Wire를 운영하며 동일한 방식으로 처리한다.

그 자세한 매커니즘은 제7장 제5절에서 다시 살펴보겠지만 비트코인에서는 지급결제 청산 절차가 동시에 발생하며[112] 그 처리에 네트워크의 모든 노드가 관여하도록 설계되어 있다. 중요한 점은 블록체인에는 금융결제원과 같은 역할을 수행할 어떠한 '신뢰받는 자'도 존재하지 않는다는 사실이다.

따라서 모든 지급결제 청산 데이터는 전 노드가 중복 보관하고 동시에 검증작업도 반복 수행한다. 이때 (ⅰ) 규칙을 준수한 데이터는 보관하고 그렇지 않은 데이터는 즉시 폐기한다. (ⅱ) 자신의 피어를 통해 이 과정에서 발생한 네트워크 내 모든 데이터를 단 한 바이트도 빠지지 않고 전달하거나 전달받아 전체 노드가 같은 데이터를 공유하게 된다.

비트코인의 경우 2020년 5월 기점으로 최소 250기가바이트의 저장공간이 필요한데, 현재 완전노드 개수는 대략 10,000여 개로 추정되므로 고작 5억 건의 거래 데이터를 저장하기 위해 무려 2,500테라바이트의 저장 공간을 낭비하는 셈이다. 또한 한번 거래가 일어날 때마다 그 무결성을 전체 노드가 중복해서 검증을 수행하며 그 결과를 끊임없이 서로 공유하기 위한 에너지를 낭비하게 된다.

한편 모든 데이터가 전체 노드에 공유되므로 정보 보안이 이루어지지 않는다. 모든 정보가 노출되기 때문이다. 비트코인의 경우 그간 일어난 5억 건의 거래 내용은 모든 노드에 그대로 노출된다.

[블록체인의 중복] 중복과 안전성

비트코인의 '모두가 저장하고 모두가 검증'하는 방식은 블록체인이 가진 매우 안전한 특성으로 왜곡되기도 하는데 이는 크게 다음 두 가지 이유로 인해 사실과 다를 수 있다.
첫째, 중복은 과도한 비용 때문에 사용을 꺼리는 일반적인 방식일 뿐 그 자체가 기술은 아니다. 중복이란 늘 비용과 안정성 사이의 트레이드오프일 뿐이다.
둘째, 중복만으로 '안전성'이 올라가지는 않는다. 기록자체는 여러 사본이 존재하지만 전체 기록이 완전 노출되어 정보 보호가 전혀 되지 않는다. 데이터보안에서의 '안전성'은 보관만 의미하는 것이 아니라 정보자체의 보호도 포함한다. 블록체인에서는 정보를 보호할 방법이 없다.

112) 제7장 제5절에서 살펴보겠지만, 비트코인은 별도의 청산결제 절차가 필요 없다. 지급행위가 곧 청산결제까지 포함하기 때문이다.

3-2 작업증명을 통한 비가역성

비트코인은 모든 노드가 데이터 전체를 검증하는 데 참여한다고 설명했다. 2020년 5월 기점으로 5억 건이 넘는 거래가 생성되었으니 비트코인 블록체인에 참여한 모든 노드들은 이 5억 건 각각에 대해 규칙위반이 없는지 검증을 수행했다는 의미가 된다.

그런데, 일단 한번만 검증을 마치면 안심해도 될까? 검증을 통과한 다음 누가 그 기록을 쉽게 변경할 수 있다면 어떻게 될까? 이런 경우라면 한번 검증한 기록이라도 일정한 시간이 지나면 주기적으로 다시 데이터의 무결성을 재검증해야만 할 것이다. 따라서 네트워크의 모든 노드가 끊임없이 재검증을 하느라 에너지를 낭비해야 할 것이며 시간이 흐를수록 트랜잭션이 누적되어 네트워크 에너지의 대부분을 재검증에만 낭비하게 될 것이다.

이 때문에 블록체인에는 '비가역적 저장장치'가 필요했다. 즉 만약 일단 기록하면 다시는 변경할 수 없는 저장장치만 존재한다면 데이터가 최초 기록될 때 단 한 번만 검증하면 다시는 재검증할 필요가 없을 것이다. 그 데이터는 다시는 바뀌지 않을 것이기 때문이다.

물론 한번 기록하면 다시는 바뀌지 않는 저장장치 같은 것은 이 세상에 존재하지 않는다. 많은 사람들이 블록체인을 항구적 저장장치로 착각하지만 당연히 그렇지 않다. 다만 그 변경이 매우 어렵도록 하는 여러 기법이 존재하는데 그것이 바로 제4절에서 자세하게 설명하게 될 작업증명(Proof of Work)이다.

비트코인은 작업증명을 사용해 기록의 변경을 어렵도록 했는데 비트코인이 설계한 작업증명에는 천문학적 에너지가 소모된다. 그 구체적인 내용은 제4절에서 자세히 설명하기로 한다.

4 채굴

땅속의 광물을 캐는 것을 의미하는 채굴이란 단어가 블록체인에서는 작업증명을 수행하는 과정을 묘사하는 데 쓰인다. 채굴만큼 작업증명도 힘들다는 것을 비유한 셈이다. 그러므로 블록체인에서의 채굴이란 작업증명과 동의어로 생각하면 된다. 천문학적 에너지가 소비되는 데도 불구하고 사람들이 굳이 블록체인의 작업증명에 참여하는 이유는 소비된 에너지 이상으로 돈을 벌 수 있다는 기대 때문이다. 작업증명에 성공하면 그 보상금으로 비트코인이 주어지는데, 그 보상금은 보조금과 수수료로 이루어진다. 보조금은 새로 생성된 비트코인으로서 정액이며 수수료는 트랜잭션을 제출한 사람이 비트코인으로 지불한 요금으로서 변동금액이다.

채굴은 단순히 비트코인을 얻기 위한 절차만이 아니라 블록체인의 운영에 있어서 가장 중요한 필수요소이다. 비트코인의 트랜잭션을 기록하려면 반드시 먼저 채굴에 성공해야 하기 때문이다. 따라서 아무도 채굴을 하지 않는다면 기록을 못하므로 더 이상 비트코인의 이전이 불가능해지고 블록체인은 멈추게 된다. 이 때문에 블록체인은 채굴에 투입된 에너지와 그로 인해 얻게 되는 이익이 잘 조화를 이루도록 설계해야 하는 인센티브 공학이 무엇보다 중요하다. 아울러 현재 블록체인의 인센티브 공학 설계는 몇 가지 문제점을 안고 있는데, 그중 가장 큰 두 가지는 다음과 같다.

첫째, 인센티브가 가상자산으로 주어진다. 가상자산은 그 내재가치가 0이며 외부에서 형성된 가격도 그 변동폭이 심해서 채굴꾼들이 가치를 예측하기 힘들고 불안정해 채굴 동인을 크게 저하시킨다.

둘째, 블록체인의 모든 인센티브는 오직 채굴업자에게만 주어진다. 앞서 설명한 대로 블록체인은 '모두에 의한 검증'에 의해 그 건전성을 유지하는데 검증에만 참여한 노드에게는 어떠한 인센티브도 주어지지 않는다. 이 때문에 검증노드의 수는 지속적으로 줄고 있어 블록체인의 건전성도 그에 따라 지속적으로 약해지고 있다.

제4절

블록체인 기반기술

이 절에서는 블록체인을 이루고 있는 기반기술을 모두 살펴본다. 따라서 다소 기술적 요소가 많아 어렵게 느껴질 수 있지만 대부분은 일반적 정리로 쉽게 해설하고 있어 이해하는 데는 큰 어려움이 없을 것이다. 이제 하나씩 살펴보도록 한다.

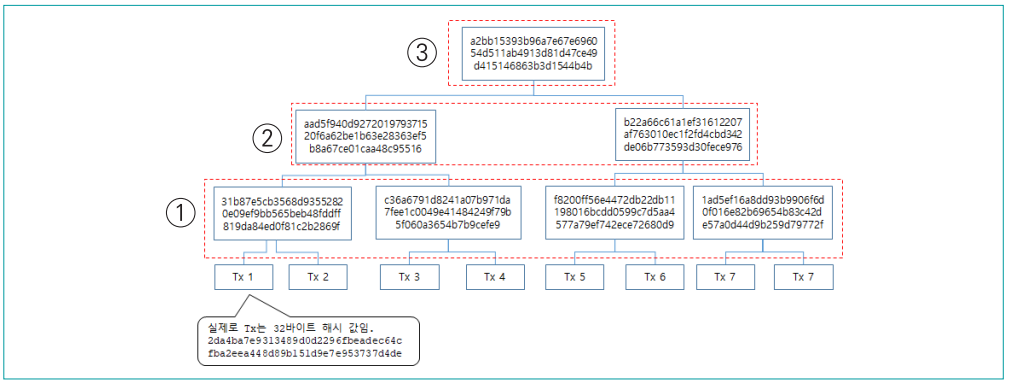
1 블록체인의 해시함수

이제 해시함수가 블록체인에서는 어떻게 사용되는지 알아본다. 비트코인은 SHA-256 암호화 해시를 사용한다. SHA-256은 미국국가안전보장국(NSA)에서 개발한 해시함수로서 그 이름에서 짐작할 수 있듯 입력 길이에 상관없이 항상 256비트 길이의 출력을 생성한다. 비트코인은 거의 모든 응용에서 SHA-256을 연속 두 번 적용한 값을 사용한다.

1-1 머클트리

머클트리는 랄프 머클(Ralph Merkle)이 1979년에 특허를 받은 기법으로 모든 데이터를 이진 트리를 이용해 하나의 대푯값으로 나타내는 기법이다. 다음 그림을 보자. 〈그림 Ⅵ-5〉는 8개의 트랜잭션(Tx1 ~ Tx8)에 대해 머클트리를 구성하는 개념도를 보여준다.

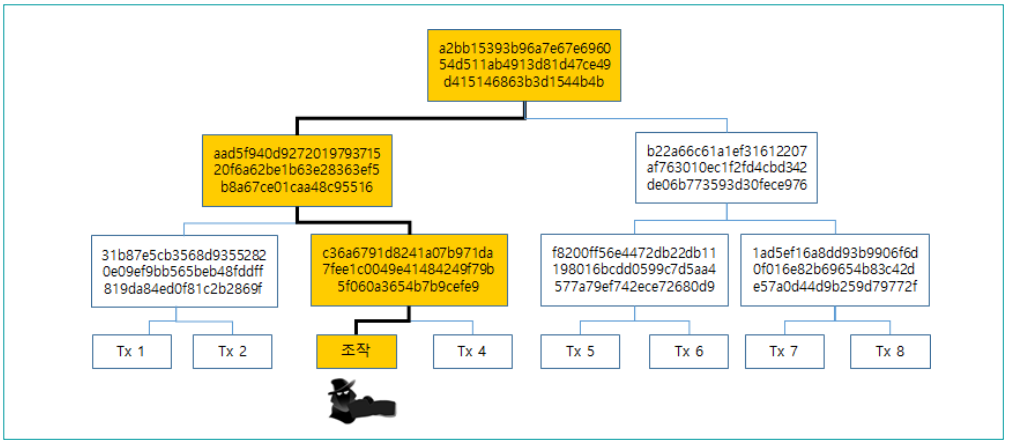
〈그림 VI-5〉 머클트리



출처: 블록체인 해설서, 2019, 이병욱, 에이콘 출판사, p. 107

그림에서 보듯 말단 노드부터 시작해서 트랜잭션을 두 개씩 쌍으로 이어붙인 뒤 이 데이터를 입력하여 하나씩 해시 값을 출력한다(①). 그 뒤 그 부모 노드에서 다시 두 개씩 쌍을 지은 후 이를 이어붙인 값을 입력으로 또 하나씩 해시 값을 만든다(②). 이 과정은 루트에 하나의 해시 값만 남을 때까지(③) 반복된다. 이런 식으로 루트에 있는 단 하나의 해시 값을 만드는 데 모든 트랜잭션이 관여하게 되므로 이 중 어느 하나의 값만 바뀌어도 루트의 값은 반드시 변하게 된다. 이제 트랜잭션이 바뀌면 어떻게 되는지 예를 살펴보자.

〈그림 VI-6〉 조작과 루트 해시의 변경



출처: 블록체인 해설서, 2019, 이병욱, 에이콘 출판사, p. 108

〈그림 Ⅵ-6〉은 Tx3이 변경되면 어떤 일이 벌어지는지 예시를 보여준다. Tx3이 변경되면 그 부모 노드의 값이 바뀌게 되고 이에 따라 그 부모의 부모 노드도 바뀐다. 이런 과정을 걸치면 결국 루트에 있는 해시 값도 변하게 된다. 결국 루트 해시 값만 보관하면 전체 트랜잭션의 변경 여부를 손쉽게 감지할 수 있게 된다.

1-2 그 외 해시 값의 사용

블록체인에는 이외에도 트랜잭션 아이디, 블록의 아이디, 해시퍼즐, 비트코인 주소[113] 등에 광범위하게 해시가 사용되고 있다. 여기서 한 가지 혼동해서는 안 될 사실은 블록체인은 해시라는 범용기술을 이용하고 있을 뿐 블록체인 자체가 해시는 아니라는 점이다. 따라서 누군가 "데이터의 변경 탐지를 쉽게 하려고 블록체인으로 구축했다."라고 말한다면 이는 주객이 전도된 잘못된 표현이라는 점을 이해하도록 하자. 데이터의 변경 탐지를 위해서는 해시함수를 이용하면 된다. 블록체인과는 무관하다. 이 관점은 제7장 제4절에서 좀 더 자세히 살펴보기로 한다.

2 비대칭 암호화 기법

제3장 제1절에서 살펴본 비대칭 암호화 기법은 블록체인에서도 사용되는데 전자서명에 활용하고 있다. A가 자신의 비트코인을 B에게 이전하려면 A는 다음의 내용이 담긴 거래 내역서를 작성해야 한다.

(A의 비트코인 주소, B의 비트코인 주소, A가 지출하려는 비트코인을 수령했던 트랜잭션 아이디, 이전하려는 금액, 기타 데이터)

113) 해시퍼즐과 비트코인 주소는 이 절 후반부에 다시 설명한다.

이제 A는 자신의 개인키를 사용하여 이 내역 전체를 전자 서명한 다음 내역서 마지막에 자신의 공개키와 함께 다음과 같이 추가한다.

(A의 비트코인 주소, B의 비트코인 주소, A가 지출하려는 비트코인을 수령했던 트랜잭션 번호, 이전하려는 금액, 기타 데이터, **A의 전자서명, A의 공개키**)

전자서명이 완료된 거래 내역서는 시스템에 제출되고 채굴과 검증과정을 통해 인증이 완료되면 그 기록은 항구히 남게 된다. 이 기록은 전자서명이 되었으므로 이제 변경이나 조작이 힘들다.

3 작업증명과 해시퍼즐

3-1 작업증명

작업증명(Proof of Work)이란 악의적 행동에 드는 에너지가 그로부터 얻을 수 있는 경제적 이익보다 더 크게 만들어 악의적 행동을 억제하려는 철학을 시스템에 구현한 것이다. 원래 1990년대에 스팸이나 서비스 거부 공격(DoS; Denial of Service) 등을 효과적으로 방지해 네트워크 자원의 오남용을 막기 위해 신시아 도크(Cynthia Dwork)와 모니 나오(Moni Naor)가 고안한 기법이다.[114] 작업증명의 핵심은 어떠한 서비스를 원하는 자에게 '결코 작지 않은 그러나 처리 가능한 수준의 과제를 요구'하는 것이다. 여기서 과제란 주로 컴퓨터의 계산 자원을 소모해야 하는 일을 의미한다.

비트코인에 구현된 작업증명은 '해시퍼즐(Hash Puzzle)'로서, 특정 패턴의 해시 값을 찾을 때까지 무차별 대입으로 무한 반복 계산하는 극단적 방식이다. 비트코인에서는 무엇을 '기록'하려면 반드시 이 해시퍼즐을 먼저 해결하도록 구현돼 있다. 그렇다면 얼마나 많은

114) wikipedia, https://en.wikipedia.org/wiki/Proof_of_work(최종 접속: 2020년 03월 16일)

횟수의 계산을 해야 하는지에 연계된 척도인 '난이도'를 살펴봄으로써, 비트코인에서의 '기록'이 얼마나 힘든 것인지 알아보자.

2009년 첫 비트코인 채굴에 필요한 해시함수 계산 요구량은 약 2^{32}번이었다. 이 2^{32}을 1이라 가정하고 이에 대한 상대적 계산요구량을 환산한 값을 '난이도'라 한다. 예컨대 난이도가 4라는 것은 2^{32}보다 네 배 더 계산이 필요하다는 의미로 $4 \times 2^{32} = 2^{34}$번의 계산이 필요하다는 뜻이다. 난이도는 하드웨어의 발전과 경쟁의 심화로 등락을 거듭하는데[115], 2020년 4월 말 기준으로 약 16조에 육박한다. 즉 최초 계산량(2^{32})보다 무려 16조 배 더 계산해야 한다는 의미이자 약 2^{76}번 정도 계산한다는 뜻이다. 이 과정을 통과해야 겨우 블록체인에 '기록'을 남길 가능성이 주어진다.[116]

[작업증명과 에너지] PC의 작업증명

2^{76}번 가까이 해시함수를 계산해야 한다는 의미가 어떤 것인지 감이 잘 안 올 것이다. 실제로 계산을 한번 해 보자. 2020년 5월 기점으로 GPU가 장착된 개인용 컴퓨터는 통상 초당 약 2천만 번 정도의 해시함수를 계산할 수 있다. 이 컴퓨터로 약 2^{76}번, 좀 더 정확히 말해 $2^{32} \times 16$조 번 해시함수를 계산한다면 무려 108,954,016년 즉, 1억 9백만 년 정도의 시간이 걸린다! 한편, 그 시간 동안의 전기세를 월 3만원 정도로 어림하면 대략 40조원의 전기세가 필요하다. 이제 비트코인의 작업증명이란 것이 얼마나 많은 에너지를 요구하는 것인지 확실히 이해되었을 것이다.

해시퍼즐을 '채굴'에 비유한 것도 이렇듯 막대한 자원이 소모되기 때문이다. 한편, 전용 칩을 사용한 전문 채굴꾼은, 2^{76}번의 계산량을 단 10분 정도에 처리한다. 이들이 개인용 컴퓨터보다 수조 배나 더 빨리 계산을 할 수 있는 비결은 병렬처리에 있다. 해시퍼즐은 구조상 전체 계산을 완전히 병렬 처리할 수 있어서, 이들은 특화된 집적 회로는 물론 때로는 수십만 대 이상의

115) 블록체인의 난이도는 조정은 2,016개 블록이 생성될 때마다 이루어지며 대략 2주에 한 번 꼴이다.

116) 이 과정을 통과했다고 반드시 기록할 수 있는 것이 아니다. 이 과정을 가장 먼저 통과한 단 한 명에게만 기록할 수 있는 권리가 주어지고, 나머지는 기회가 박탈된다.

컴퓨터를 동원하고 여러 업체가 연합하기도 하는 등 전체 해시 연산을 병렬로 수행한다. 이 과정에 대규모 하드웨어와 막대한 전기가 소요되는 것은 물론이다.

비트코인에서 '채굴'은 '기록'과 동의어로 이해해도 무방하다[117]. 채굴하지 않으면 기록할 수 없고, 기록하지 않으면 시스템은 멈춘다. 비트코인은 '지급/결제 시스템'이므로, 결제 내역을 기록할 수 없다면 더 이상의 거래는 일어날 수 없기 때문이다.

[채굴에너지와 보상금] 채굴업의 손익분기점

엄청난 에너지가 소모되는 데도 불구하고 채굴을 하는 이유는 성공하면 새로 생성된 비트코인을 얻을 수 있고, 이를 시중에 내다 팔면 법정화폐로 교환할 수 있기 때문이다.
2020년 초 전문 채굴업자의 손익분기는 대략 비트코인 시세가 USD7,000 ~ 8,000인 지점으로 추정된다. 비트코인은 약 4년마다 보상이 반감하는데, 최근의 반감은 2020년 5월 11일에 있었으며, 그 이후의 손익분기 시세는 약 USD12,000 ~ 15,000 정도로 추정된다.[118] 따라서 그 시점 이후는 막대한 손실을 감내하지 못해 채굴이 멈출 수도 있다. 2020년 3월 16일 기점의 비트코인 시세는 USD5,350이다.[119]

3-2 해시퍼즐

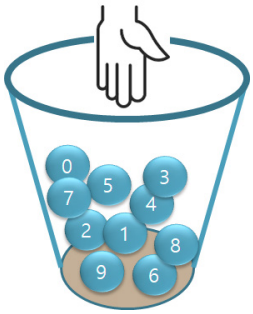
비트코인이 처음 소개되었을 때, "수학문제를 풀면 돈을 준다."는 말을 들어본 적이 있을 것이다. 그 수학문제가 바로 해시퍼즐이자 비트코인의 작업증명이다. 그러나 사실 수학이 아닌 산수이며 그 답을 알 수 있는 유일한 방법은 오로지 시행착오밖에 없다. 이제 비유를 통해 비트코인의 해시퍼즐이란 무엇인지 알아보도록 하자.

---

117) 엄밀히 말하면 채굴은 기록을 위한 조건이지만, 채굴은 오직 기록만을 위해 존재하므로 둘은 동의어라고 생각해도 무방하다.
118) COINTELEGRAPH, https://cointelegraph.com/news/bitcoin-halving-can-have-negative-short-term-effect-on-btc-price-heres-why(최종 접속 2020년 3월 16일)
119) CoinMarketCap 기준, 최종 접속(한국 시각 2020년 3월 16일 오전 11시 20분 기준)

가. 바구니에서 공 꺼내기

〈그림 Ⅵ-7〉 바구니에서 공 꺼내기



〈그림 Ⅵ-7〉은 0부터 9까지 숫자가 적혀 있는 공 10개가 들어 있는 바구니에서 무작위로 하나의 공을 꺼내는 실험을 보여주고 있다. 이 실험은 사전에 정한 목푯값 T보다 작거나 같은 숫자가 적힌 공을 꺼낼 때까지 무작위로 공을 꺼냈다 다시 집어넣기를 반복한다.

만약 목푯값 T가 9라면, 꺼낸 공에 적힌 숫자가 9보다 작거나 같을 확률은 100%이므로 단 한 번에 성공할 수 있다. 공에 적힌 모든 숫자는 9보다 작거나 같기 때문이다. 또 T 값이 4라면 무작위로 꺼낸 공에 적힌 숫자가 T보다 작거나 같을 확률은 50%이다. 10개의 공들 중에서 4보다 작거나 같은 숫자가 적힌 공은 5개(0, 1, 2, 3, 4)이기 때문이다. 따라서 공 꺼내기를 두 번 정도 시행하면 성공할 것으로 기대할 수 있다. 계속해서 만약 T가 0이라면 무작위로 꺼낸 공에 적힌 숫자가 0보다 작거나 같을 확률은 10%이다. 이때 성공할 때까지 공을 꺼내야 하는 횟수의 기댓값은 10번이 될 것이다. 이 실험에서 직관적으로 알 수 있는 것은 범위가 정해진 숫자를 무작위로 하나 꺼낼 때 그 값이 목푯값 T보다 작거나 같을 확률은 T가 작을수록 줄어들고 그에 따라 성공할 때까지 필요한 시행 횟수는 더 늘어난다는 점이다.

나. 비트코인 해시퍼즐

바구니에서 공 꺼내기를 이해했다면 비트코인 해시퍼즐을 이미 완벽히 이해한 셈이다. 유일한 차이는 이제 공의 개수는 10개가 아니라 2^{256}개이며 공에 적힌 숫자도 0부터 9가 아니라 0부터 $2^{256}-1$로 무척 많아졌다는 것뿐이다. 나머지 과정은 모두 동일하다.

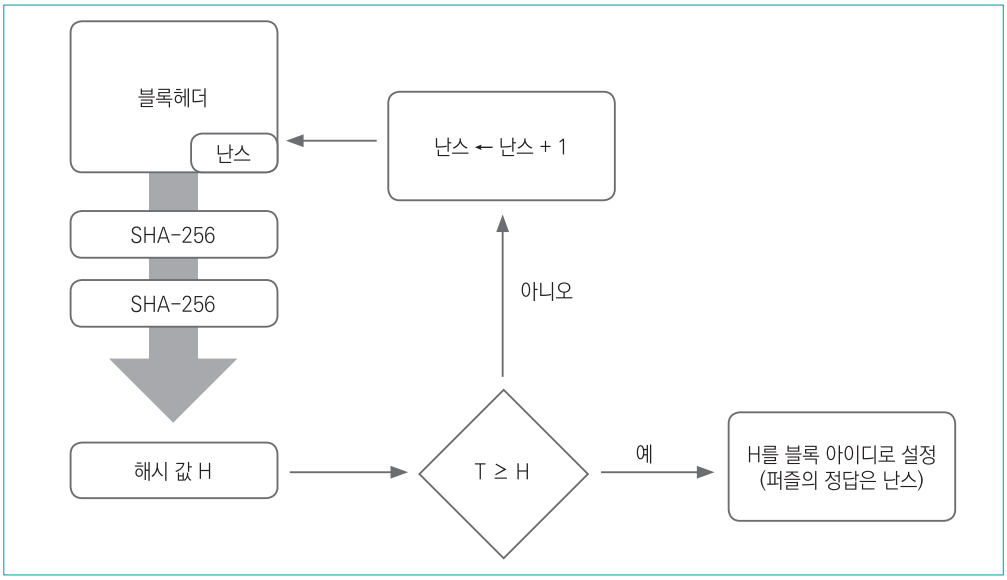
SHA-256 함수는 임의의 입력에 대해 항상 256비트의 고정된 출력을 생성한다는 것을 기억하자. 따라서 SHA-256의 출력은 이진수로 0이 256개 있는 00000000 … 000부터 1이 256개 있는 11111 … 111 사이의 어느 정수일 것이다. 따라서 그 값은 0부터 $2^{256}-1$ 사이의 어떤 정수인 셈이다. 결국 해시퍼즐이란 어떤 입력에서 우연히 발생한 해시 값이 사전에 정해진 목푯값인 T 값보다 작거나 같을 때까지 반복하며 찾아가는 과정이다. 이때 찾은 값이 바로 그 블록만의 고유 아이디가 된다.

다. 비트코인 블록 아이디와 해시퍼즐

지금까지 0번 블록, 620,000번 블록처럼 블록이 만들어진 순서를 이용해 특정 블록을 지칭해 왔지만 사실 블록체인의 모든 블록은 자신만의 고유한 숫자를 가지고 있다. 그 고유번호는 256비트 길이의 임의의 정수이며 해시퍼즐을 통해 생성된다.

해시퍼즐이란 그 정답인 난스(Nonce)를 찾는 과정인데, 그 결과로 얻게 된 해시 값이 바로 블록의 고유한 아이디가 된다. 이를 자세히 알아보기 위해 해시퍼즐 과정을 요약한 개념도인 〈그림 Ⅵ-8〉을 살펴보자.

〈그림 Ⅵ-8〉 비트코인 해시 정답인 난스를 찾는 과정



비트코인의 각 블록에는 그 블록의 모든 정보를 요약한 80바이트의 고정된 크기인 블록헤더가 있다. 블록헤더는 모두 6가지 구성요소를 가지고 있는데 그 마지막 구성요소가 바로 해시퍼즐의 정답을 기록할 난스이다. 이 난스를 찾는 과정은 다음과 같다.

1) 블록헤더에 있는 난스 값을 0으로 초기화한다.
2) 블록헤더에 SHA-256을 연속 두 번 적용해 해시 값 H를 얻는다.
3-1) T(목푯값) ≥ H(해시 값)이면 해시퍼즐에 성공한 것이며, 이때의 H 값이 이 블록의 고유한 아이디가 되며 과정은 끝이 난다. 이때의 난스 값이 바로 해시퍼즐의 정답이 된다.
3-2) T(목푯값) < H(해시 값)이면 난스 값을 1 증가시킨 다음 2)번 과정으로 다시 돌아간다.

라. 해시퍼즐의 난이도 조절

그렇다면 목푯값 T 값는 어떻게 정해지는 것일까? 비트코인은 2,016개의 블록이 생성될 때마다(약 2주) 그 사이에 블록이 생성된 속도를 측정하여 T 값을 조절한다. 앞서 설명한 논리대로 T 값을 낮추면 해시퍼즐의 난이도는 상승하게 되고 T 값을 올리면 난이도는 내려가게 된다. 2009년 비트코인이 최초로 만들어 졌을 때의 목푯값을 T_0이라 하고 m번 블록이 생성된 시점의 목푯값을 T_m이라 하면, m번 블록의 난이도 D_m은 다음과 같이 구할 수 있다.

$$D_m = T_0 / T_m$$

628,000블록은 2020년 4월 28일에 생성되었다. 그렇다면 $D_{628,000}$은얼마나 될까? 그 값은 무려 15,958,652,328,578.42나 된다. 즉 제네시스 블록보다 약 16조 배 이상 더 어려워졌다는 의미가 된다. 앞서 최초의 블록에서 채굴을 위한 계산량이 2^{32}번이었다고 설명한 것을 기억하는가? 그 2^{32}번이란 T 값을 찾을 때까지 난스를 1씩 증가시키면서 반복해서 해시함수를 계산해야 했던 횟수가 2^{32}번이라는 의미가 된다. 또 같은 맥락에서 628,000번 블록을 채굴하는 데 필요한 계산 횟수는 2^{32} x 15,958,652,328,578.42이라는 의미가 된다!

마. 난이도 조절의 이유

사토시 나카모토는 비트코인의 블록이 평균 10분에 하나씩만 생성되기를 원했다. 그러나 소위 무어의 법칙(Moore's Law)에 따라 반도체 기술의 발달속도는 매 18개월마다 그 집적도가 두 배가 되어 성능도 두 배로 발달해 오고 있다. 이 때문에 비트코인은 2,016개의 블록이 생성될 때마다 실제 블록이 생성된 시간을 측정해 난이도를 조절했던 것이다.[120] 즉, 정확히 10분에 하나의 블록이 생성된다면 2,016개의 블록을 생성하는 데 소요되는 이론적 시간은 1,209,600초이어야 한다. 따라서 2,016개의 블록이 이보다 더 빨리 만들어졌다면 이는 하드웨어가 발전했다는 의미이므로 난이도를 높여야 할 것이고 이보다 더 늦게 만들어졌다면 난이도를 낮춰야 할 것이다. 난이도 조절은 직전 난이도에 비해 최대 300%까지 올리거나 최대 75%까지 낮추면서 조정된다. 이 난이도 조절 방식은 블록체인마다 상이하다. 예컨대 이더리움의 경우 매번 블록이 생성될 때마다 난이도를 조절하므로 평균 15초에 한 번씩 난이도를 조절하고 이는 비트코인보다 80,640배나 더 빈번한 것이다.

한편 비트코인의 난이도가 무어의 법칙에 따라서만 변해왔다면 2009년 1월부터 대략 136개월이 경과한 2020년 5월 기점의 난이도는 고작 157.6 정도에 불과해야 한다. 그러나 실제 난이도는 그보다 1,000억 배나 더 많은 16조 배에 이른다. 이는 비트코인의 난이도가 하드웨어의 자연스러운 발전을 따라 변해온 것이 아니라 채굴업자들의 무분별한 치킨게임을 통해 기하급수로 증가해왔다는 의미가 된다. 해시퍼즐은 완벽히 병렬처리가 가능하므로 컴퓨터를 두 대 동원하면 두 배 더 빨리 해결할 수 있고, 10만 대를 동원하면 10만 배 더 빨리 해결할 수 있다. 전문채굴업자들은 병렬처리가 가능한 특수칩을 장착한 컴퓨터를 수만 대 동원하여 일반 PC보다 수조 배 더 빨리 계산할 수 있다. 이 때문에 앞서 설명한 대로 일반 PC로 1억 9백만 년이나 걸리는 계산량을 전문 채굴꾼들은 지금도 단 10여 분에 해결하고 있다. 따라서 현재 비트코인 블록을 일반 사람이 생성할 수 있는 확률은 0이다. 이것이 바로 전체 블록생산의 90%를 단 10개의 대형 채굴업자가 독점하고 있는 근본적 이유이다.

---

120) 실제로는 버그로 인해 2,015개마다 조절한다. 이렇듯 종종 0부터 시작하는 지수를 착각해 일어난 프로그램 버그를 off-by-one-error라고 부른다.

4 연쇄해시

이제 해시와 작업증명을 알아보았으니, 블록체인에서는 어떤 식으로 기록의 비가역성을 구현했는지 살펴보도록 한다. 앞서 잠시 언급한 블록헤더의 6개 구성요소 중 하나는 이전 블록의 아이디 값이다. 앞서 현재 블록헤더 값에 SHA-256을 두 번 연속 적용하여 해시퍼즐을 반복하며 블록의 고유 아이디를 찾았던 과정을 기억하자. 현재 블록의 아이디를 찾기 위한 해시함수의 입력에 이전 블록의 아이디 값이 들어 있음으로 해서 재미있는 관계가 형성된다.

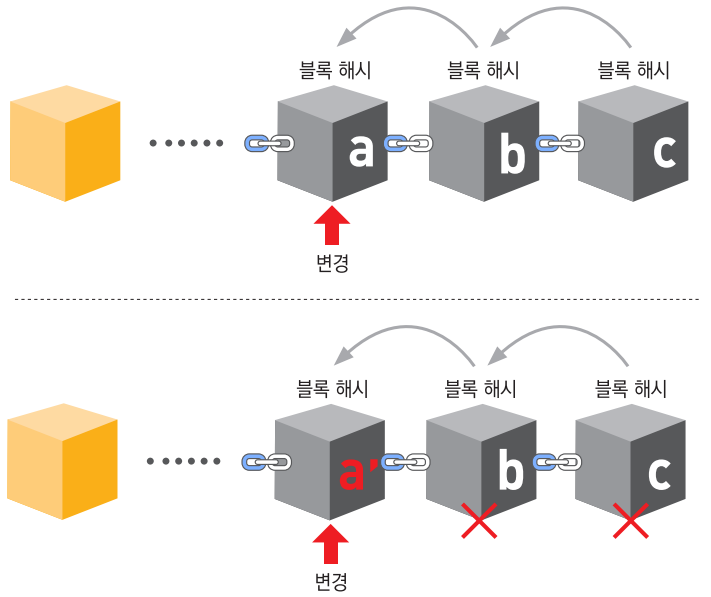
H_n을 블록 n의 해시 값 즉 고유 아이디라 하고, BH_n이 n번 블록헤더 중 이전 블록 아이디(해시 값)를 제외한 나머지 5개 요소라고 하자. 그렇다면 H_n은 다음을 만족한다.

$$H_n = Hash(BH_n, H_{n-1})$$
$$H_n = Hash(BH_n, Hash(BH_{n-1}, H_{n-2}))$$
$$H_n = Hash(BH_n, Hash(BH_{n-1}, Hash(BH_{n-2},... Hash(BH_1, H_0).....)))))$$

즉, 블록 n의 해시 값을 생성하는데 n-1번 블록 아이디가 관여했다는 의미는, n-1번 블록의 아이디에는 n-2번 블록 아이디가 관여했다는 의미가 된다. 이 말은 n번 블록의 해시 값에 영향을 끼친 n-1번 블록 아이디는 n-2번 블록의 아이디로부터 영향을 받았다는 것이므로 결국 n-2번 블록 아이디가 n번 블록 아이디의 생성에까지 영향을 끼친 것이다. 이렇게 연쇄적으로 n번 블록의 아이디 생성에는 결국 0번 블록인 제네시스부터 시작해서 n-1번까지의 모든 블록 아이디가 영향을 끼친 셈이 된다.

이 때문에 m번 블록의 내용이 변경되어 그 해시 값이 변경되면 모든 k ($k > m$)번 블록의 해시 값도 같이 변경되게 된다. 다음 〈그림 Ⅵ-9〉를 보자.

〈그림 Ⅵ-9〉 연쇄 해시로 인한 변경과 영향



〈그림 Ⅵ-9〉[121]에서 a번 블록이 변경되어 그 블록 아이디가 변경되면, 그 이후에 생성된 모든 블록의 아이디도 바뀌게 된다. 그 이후의 블록 아이디를 생성할 때 a번 블록의 아이디가 사용되었기 때문이다. 이 때문에 m번 블록의 어떤 값을 변경한 후 일관성을 유지하기 위해서는 모든 k(k ≥ m)번 블록의 해시 값을 다시 계산해야만 한다.

앞서 블록의 해시 값을 계산하는 데는 엄청난 에너지가 필요했다는 점을 기억하자. 만약 제네시스 블록의 값이 변경된다면 630,000여 개에 달하는 모든 블록의 해시 값을 다시 계산해야 하고 이는 사실상 불가능하다. 따라서 블록체인에서 한번 기록한 것을 변경하는 것이 무척 힘든 이유는 기록의 변경으로 인해 바뀌어 버린 해시 값을 다시 계산하는 데 천문학적인 에너지가 필요하기 때문이다. 그러나 변경에 대한 이 저항성은 오래된 블록에만 해당된다.

121) 비트코인과 블록체인, 탐욕이 삼켜버린 기술, 이병욱, 2018, 에이콘 출판사, p. 124

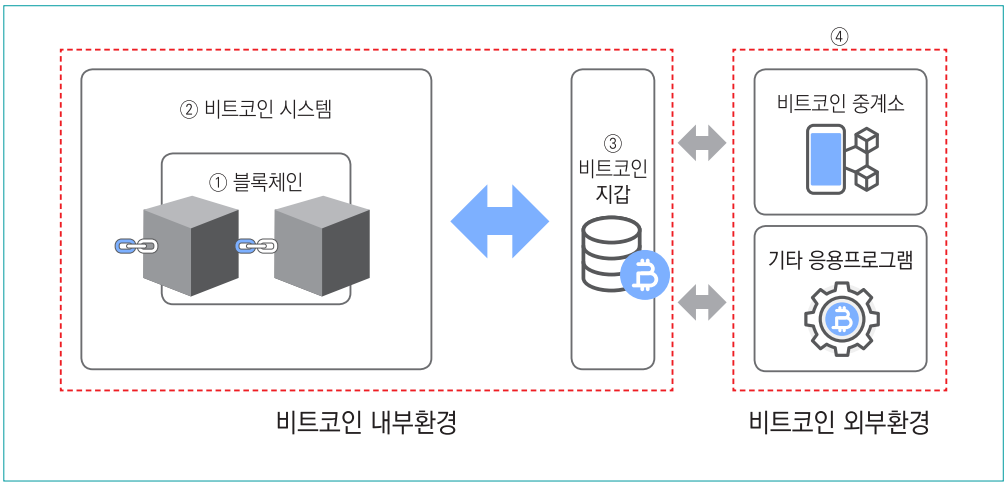
예컨대 새로 만들어진 블록의 경우 그 값이 변경되더라도 다시 계산해야 하는 해시 값은 현재 만들어진 블록 아이디뿐이다(k ≥ m에서 k = m이므로 단 하나만 계산하면 된다). 따라서 블록체인은 생성이 오래된 블록일수록(=자기 다음의 블록이 많아질수록) 그 변경에 대한 저항성이 기하급수로 증가하는 구조를 가지고 있다.

5 지갑과 비트코인 주소

5-1 비트코인 지갑

비트코인을 사용하기 위해서는 소위 지갑 소프트웨어가 필요하다. 지갑 소프트웨어는 블록체인을 이루는 구성요소는 아니며 블록체인을 이용하기 위한 인터페이스를 제공해 주는 역할을 한다. 다음 그림을 보자.

〈그림 Ⅵ-10〉 블록체인과 그 주변환경



출처: 비트코인과 블록체인, 탐욕이 삼켜버린 기술, 이병욱, 2018, 에이콘 출판사, p. 184

〈그림 VI-10〉은 블록체인과 지갑과의 관계를 보여준다. 그림의 ①번 영역이 블록체인의 고유 영역이며 ②번 영역은 이를 비트코인이라는 가상자산에 응용한 비트코인 시스템을 보여준다. ③번 영역이 바로 지갑이다. 그림에서 보듯 지갑 소프트웨어는 비트코인 시스템과 상호작용하며 블록체인을 이용하고 있다. 가상자산 중개소는 모두 이 지갑 소프트웨어를 이용하여 판매자와 구매자를 중개하는 역할을 한다. 지갑 소프트웨어는 크게 세 가지 역할을 수행한다.

첫째, 사용자가 이용할 암호화 개인키와 공개키를 생성해 준다.
둘째, 비트코인 주소를 생성한다. 지갑은 생성된 암호화 키를 이용하여 사용자의 비트코인 주소를 만들어 주는데, 이 주소를 사용하여 비트코인을 서로 주고받을 수 있다.
셋째, 비트코인 거래 요청서를 작성한 다음 이를 블록체인 네트워크에 제출한다.

한편 해킹으로부터 안전하게 보호하기 위해 일반적인 소프트웨어 대신 하드웨어로 된 지갑을 사용하기도 한다. 이 하드웨어 지갑은 대개 USB 모양을 하고 있는데, 평소에 암호화 키를 오프라인에서 보관하고 있다가 사용할 때에만 컴퓨터에 접속하므로 해킹으로부터 비교적 안전하게 보호할 수 있다는 장점을 가지고 있다. 이런 하드웨어 지갑을 보통 콜드 월릿(Cold Wallet)이라 부른다.

〈그림 VI-11〉 아마존에서 판매 중인 콜드 월릿

출처: Amazon, http://www.amazon.com/s?k=ledger&ref=nb_sb_noss+1

[지갑과 호환성] 가상자산 지갑들 간의 호환

가상자산마다 그 작동방식이 서로 상이할 수 있다. 일반적으로 서로 다른 가상자산의 지갑 소프트웨어끼리는 호환되지 않는다(한편, 이더리움의 토큰은 조금 다른데 이 부분은 제8장 제1절에서 다시 살펴본다.) n개의 가상자산을 사용하려면 통상 n개의 가상자산 지갑 소프트웨어가 필요하지만 하나의 지갑에 여러 기능을 통합하여 다수의 가상자산을 취급할 수 있게 구현된 통합형 지갑도 존재한다.

핵심정리

- 블록체인 개요
  - 1980년대 초에서 시작된 프라이버시 보호 운동은 1990년대 사이퍼펑크들에 의해 조직화되고, 2008년에 비트코인이라는 극단적 모습으로 등장한다.

  - 비트코인은 금융기관을 배제한 익명성을 추구했고 이 때문에 어노니머스라는 절대 익명성 때문에 반 금융적 속성을 가지게 되었다.
    절대 익명성을 위해 비트코인은 극단적 중복이라는 비효율이 필요했고 이는 일반적 분산 시스템과는 다른 모든 노드에 의한 중복이었다.

  - 블록체인의 원형인 비트코인은 절대 익명의 구현을 위해 비대칭형 암호화 기법의 전자서명, 연쇄 해시, 작업증명이라는 방법을 사용하고 있고, 이 방법은 여러 비효율과 관련되어 상업적 용도로 사용하기에 적합하지 않은 여러 걸림돌이 되고 있다.

헬로, 핀테크!(보안인증 · 블록체인)

7장

블록체인의 작동원리와 효용

7장 블록체인의 작동원리와 효용

학습목표

1. 블록체인의 작동원리를 설명할 수 있다.
2. 블록체인의 정의를 설명할 수 있다.
3. 블록체인의 효용을 설명할 수 있다.

학습개요

블록체인의 기본 작동원리인 브로드캐스팅(Broadcasting)과 리더선출을 이해하고, 서로 다른 노드가 동일한 데이터를 가지도록 해주는 매커니즘인 탈중앙화 합의에 대해 알아본 후 블록체인의 정의(Definition)를 정리해 본다.

이 장에서는 블록체인의 작동원리와 함께 그 정확한 정의, 비트코인 이후에 등장한 이더리움과 하이퍼 레저 등의 변형 그리고 블록체인의 진정한 효용 등에 대해 살펴본다.

용어해설

❶ 브로드캐스팅(Broadcasting)

네트워크 통신에서 대상을 별도로 지정하지 않고 접속된 모든 노드에게 데이터를 전달하는 방식이다.

❷ 엄브렐러(Umbrella) 프로젝트

엄브렐러 프로젝트는 그 안에 다른 서브(Sub) 프로젝트를 포함하고 있는 상위 프로젝트를 의미한다.

❸ 개념증명(Proof of Concept)

기존 시장에 없었던 신기술을 도입하기에 앞서 이를 검증하기 위해 소규모로 진행하는 프로젝트 등을 통한 타당성 증명 과정을 의미한다.

제1절

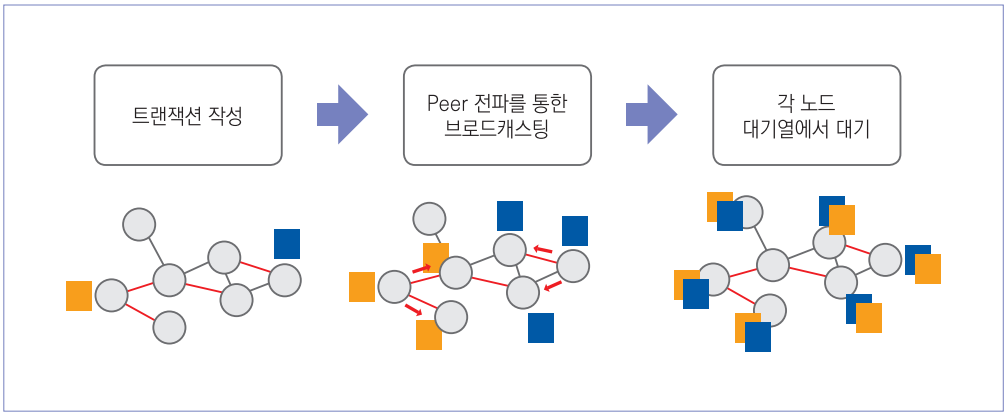
블록체인의 작동원리

1 브로드캐스팅과 리더 선출

1-1 브로드캐스팅

네트워크에서 브로드캐스팅(Broadcasting)이란 지정한 상대방이 없이 모든 접속자에게 데이터를 전송하는 방식을 일컫는다. 비트코인 블록체인에서 생성된 데이터는 모두 거래 내역(=트랜잭션)들이다. 이 거래 내역들은 앞서 설명한 것처럼 지갑 소프트웨어를 사용해 네트워크에 제출된 데이터들이다. 비트코인을 소지하고 있다면 누구든 지갑 소프트웨어를 이용해 이전 거래 내역서를 작성하고 네트워크에 제출할 수 있다. 이렇게 제출된 거래 내역 데이터들은 피어를 통해 모두에게 복제되어 전달된다. 즉, 자신이 만든 거래 내역은 물론 자신이 전달받은 데이터들도 빠짐없이 모두 피어에게 전달한다. 이를 전달받은 피어는 또 그의 피어에게 전달하므로 결국에는 모든 노드가 데이터를 전달받게 된다.

〈그림 Ⅷ-1〉 피어를 통한 브로드캐스팅 개념



〈그림 Ⅷ-1〉은 피어를 통해 데이터가 브로드캐스팅 되는 개념을 보여준다. 제일 좌측 그림에서 양 끝단의 두 노드가 동시에 트랜잭션을 제출하고, 이는 피어를 통한 브로드캐스팅으로 궁극적으로 제일 우측의 그림에서처럼 전체 노드에게 전달되는 과정을 보여준다.

이처럼 블록체인에서는 누구나 트랜잭션 요청서를 제출할 수 있고 그렇게 제출된 데이터는 모든 노드에게 전달된다. 그러나 이 많은 트랜잭션 중 무엇을 먼저 처리할 것인지 선택할 수 있는 권리는 오직 한 노드에게만 주어지는데, 그러한 권리를 가진 노드를 통상 리더(Leader)라 부른다.

1-2 리더의 선출

비트코인에서 리더를 선출하는 방식은 해시퍼즐이다. 즉, 해시퍼즐을 가장 먼저 해결한 노드가 리더로 선출되는 것이다. 이렇게 선출된 리더는 제출된 수많은 트랜잭션 중 먼저 처리할 것을 임의로 선택할 권리를 가지는데, 예외 없이 수수료를 더 많이 지불한 트랜잭션을 먼저 고르게 된다.

[트랜잭션 수수료] 이전 수수료

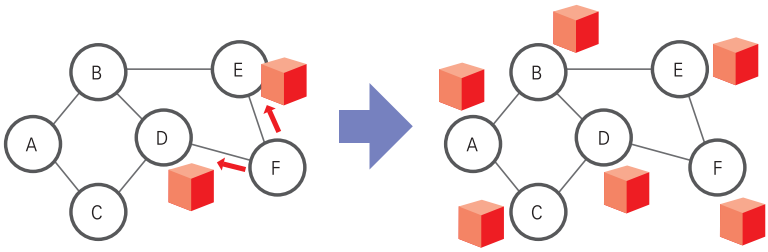
비트코인을 이전하려면 송신자가 채굴업자에게 수수료를 지불해야 한다. 수수료는 정해져 있지 않고 송신자 스스로 결정한다. 수수료가 높을수록 먼저 처리될 확률이 높아진다. 채굴업자들이 수수료가 높은 것을 먼저 처리할 것이기 때문이다. 이론적으로는 수수료가 낮은 트랜잭션은 영원히 처리되지 않을 수도 있다.

사용자들이 제출한 트랜잭션 중 현재의 리더가 선택한 것만이 이번 라운드에서 블록에 저장되고, 선택되지 못한 트랜잭션은 다음 라운드에서 새로운 리더가 다음 블록을 생성할 때 자신이 선택되기를 기다릴 수밖에 없다. 그렇다면 이때 트랜잭션을 선택하여 블록에 담는 리더의 정직성을 어떻게 믿을 수 있을까? 리더가 트랜잭션을 담으면서 그 내용을 조작한다거나 규칙에 맞지 않는 트랜잭션을 끼워 넣는다면 어떻게 될까? 바로 이 문제 때문에 '모두에 의한 검증' 절차가 필요하게 된다.

1-3 모두에 의한 검증

선출된 리더가 임의로 선택한 트랜잭션이 블록에 담기고 나면 그 내용을 모든 구성원에게 검증받아야 한다. 즉 리더가 트랜잭션을 조작한 것이 없는지 확인하는 절차이다. 이를 위해 다시 브로드캐스팅이 사용된다. 리더는 자신이 만든 블록을 브로드캐스팅을 통해 전체 노드에게로 전달한다. 새로 만들어진 블록을 전달받은 각 노드들은 블록 내의 트랜잭션에 이상이 없는지 확인한다.

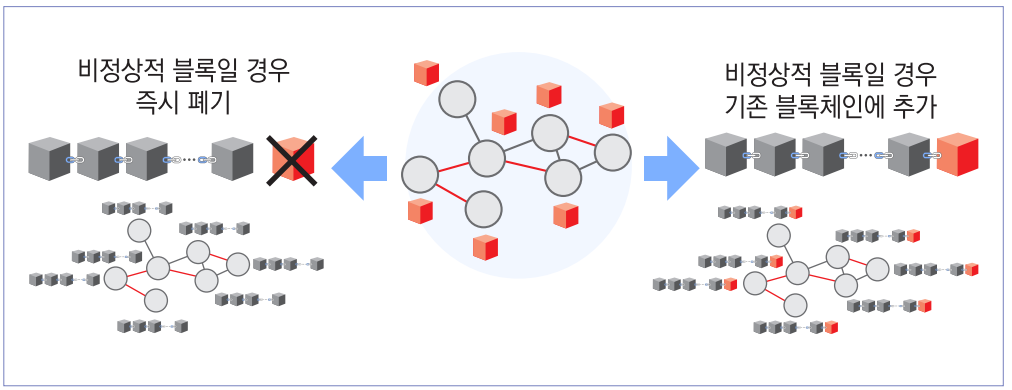
〈그림 Ⅷ-2〉 리더가 자신이 만든 블록을 브로드캐스팅하는 모습



〈그림 Ⅷ-2〉는 해시퍼즐을 가장 먼저 풀어 리더로 선출된 F가 자신이 만든 블록을 브로드캐스팅을 통해 전체 노드에게 전달하는 과정을 보여준다. 이렇게 전달된 블록의 무결성을 판단하는 것은 간단하다. 앞서 설명한대로 모든 트랜잭션은 전자서명되어 있으므로 트랜잭션을 변경하면 바로 발각된다. 따라서 블록의 검증이란 해시 값을 통해 전자서명의 무결성 여부를 확인하는 것이고 이를 통해 트랜잭션이 변경된 적이 없는지 알아보는 절차인 것이다.[122)]

122) 이 과정에는 해시퍼즐의 난스 값이 맞는지 확인하는 절차도 포함된다.

〈그림 Ⅷ-3〉 블록의 성장



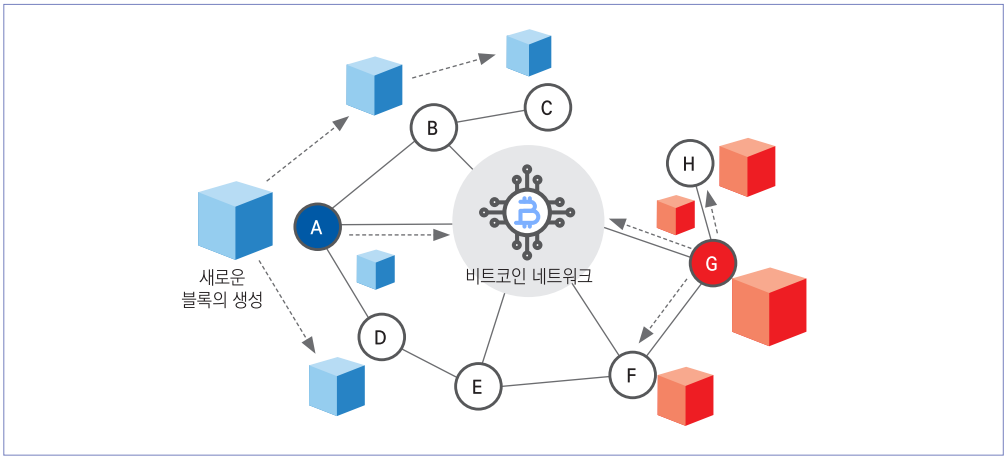
〈그림 Ⅷ-3〉은 검증을 거친 블록이 저장되거나 폐기되는 과정을 보여준다. 그림의 왼쪽은 해시 값을 통해 내용이 조작되었음을 확인한 경우 해당 블록을 즉시 폐기하는 상황을 보여준다. 그림의 오른쪽은 모든 검증과정을 통과한 경우로서 자신의 로컬 저장소에 이미 저장되어 있던 블록들 다음에 검증을 통과한 새로운 블록을 보관함으로써 블록체인의 길이가 하나 더 늘어나는 모습을 보여준다. 비트코인은 2009년 1월 3일부터 2020년 5월까지 10분에 한 번씩 약 63만여 번 이러한 과정을 거쳐 블록을 생성해 오고 있다. 또한 이렇게 생성된 블록은 검증에 참여한 모든 노드들의 로컬 저장소에 동일한 데이터로 보관된다.

2 탈중앙화 합의

2-1 블록의 동시 생성

앞서 리더 선출과정을 '가장 먼저' 해시퍼즐을 해결하는 것이라고 설명했는데 사실 이 설명은 기술적으로는 부정확하다. 블록체인은 비동기화 네트워크로서 그 전체 구성원이 누구인지 그리고 현재 상태가 어떠한지 알 수 있는 방법이 없다. 따라서 누가 먼저 해시퍼즐을 해결했는지도 알 수가 없다. 그러므로 다음 그림과 같은 상황이 빈번히 발생한다.

〈그림 Ⅷ-4〉 블록의 동시 생성



출처: 비트코인과 블록체인, 탐욕이 삼켜버린 기술, 이병욱, 2018, 에이콘 출판사, p. 98

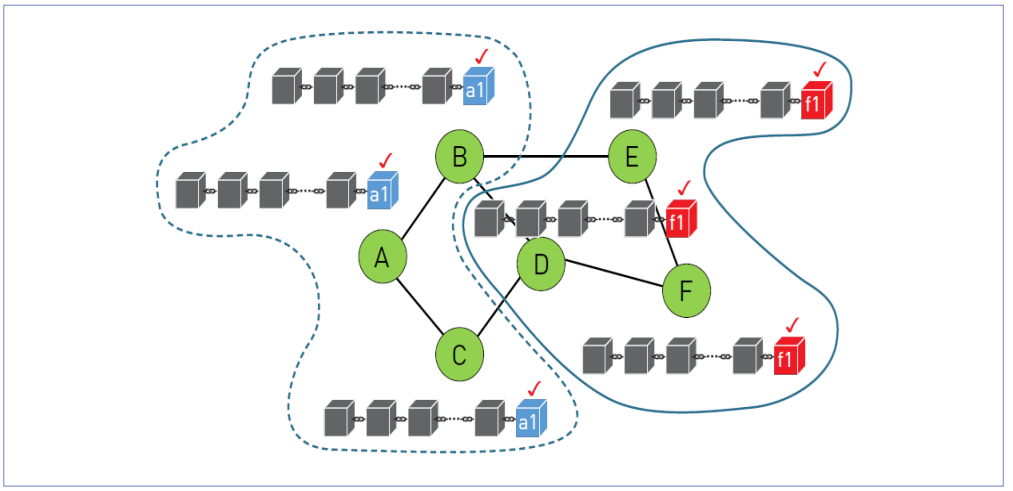
〈그림 Ⅷ-4〉는 노드 A와 노드 G가 (거의) 동시에 해시퍼즐을 해결한 상황을 보여준다. 이 시점에서 A와 G는 누가 해시퍼즐을 해결했는지 알 수도 없을뿐더러 서로의 존재조차 알지 못한다. 이때 A, G는 서로 자신이 가장 먼저 해시퍼즐을 해결했다고 믿고 '모두에 의한 검증'을 위해 브로드캐스팅을 통해 블록을 전달하게 된다. 그림의 B, D는 푸른색 블록을 전달받으며 G의 존재나 G가 블록을 만들었다는 사실을 알 길이 없으므로 단순히 방금 전달받은 푸른색 블록의 검증에 돌입한다. 마찬가지로 H와 F는 붉은 블록을 전달받아 검증에 돌입할 것이다. 이때 두 블록 모두 이상이 없다면 B, D는 자신의 로컬 저장소에 푸른 블록을 보관하며 블록체인이 자라게 될 것이지만 H와 F는 붉은 블록을 보관하며 블록체인이 자라게 되므로 같은 네트워크 내에 서로 다른 블록체인이 보관되는 결과가 초래된다.

2-2 블록의 충돌

〈그림 Ⅷ-5〉는 각기 서로 다른 블록을 저장함으로써 같은 네트워크에 다른 블록체인이 자라게 된 모습을 보여준다. 그림 좌측의 파란 점선 내의 노드들(A, B, C)은 파란 블록을 저장하고 우측의 파란 실선 내의 노드들(D, E, F)은 붉은 블록을 저장한 모습을 보여준다. 그러다 시간이 흐르면 어느 순간에 피어를 통해 각자가 서로 다른 블록체인을 저장하고

있다는 사실을 발견하게 된다. 동일한 네트워크에 두 개의 서로 다른 진실이 존재할 수는 없다. 그러므로 충돌된 것 중 어느 하나로 반드시 통일시켜야 하며 따라서 규칙이 필요하다.

〈그림 Ⅶ-5〉 서로 다른 블록의 생성



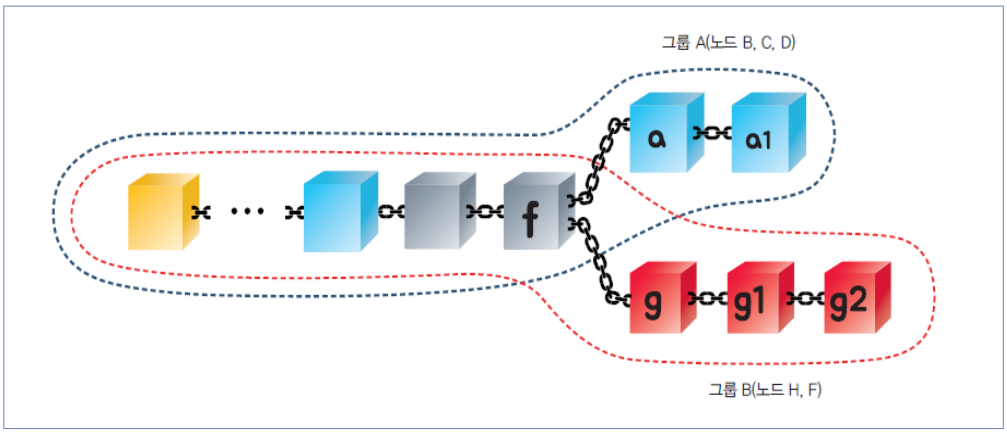
출처: 비트코인 해설서, 이병욱, 2019, 에이콘 출판사, p. 71

2-3 블록의 합의

서로 다른 블록체인이 충돌할 경우 이에 대한 합의 규칙은 다음과 같다.

1) 상대방의 블록체인이 규칙을 모두 지켰는지 확인한다. 만약 상대방의 블록체인이 규칙을 어겼다면 비교할 필요도 없이 승리한다.
2) 상대방의 블록체인이 모두 규칙을 지킨 경우라면, 서로의 길이를 비교한다.
2-1) 서로의 길이가 동일하다면 무승부가 되어 합의하지 않고, 계속해서 각자 더 긴 블록체인을 형성하려고 시합한다.
2-2) 서로의 길이가 다르다면 길이가 더 긴 쪽이 승리하게 된다. 이때 길이가 더 짧은 쪽은 양쪽 블록체인 중 상이한 부분의 블록은 모두 폐기처분해야 하며 길이가 더 긴 쪽의 블록들을 모두 복사해서 자신의 블록체인에 추가해야 한다. 이 과정을 거치면서 이제 네트워크의 모든 노드는 다시 동일한 블록체인을 가지게 된다.

〈그림 Ⅷ-6〉 서로 다른 블록체인의 충돌



출처: 비트코인과 블록체인, 탐욕이 삼켜버린 기술, 이병욱, 2018, 에이콘 출판사, p. 120

〈그림 Ⅷ-6〉은 어느 순간 어느 한쪽의 길이가 더 길어진 상황을 보여준다. 이 경우 그룹 B의 블록체인이 더 길기 때문에 그룹 A에 속한 노드들은 그룹 B와 상이한 부분인 블록 a와 a1을 폐기처분하고 g, g1, g2를 복제해 와서 서로 동일한 블록체인을 가지게 된다.

이처럼 어느 한순간에는 모든 노드의 블록체인이 서로 다를 수 있지만 시간이 지나면서 궁극적으로 같은 데이터를 가지도록 서로 맞춰나가는 과정을 탈중앙화 합의라고 한다.

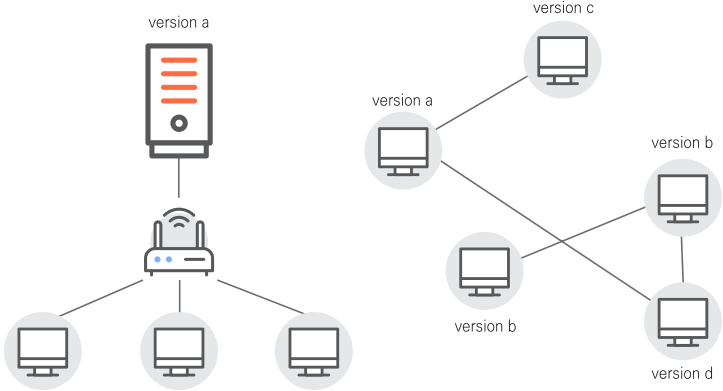
[길이 vs. 무게] 더 무거운 블록체인

더 긴 블록체인이 승리한다고 설명했지만 정확히 말하면 '더 많은 에너지를 소비한' 블록체인이 승리한다. 블록마다 생성 난이도가 다를 수 있으므로 난이도의 가중치를 고려하면 길이가 더 길어도 에너지 소비가 더 적을 수 있다. 이 때문에 가중치까지 고려해 더 '무거운' 블록체인이라는 표현을 쓰기도 한다. 그러나 대부분의 경우에 더 긴 블록체인이 더 무거운 블록체인과 일치한다. 또 실제 구현은 더 무거운 체인으로 돼 있지만 정작 비트코인의 원 논문에는 더 긴 블록체인이라고만 표현했다.

3 소프트 포크와 하드 포크

블록체인처럼 중앙 서버가 없는 경우에는 소프트웨어의 유지보수가 지극히 힘들며 일관성을 유지할 수 없는 단점이 생긴다. 이 때문에 발생하는 것이 바로 소프트 포크와 하드 포크이다.

〈그림 Ⅷ-7〉 블록체인과 중앙집중 시스템의 유지보수

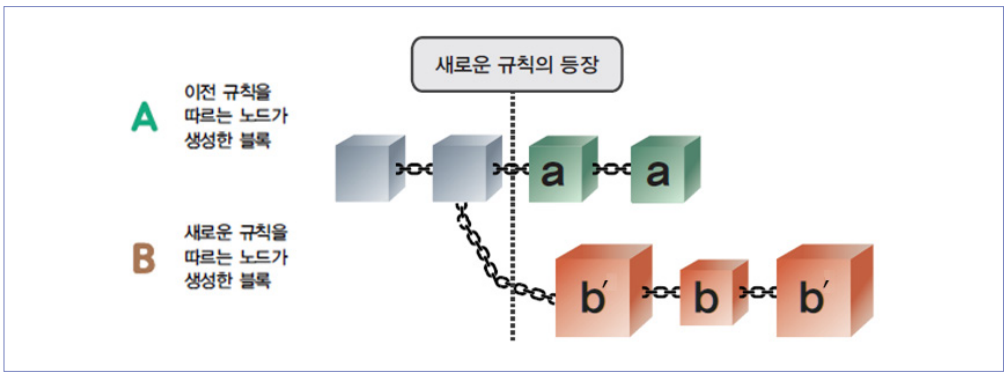


〈그림 Ⅷ-7〉은 일반적인 중앙집중 시스템과 블록체인의 시스템 유지보수상의 차이를 보여준다. 그림 왼편의 [(a) 중앙집중 시스템]에서는 모든 사용자가 동일한 서버에게서 서비스를 받는다. 따라서 전체 사용자는 현재 서버에 설치된 동일한 소프트웨어가 제공하는 서비스를 받으므로 시스템을 업그레이드하거나 오류를 수정하더라도 이 또한 모든 사용자에게 동일하게 적용된다. 그러나 그림의 (b)에서처럼 블록체인에 접속한 각 사용자는 각자가 다운로드받은 클라이언트 프로그램을 이용하여 접속하기 때문에 서로 다른 버전을 사용할 수 있다. 예를 들어 클라이언트 프로그램이 여러 번 업그레이드되거나 오류수정을 반영했다면 모든 사용자가 (부지런히) 새로운 버전으로 다시 다운로드하고 설치하지 않는 한 그 이전 버전의 소프트웨어를 사용한 접속자가 존재할 수 있다. 당연히 모든 사용자가 가장 최신의 소프트웨어만 사용하도록 강제할 수 있는 방법은 없다. 이제 이 때문에 생기는 두 가지 유형의 문제를 각각 살펴보도록 한다.

3-1 하드 포크(Hard Fork)[123]

이전에는 무효이던 규칙을 유효화하는 변화가 생긴 경우를 먼저 생각해 보자. 예를 들면 현재 비트코인의 블록은 1M 바이트까지만 유효하며 이를 넘긴 블록은 규칙을 어긴 것이므로 퇴출된다. 그런데, 어느 날 규칙을 변경하여 4M 바이트까지 블록을 허용하도록 프로그램을 수정한 경우를 가정해 보자. 이때 새로운 규칙을 적용한 버전의 프로그램을 사용하는 집단을 B라고 하고 그렇지 않고 이전의 버전을 그대로 사용하고 있는 집단을 A라고 가정해 보자.

〈그림 Ⅷ-8〉 하드 포크 상황



출처: 비트코인과 블록체인, 탐욕이 삼켜버린 기술, 이병욱, 2018, 에이콘 출판사, p. 133

〈그림 Ⅷ-8〉은 서로 다른 버전의 소프트웨어를 사용하는 두 집단의 블록체인이 충돌한 경우를 보여준다. B는 이제 4M 바이트까지 블록을 만들지만 A는 여전히 1M 바이트 이하의 블록만 유효한 것으로 인정한다. 이때 B의 블록체인의 길이가 A보다 더 길어진 경우를 생각해 보자. 탈중앙화 합의에 따르면 A는 더 긴 블록체인을 따라가야 하겠지만 여기서는 얘기가 다르다. A 입장에서는 B는 규칙을 어기고 1M 바이트를 초과하는 블록을 만들었기 때문이다. 따라서 B의 블록체인을 따라가지 않고 A 내에서 가장 긴 블록체인을 따라간다.

123) 포크는 그 갈라져 나온 모습을 빗대어 비유하는 용어이다. 전산학에서는 프로세스의 분기나 원 프로젝트에서 분기된 복제 프로젝트 등을 묘사하는 용어인데, 블록체인에서는 블록체인이 분기되어 갈라진 모습을 묘사한 용어이다.

한편 B는 A나 B 모두의 블록체인을 유효한 것으로 인정하지만 자신의 집단에서 만든 블록체인이 더 길어졌기 때문에 자신의 집단에 있는 블록체인을 따라간다. 이 경우 두 집단은 탈중앙화 합의를 이루지 못하고 영원히 서로 다른 블록체인을 쫓아가게 된다. 두 집단이 합의를 이룰 수 있는 방법은 A 집단의 길이가 더 길어지거나 A의 모든 구성원이 새로운 버전으로 업그레이드해야 하는 것인데, 그렇지 않은 경우 영원히 갈라진 채로 서로 다른 블록체인이 자라게 된다. 비트코인 캐시와 비트코인 골드는 이런 하드 포크 과정을 거쳐 갈라져 나온 새로운 가상자산이며 이더리움도 이더리움과 이더리움 클래식으로 갈라져 나왔고 여러 번 하드 포크를 통해서 소프트웨어를 변경해 오고 있다.

3-2 소프트 포크(Soft Fork)

소프트 포크는 하드 포크와 반대의 경우다. 즉 예전에는 유효하던 규칙을 갑자기 무효화하는 경우이다. 예컨대 예전에 사용하던 규칙에서 심각한 보안상의 결함을 발견하게 된다면 그 규칙을 무효화하는 것이 합리적일 것이다. 이번에도 새로운 규칙을 적용해 업그레이드한 버전을 사용하는 집단을 B라고 하고 그렇지 않고 이전 버전을 그대로 사용하는 집단을 A라고 하자.

이때 만약 B가 만든 블록체인의 길이가 A보다 더 길어졌다고 가정해 보자. 앞서 A는 B가 규칙을 어겼기 때문에 더 길지만 따라가지 않았다. 그러나 지금은 그렇지 않다. A의 입장에서는 B가 만든 모든 블록이 유효하다. B의 규칙집합은 이제 A의 부분집합이기 때문이다. 따라서 A는 길이가 더 긴 B를 따라 탈중앙화 합의를 이루게 된다. 이렇듯 A가 새로운 버전으로 업그레이드 하지 않아도 새로운 버전의 사용자들이 더 긴 블록체인을 만들면 강제로 합의를 이루게 되는 경우를 소프트 포크라고 한다.

3-3 포크와 블록체인의 유지보수

포크(Fork)는 블록체인의 유지보수가 얼마나 힘든 지를 단적으로 보여주는 예이다. 블록체인에서는 중앙화 시스템에서와 같은 일목요연하고 잘 계획된 관리는 원천적으로 불가능하다. 이 때문에 블록체인은 매우 단순하며 반복적인 작업 이외의 용도로 확장하는 것이 쉽지 않다. 비트코인이나 이더리움이 고작 가상자산을 주고받는 용도 이외에 별다른 효용을 보여주지 못하는 것도 비슷한 맥락이다. 여러 가지 사유와 관점에서 비트코인 블록체인에는 많은 변형이 가해졌는데 이러한 변종들에 대해서는 제3절에서 다시 살펴보기로 한다.

제2절

블록체인의 정의

1 블록과 체인

지금까지 블록체인에 대해서 줄곧 설명해 왔으나 정작 블록체인이 정확히 무엇인지 그 정체에 대한 정의를 언급한 적은 없었다. 놀랍게도 블록체인에 대한 정의는 그 어디에도 없다. 심지어 사토시 나카모토의 원 논문에는 블록체인이라는 용어가 단 한 차례도 언급조차 되지 않는다. 원 논문에는 앞서 설명한 한꺼번에 처리하는 데이터 단위인 '블록'과 이들이 논리적으로 사슬처럼 묶여 있는 것을 묘사한 '체인'이라는 일반 명사만 개별적으로 등장한다. 블록체인의 정의가 없다는 사실은 대단히 중요한데, 이 때문에 어떤 시스템이 '블록체인으로 구성'되었다는 말에는 정작 아무런 정보도 들어있지 않는 셈이다. 원 논문을 충실히 해석한 정의도 있지만 그와 정반대의 속성을 가졌으면서도 블록체인이라 주장하는 일도 흔하다. 예를 들어, 비트코인은 '익명'의 '불특정 다수'가 '어떠한 통제도 없이' 운영되는 '탈중앙화' 시스템이지만 IBM의 하이퍼레저 패브릭은 '실명'의 '인가받은 소수'가 '특정 서버의 통제에 따라' 운영되는 '중앙통제' 시스템이다.

블록체인에 대한 정반대의 대립된 견해 즉, 무용론과 예찬론이 오랫동안 지속되고 있음에도 불구하고 그 결론이 모호한 원인도 바로 정의(定義)의 부재 때문이다. 정반대의 목적물이 동일한 명칭을 사용하게 되면 그 명칭이 가진 분류의 역할은 사라질 수밖에 없다. 그러므로 범위와 정체성을 특정할 수 없는 대상에 대한 결론이 가능할리 없고, 사실을 호도하더라도 이를 적시하기가 불가능해 진다. 그러나 분명한 것은 비트코인은 틀림없이 블록체인이라는 점과 블록체인의 효용을 둘러싼 모든 예찬들, 예컨대 '기록의 비가역성', '제3자 배제', '탈중앙화' 등은 모두 비트코인류에만 적용될 뿐 이를 크게 변형한 다른 시스템에는 해당되지 않는다는 사실이다. 따라서 블록체인의 정의가 비트코인에 충실해야 함은 자명하다. 이제 블록체인의 실체에 대해 보다 명확히 정의를 내려 보자. 사물에 대해 명확히 정의하지도 않은 채 논의한다는 것은 그 자체로도 모순이며 혼란만 가중시킬 것이기 때문이다.

2 블록체인의 정의

블록체인은 '자발적으로 구성된 익명의 네트워크'를 의미하며 그중 다음의 네 가지 성질을 모두 만족하도록 설계된 것만을 의미한다. 그러나 기술적 한계로 인해 이 네 가지를 완전히 만족하지 않더라도, 속성상 이를 모두 만족시키기 위해 설계되었거나 이 모두를 강화하는 방향으로 지속적인 개선을 해 나가는 경우까지 포함한다.

1) 각 노드는 자의로 네트워크 구성원으로 참여하거나 탈퇴할 수 있어야 하고 이를 통제하는 어떠한 서버도 없어야 한다. 따라서 구성은 동적이며 어떠한 제약도 없어야 한다.
2) 모든 노드는 동일한 권리와 의무, 정보를 가져야 하며, 어느 한 노드도 더 많은 권한이나 의무, 정보를 가져서는 안 된다.
3) 각 노드는 원할 경우, 항상 기록 및 검증에 참여할 수 있는 권리가 보장되어야 한다.
4) 기록의 불변성은 첫째, 기록자 선정의 무작위성과 둘째, '기록 변경 자체의 어려움'이라는 속성을 모두 갖춘 방식으로 구현돼야 한다.

이제, 이 네 가지 속성이 각각 어떤 의미를 가지는지 살펴보자.

1)번 속성은 자발적인 형성을 강조하는데, 이 속성이 깨진다면, '누군가' 참여와 탈퇴에 관여한다는 의미가 되고 그 누군가는 통제의 권한과 정보를 가지므로 '익명의 자발적 노드'라는 기본전제가 무너진다.[124)]

2)번은 '내부자에 의한 시스템 남용'을 방지하는 역할을 한다. 현재의 강력한 보안 시스템은, 외부의 해킹은 비교적 효과적으로 방어하지만, 내부자의 침입에는 여전히 취약하다. 권한을 가진 누군가의 강압이나, 운영자 권한을 가진 자가 자신의 이익을 위해 시스템을 남용할 가능성은 여전히 남아 있다. 어느 특정 노드가 더 많은 권한이나 정보를 가질 수 없도록 하면 어떠한 내부자 위협도 발생하지 않게 할 수 있다. 블록체인은 내 · 외부인의 구분 자체가

124) 이런 관점에서는 프라이빗이나 컨소시엄 블록체인이라 불리는 허가형 블록체인은 여기서의 블록체인의 정의에 포함되지 않는다.

무의미하기 때문이다. 모두가 내부자이자 외부자이다. 따라서 이 조건이 깨어지면 내부인에 의한 위협이 되살아난다.

3)은 기록자체에 대한 신뢰를 위한 요소이다. 모든 노드는 원할 경우 기록할 권리를 얻기 위한 과정에 참여할 수 있어야 하고, 타인이 기록한 내용의 진위를 검증하는 과정에 참여할 수 있어야 한다. 기록할 권리나 기록의 진위를 검증할 권리를 소수의 노드가 독점하면 2)의 가정이 무너진다.

4)의 성질은 3)에 더해 기록의 '비가역성'을 추구한다.

현재 시중에는 블록체인의 명칭이 너무나 광범위하게 사용되고 있다. 여기서 블록체인을 분명히 정의하는 이유는 기존의 분류체계로 잘 설명할 수 있는 시스템까지 블록체인에 포함되는 것을 막고 이들을 분리하기 위해서이다. 이를 통해 블록체인이라는 '새로운' 접근 방법을 보다 정확히 평가할 수 있을 것이다. 목적물의 정체와 범위도 규정하지 않은 채 그 효용을 논하는 것은 무의미하기 때문이다.

[이론과 실제] 진정한 블록체인

사실 이 정의에 가까운 블록체인은 겨우 비트코인과 이더리움 정도뿐이며 나머지는 모두 위배된다. 심지어 엄밀한 관점에서는 비트코인과 이더리움도 이 정의에 정확히 부합하지 않는다. 결국 지금껏 예찬해 온 속성을 모두 가진 '진정한 블록체인'은 단 한 번도 완전히 구현된 적이 없었던 '상상 속의 존재'인 셈이다.

제3절

블록체인의 변형

1 이더리움과 스마트 컨트랙트

컴퓨터는 범용 기계(General Purpose Machine)라고 불린다. 용도가 정해진 일반 기계, 예컨대 전자계산기는 계산기 이외의 기능은 수행할 수 없다. 그러나 컴퓨터에는 '메모리'가 존재해서 그곳에 '프로그램'이 저장된다. 그리고 이 프로그램만 바꾸면 컴퓨터의 역할은 무한대로 늘어난다. '워드' 프로그램을 저장하면 '문서 편집기' 역할을 하고 '그림판'을 저장하면 '스케치북 도구'가 되며 '게임'을 저장해 두면 '게임기'로 변신한다.

블록체인도 이와 유사하게 변형되었다. 비트코인의 블록에는 정적인 '거래 내역'만 저장된다. 따라서 그 이외의 용도로는 쓸 수 없다. 앞서 전자계산기처럼 용도를 변경할 수 없는 경우에 비유할 수 있다. 이더리움[125]은 블록 공간에 정적인 기록은 물론 임의의 프로그램 코드도 저장할 수 있도록 설계를 변경했다. 이때부터 블록체인의 용도를 다양화할 수 있게 되었다. 서로 이더리움을 주고받는 정적인 기록은 물론, 다양한 프로그램을 블록에 저장한 뒤 호출함으로써 새로운 기능을 쉽게 '정의'할 수 있게 된 것이다. 이런 관점에서 이더리움을 범용 블록체인(General Purpose Blockchain)이라 주장하기도 한다.[126] 이더리움은 이 기능에 '스마트 컨트랙트(Smart Contract)라는 이름을 붙였다. 스마트 컨트랙트는 디앱/댑(DApp; Decentralized Application)으로도 명명한다.

125) 이더리움은 비탈릭부테린이라는 러시아 개발자가 만든 코인 이름이다.

126) 사실 이 변경은 혁신적인 것은 아니다. 이 방식은 소프트웨어를 제작할 때의 통상적인 상식이다. 비트코인도 이러한 확장성을 고려한 흔적이 그대로 남아 있다. 다만, (시간 혹은 인적 자원 문제로 추정되는) 어떤 제약에 의해 편의상, 범용이 아닌 고정된 기능 하나만으로 구현한 것이다.

1-1 스마트 컨트랙트

스마트 컨트랙트(Smart Contract)라는 용어는 원래 1990년대 닉 사보(Nick Szabo)가 만들었다. 전산학을 공부하고 동시에 법률과 경제학도 공부한 것으로 알려진 그는 디지털 환경을 잘 꾸미면 '변호사 등의 제3자가 개입하지 않아도' 법적 효력을 가진 계약을 자동으로 '집행'할 수 있을 것이라 생각하고 이러한 가상의 프로토콜을 스마트 컨트랙트라 불렀다. 그러나 그의 '구상'은 단 한 번도 온전히 구현된 적은 없다. 이더리움의 스마트 컨트랙트는 명칭만 같을 뿐, 닉 사보의 구상과는 거리가 멀다. 닉의 구상의 핵심은 법률행위가 스스로 집행되는 '프로토콜'이지만, 이더리움은 그저 단순한 컴퓨터 프로그램을 '실행'하는 플랫폼에 불과하다. 사실 닉의 구상이 실현 가능한 것인지 차제에도 의문이 제기되고 있으며, 그 가능성에 대한 논의는 차치하더라도 중요한 것은 닉의 구상과 이더리움의 스마트 컨트랙트는 명칭만 같을 뿐 기능은 별 관련이 없다는 점이다.

[닉 사보의 트위터] 닉 사보의 블록체인 진단

닉 사보는 2019년 10월 15일 자신의 트위터를 통해 다음과 같이 블록체인을 평가했다.
"블록체인은 중앙화되었고, 스스로 신뢰를 무너뜨리고 있다는 것을 부정할 수가 없다. 모든 블록체인은 결함이 있고 특히 이더리움은 금융에 부적합하며, 단순 토큰 이상으로 사용하기에는 심각한 위험이 있다."

1-2 유용한 디앱

이더리움이 등장하고 5년이 흘렀지만 그동안 개발된 DApp이라곤 토큰[127]을 만들거나, 단순한 게임 정도가 거의 전부인 실정이다. 법률 집행은 고사하고 의미 있는 DApp도 찾아보기 힘든데, 이러한 현상은 다음과 같은 이유에서 기인한다.

1) 블록체인의 모든 정보는 노출된다. 의미 있는 계약을 위해서는 개인정보를 포함한 민감한

127) 토큰은 제8장 제1절에서 자세히 설명한다.

데이터를 다룰 필요가 있는데, 이러한 데이터는 노출로 인해 원천적으로 사용할 수가 없다.

2) 닉 사보의 스마트 컨트랙트의 핵심은 프로그램을 구동하는 플랫폼이 아니라 법률행위를 프로그램으로 표현하는 것이 가능할 것인가에 있다. 이더리움의 DApp 방식으로 스마트 컨트랙트를 구현하려면 먼저 복잡한 법률 행위를 스크립트 코드로 표현해야 하는데 그 자체가 하나의 새로운 과제이며, 또 그 코드를 보고 해당 법조문을 이해한다는 것은 전산 전문가도 사실상 불가능한 일이다.

3) DApp으로 프로그램을 구현하고 실행하는 것은 통상적인 방식에 비해 훨씬 더 많은 비용이 소모된다. DApp의 핵심이 비용절감인데, 더 많은 비용이 들고, 더 복잡하고 더 느리며 더 관리가 힘든 방식이라면 굳이 사용할 이유가 적다.

4) 블록체인은 제3자가 배제된 거래를 구현할 수 없다. 블록체인은 제3자의 중계가 반드시 필요한 시스템이다.

2 하이퍼레저 패브릭

2015년 12월 리눅스(Linux) 재단은 하이퍼레저(Hyper ledger)라는 이름의 엄브렐러 프로젝트를 출범했다. 이 프로젝트가 표방한 목적은 오픈소스 블록체인을 만드는 것이었고 IBM, 인텔, SAP 등이 주요 스폰서였다. 하이퍼레저는 블록체인 무용론 속에서 상업적으로 활용 가능한 블록체인을 개발한다는 목표 아래 출범했다. 하이퍼레저가 던진 가장 원론적인 질문은 "왜 굳이 익명이어야 하는가?"였고 이에 따라 그 기본 아키텍처는 누구나 참여하는 개방된 네트워크가 아니라 오로지 인증을 통해 사전에 허가받은 노드만 참여할 수 있는 형태로서 비트코인과는 완전히 정반대의 형태를 취하게 된다.

2-1 하이퍼레저 패브릭

하이퍼레저라는 이름의 엄브렐러 프로젝트에서는 10여 개 이상의 개별 프로젝트가 진행되었고 그중 IBM이 주축이 된 하이퍼레저 패브릭이라는 이름의 플랫폼 구축 프로젝트가 지금까지 가장 많은 주목을 받고 있다. 하이퍼레저 패브릭(이하, 패브릭)은 기존의 비트코인과 이더리움과는 완전히 다른 형태로 설계되었다. 〈표 Ⅲ-1〉에서 알 수 있듯 패브릭은 비트코인과 그저 다르다고 설명하는 것보다 정반대라고 설명하는 것이 더 정확할 정도로 유사한 점이라고는 찾아보기 힘들다.

〈표 Ⅶ-1〉 비트코인과 하이퍼레저 패브릭의 비교

	비트코인/이더리움	하이퍼레저 패브릭
노드의 정체	익명	실명
연결 형태	P2P	중앙 집중식
참여 자격	누구나	인증 필요
중앙 서버	없음	있음
주목적	가상자산	일반 프로그램

앞서 하이퍼레저가 던진 "왜 굳이 익명이어야 하는가?"라는 질문은 다른 측면에서 보면 "그게 아니라면 왜 블록체인인가?"로 바꾸어 생각해 볼 수도 있다. 패브릭은 여러 측면에서 기존에 블록체인이라 불리던 것과는 상당히 다른 속성을 가지고 있다.

3 퍼블릭과 프라이빗 블록체인

3-1 프라이빗과 컨소시엄 블록체인

하이퍼레저의 등장과 함께 프라이빗 블록체인이라는 용어가 등장했다. 이는 스스로를 비트코인과 구분하기 위해 만든 명칭으로, 전통적인 블록체인은 퍼블릭 블록체인이라 부르고 하이퍼레저는 프라이빗 또는 컨소시엄 블록체인이라 부르기 시작했다.

현재 프라이빗 블록체인이라는 용어는 사전에 인가된 노드들로만 구성된 블록체인 네트워크를 지칭하는 용어로 사용되고 있다. 또 그 네트워크의 구성체가 단일 회사로만 이루어진 경우와 복수의 회사가 모여 이루어진 경우를 구분해서 각각 프라이빗 블록체인과 컨소시엄 블록체인이라는 용어를 사용한다. 이러한 형태의 구체적 사례는 제9장 제3절에서 K생명의 소액 보험금 지급 시스템과 15개 은행 연합체의 공동 인증 시스템인 뱅크사인을 통해 다시 살펴보기로 한다.

3-2 프라이빗과 컨소시엄 블록체인의 용도

프라이빗과 컨소시엄 블록체인이 과연 기존의 시스템과 다른 어떠한 효용이 있는지에 대해서는 아직 좀 더 지켜봐야 할 것 같다. 그 구성 아키텍처만 놓고 보면 특히 프라이빗 블록체인은 일반적인 중앙집중 시스템과 구분하기 힘들 정도다.

한편, 컨소시엄 블록체인의 경우에는 복수의 여러 회사가 서로 협업한다는 모델이라는 점에서 여러 가지 새로운 시도가 가능할 수 있다. 특히 서로 고립된 생태계로 성장해 온 금융계의 경우에는 각 회사 간의 협업이라는 생소한 세계로의 여러 가능성을 실험해 볼 수 있을 것이다. 그러나 협업을 위한 아키텍처는 매우 다양하다는 점과 패브릭은 협업 중에서도 주로 반복 검증의 기능에만 집중된다는 점을 고려해 보면 협업을 위한 여러 인프라 후보 중 하나로서의 패브릭은 향후 여러 가지 측면에서 그 효용을 검증받아야 할 것이다. 분명한 것은 명칭보다 중요한 것은 실제 효용이라는 것이다. 마케팅 용어에 매몰되어 주객이 전도되어서는 안 될 것이다.

3-3 하이퍼레저 패브릭의 기본 작동 방식

패브릭은 PKI 구조를 따라 인증 서비스를 제공하는 서버인 MSP(Membership Service Provider)에서 인증된 노드들로만 구성되며, 속성에 따라 채널(Channel)이라 불리는 서로 다른 인증 그룹이라고 정의할 수 있다. 통상 같은 채널은 서로 데이터를 공유하지만 채널이 다르면 접근할 수 있는 정보가 달라진다.

패브릭은 스마트 컨트랙트라는 용어 대신 체인코드(Chain Code)라는 용어를 사용하는데, 피어(Peer)라 불리는 서버에 의해 중복 실행을 통해 결과를 검증하고 오더러(Orderer)라 불리는 서버에 의해 결과를 최종 확인받은 뒤, 오더러가 각 피어에게 저장허가를 내리면 각 피어가 블록에 저장하는 방식을 취한다. 피어와 오더러는 내부 조직에 의해 통제되는 서버들이고, 컨소시엄의 경우 다수의 회사가 피어와 오더러를 같이 구성할 수 있다.

패브릭은 피어가 중복해서 실행 결과를 확인하는 점, 암호화 해시를 사용하여 저장 데이터의 무결성을 검증하는 점 등이 비트코인의 작동방식과 닮아 있지만, 중앙에서 통제되는 서버에 의해 작동된다. 따라서 비트코인 블록체인의 가장 큰 속성 중 하나인 '서비스 거부 공격'으로부터의 안전성은 존재하지 않는다. 특히 오더러만 해킹당하면 시스템은 제대로 작동할 수 없다.

제4절

블록체인의 효용

이 절에서는 그동안 잘못 알려져 있던 블록체인의 효용에 대해 몇 가지 살펴본다. 그중 가장 보편적으로 잘못 알려져 있던 수수료에 관련한 부분부터 살펴보기로 한다.

1 왜곡된 수수료 – 중개와 중계

블록체인이 초기에 주목받은 이유 중 하나는 '제3자가 배제'된 거래를 통해 불필요한 수수료를 절약할 수 있는 유통혁신과 관련된 것이었다. 그러나 블록체인을 사용해 불필요한 수수료를 낮출 수 있다는 것은 사실과 다르다. 블록체인은 결코 제3자를 배제할 수 없기 때문이다.

1-1 중개와 중계

거래에 있어 제3자의 역할은 크게 중재 또는 중개(仲裁, Mediation)와 중계(中繼, Relay)로 나눌 수 있다. 중재 또는 중개는 제3자가 적극적으로 개입하는 형태를 의미하며 중계는 수동적 가교역할을 의미한다. 블록체인에서 제3자가 필요 없다는 주장은 잘못된 것이다. 블록체인은 각 노드가 제3자로서 중계역할을 해 줘야만 시스템이 작동될 수 있다. 문제는 블록체인의 중계에는 천문학적 비용이 소모된다는 것과 대부분의 금융수수료는 중재가 아니라 중계에서 발생한다는 것이다. 우리가 은행에서 계좌이체를 할 때 은행과 금융결제원의 역할은 중재가 아니라 중계이다. 앞서 설명한대로 블록체인은 중복에 의한 시스템이며 동시에 신뢰받는 제3자를 없애기 위해 작업증명이라는 비효율을 사용하고 있다. 따라서 중계비용은 항상 더 올라갈 수밖에 없다. 항상 더 많은 에너지를 사용하기 때문이다.

1-2 불필요한 중재

그렇다면 중재는 어떨까? 불필요한 중재를 없앰으로써 비용을 더 낮출 수 있지 않을까? 여기서의 함정은 '불필요한'이란 단어이다. 불필요한 중재라면 그냥 없애면 된다. 네트워크 아키텍처와 상관없다. 블록체인은 중재를 없앤 것이 아니라 중재가 불가능한 아키텍처이다. 필요하든 않든 구현할 수가 없다. 이 때문에 꼭 필요한 중재기능인 자금세탁방지 등도 구현이 불가능하다.

제3자의 중재기능은 대부분 소비자의 필요에 의해서 존재한다. 그 때문에 우리는 경우에 따라 자발적으로 수수료를 지불하면서도 그 서비스를 이용하기도 한다. 특히 금융에는 꼭 필요한 중재가 많다. 계좌번호 입력 오류로 송금을 잘못한 경우, 계좌 비밀번호를 분실한 경우, 보이스 피싱 등 범죄로부터 추가피해를 방지해야 할 경우, 신용카드의 도난 등 금융기관의 적극적 개입이 꼭 필요한 중재가 수도 없이 많다. 블록체인은 이런 중재가 불가능하다. 암호화 키를 잃어버리거나 비트코인을 잘못된 주소로 보내면 그것으로 끝이다. 다시는 회복할 수 없다.

[필요한 중재의 빈자리] 분실된 비트코인

포춘(Fortune) 잡지는 암호화 키 분실로 인해 영원히 사용할 수 없는 비트코인이 2017년 11말 기준으로 약 380만 개로 추정된다는 기사를 실었다[128]. 이는 당시 시세인 2,500만원으로 환산하면 무려 95조원에 이르고 그 시점 총 비트코인 총 수량의 23%에 이르는 엄청난 양이다!

결론적으로 블록체인은 항상 더 많은 에너지를 사용한다. 수수료를 낮추려면 불필요한 중재를 없애고 중계비용을 최소화해야 하는데 그 용도에는 오히려 중앙화 시스템이 더 유리하다. 무엇보다도 비트코인 블록체인을 만든 목적은 수수료의 절감이 아니라 프라이버시의 보호이다.

128) FORTUNE. https://fortune.com/2017/11/25/lost-bitcoins/ (최종 접속: 2020.03.25.)

[수수료의 진실] 소액거래의 역설

비트코인 원 논문에는 '금융기관의 중재(Mediation)가 수수료를 증가시켜 특히 소액거래를 방해한다.'는 사토시 나카모토의 주장이 들어 있다. 이 문구가 블록체인이 수수료를 낮출 수 있는 근거처럼 인용되는데 이 주장에는 두 가지 모순이 있다.
첫째, 앞서 설명한 것처럼 금융수수료는 대부분 중계와 관련되며 블록체인의 중계에는 막대한 에너지가 소모된다.
둘째, 비트코인의 수수료는 송금액이 아닌 트랜잭션의 크기를 바이트로 측정한 것에 비례한다. 즉 1,000억을 송금하든 1원을 송금하든 수수료가 같다. 이 때문에 소액거래에 절대적으로 불리하다.

소액거래를 방해한다고 기존 금융을 성토하던 사토시 나카모토의 주장과 반대로 비트코인 수수료 체계가 오히려 소액 거래를 크게 방해하고 있는 모순을 안고 있는 셈이다.

2 블록체인과 데이터베이스

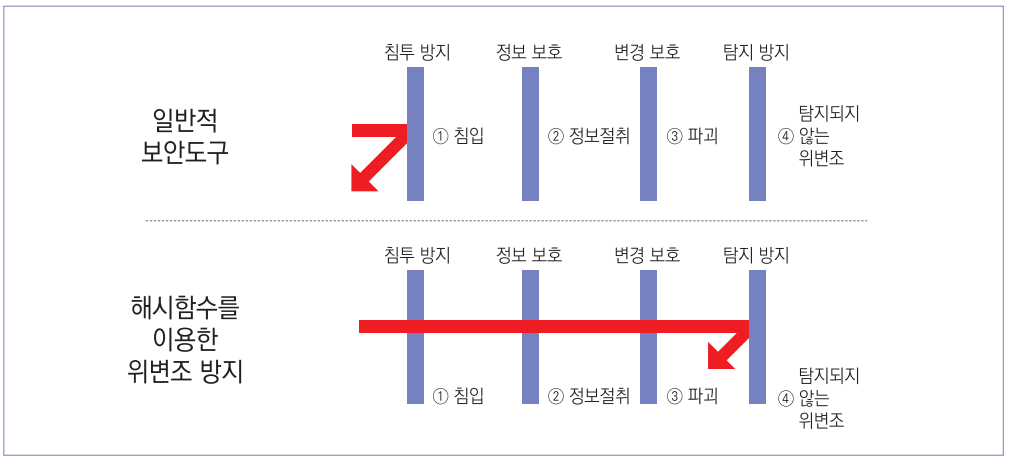
블록체인을 일반적인 저장장치로 사용하려는 것은 블록체인의 용도를 오인하고 있는 것이다. 블록체인에 데이터를 저장하는 비용이 막대한 것은 차치하더라도 데이터의 추출, 수정, 검색, 보안 등 모든 면에서 가장 좋지 않은 선택이 된다. 데이터를 블록체인에 보관해야 할 아무런 이점이 없다.

일각에서는 투명하고 안전한 저장장치라는 잘못된 주장도 하지만 블록체인에 저장된 데이터는 투명하고 안전한 것이 아니라 모두 노출되어 보호가 되지 않는다.

3 블록체인과 보안

블록체인이 보안장치로 오해받는 것은 암호화 해시라는 특정 속성이 과장된 측면이 강하다. 다음 그림을 보자.

〈그림 Ⅷ-9〉 시스템 침입 단계



출처: 블록체인 해설서, 이병욱, 2019, 에이콘 출판사, p. 252

〈그림 Ⅷ-9〉는 일반적인 해킹의 단계를 보여준다. 첫 단계는 허가받지 않은 침입이며, 그 다음 단계는 침입자가 '읽기' 허가를 획득해 정보를 탈취하는 것이다. 그 다음은 '쓰기' 허가까지 획득하여 시스템 내용을 변경하는 것이다. 그리고 마지막 단계는 내용을 변경시키고도 이를 들키지 않기 위해 위변조 방지 해시 값까지 다시 계산하는 것이다. 그림에서 보는 것처럼 해시는 이미 변경이 일어난 뒤 사후적인 탐지 기능이다. 보안도구라 함은 사후적인 탐지 기능만을 의미하는 것이 아니라 시스템의 침입 단계부터 전 단계에 걸친 보안 기능을 의미한다. 결국 사후적 탐지 기능인 해시함수를 사용한다는 이유로 블록체인을 보안도구로 분류하려는 것은 하나의 속성을 과장하여 일반화한 오류에 가깝다. 블록체인은 보안도구라기보다는 보안에 사용되는 보편적 기술인 암호화 해시를 활용하는 여러 이용자 중 하나라고 설명하는 것이 더 타당하다.

4 탈중앙화의 민낯 - The DAO 사건

DAO는 Decentralized Autonomous Organization의 약자로 우리말로 하면 '탈중앙화 자율 기구' 정도로 번역할 수 있다. DAO는 블록체인 커뮤니티를 중심으로 독립되고 투명을 상징하는 용어인 것처럼 퍼져 나갔다. 이더리움 재단은 블록체인이야 말로 DAO를 실현할 수 있는 최적의 플랫폼이라는 점을 보여주고자 'The DAO'라는 이름의 단체를 조직하여 재미있는 실험을 감행한다.

4-1 The DAO - 사람이 개입되지 않는 투자 프로젝트

The DAO의 실험은 다음과 같은 클라우드 펀딩 프로젝트였다.

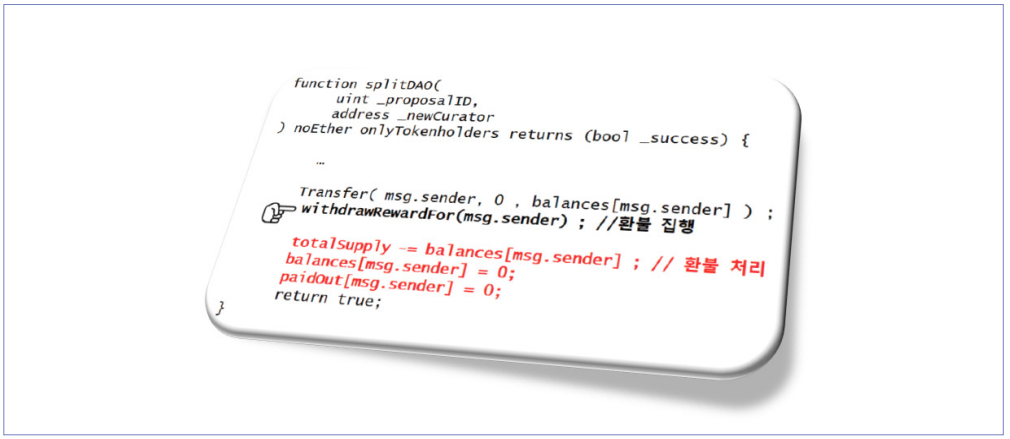
1) 클라우드 펀딩방식으로 이더리움을 펀딩받는다.
2) 펀딩받은 이더리움을 스타트업 회사에 투자한다.
3) 투자 수익금은 투자자에게 배분한다.
4) 이 전체 과정은 오로지 스마트 컨트랙트로만 진행하고 이사회 등을 포함한 사람이 개입되는 모든 절차를 배제한다.

이 프로젝트와 기존의 클라우드 펀딩과의 핵심 차별점은 사람이 전혀 개입되지 않은 상태에서 오로지 스마트 컨트랙트로만 진행한다는 4)번 조항이었으며, The DAO는 이를 위해 자신들이 작성한 프로그램 소스를 모두 공개하였다.

4-2 결정적 버그

그러나 자신 있게 공개한 프로그램에는 결정적 버그가 하나 숨어 있었다. 바로 환불과 관련된 부분이었다. 다음 그림을 보자.

〈그림 Ⅶ-10〉 The DAO 스마트 컨트랙트의 버그



〈그림 Ⅶ-10〉은 The DAO가 실제 사용했던 스크립트의 버그를 보여준다. 프로젝트는 모금 기간 내에 환불해 주었는데, The DAO는 환불요청이 들어오면 환불을 먼저 해 주고 나서 환불 완료 플래그를 설정하도록 프로그래밍을 작성했다. 일반 시스템에서는 아무 문제도 되지 않는 이 처리 순서가 느린 블록체인에서는 큰 문제가 되었다.

느린 블록체인의 특성상 환불 완료 플래그를 설정하기도 전에 또 다시 환불 요청이 오면 환불이 중복돼 집행될 수 있었던 것인데, 이를 간파한 해커는 2016년 6월 18일 실제로 중복 환불 요청에 의한 공격을 감행하여 전체 모금액의 28%에 이르는 360만 이더를 편취했다. 이더리움 최고 시세 대비로는 5조 6,000억원에 이르는 거액이며 모금 당시 시세로는 600억원에 이르는 금액이었다.[129]

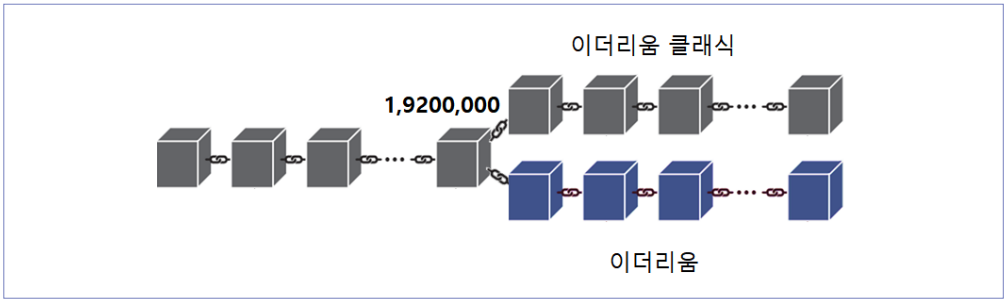
4-3 이해의 상충

이 해킹 사건에 대한 The DAO 내부의 의견은 두 가지로 나뉘었다. 비탈릭 부테린이 중심이 된 그룹은 하드 포크를 통해 기록을 변경하여 잃어버린 이더리움을 되찾자고 주장한 반면,

129) 위키피디아, http://en.wikipedia.org/wiki/The_DAO_(organization)

반대파는 블록체인의 정신은 비가역적 기록이므로 절대 하드 포크를 해서는 안 된다고 맞섰다. 반대파는 무엇보다도 DAO 정신은 절대 사람이 개입하지 말자는 것이며 The DAO의 실험 목적도 사람의 개입을 배제하는 것이라고 주장했다, 또 무엇보다도 해킹은 블록체인의 문제가 아니라 스마트 컨트랙트의 버그였으므로 절대 사람이 개입해서는 안 된다고 거듭 설득했다. 그러나 대립은 싱겁게 끝났다. 90% 이상의 채굴업자를 등에 업은 비탈릭 부테린은 주저 없이 192만 번 블록을 하드 포크 시켜 잃어버린 이더리움을 되찾는다. 이때부터 이더리움은 이더리움 클래식과 이더리움으로 갈라지게 된다(〈그림 Ⅷ-11〉).

〈그림 Ⅷ-11〉 The DAO 사태로 인한 이더리움 하드 포크



힘의 논리에 의해 하드 포크로 갈라져 나온 비탈릭 부테린의 변종 이더리움은 '이더리움'이란 이름을 계속 사용했고, 반대파들이 지켜낸 원래의 이더리움은 '이더리움 클래식'이라는 다른 명칭으로 변경하는 수모를 겪게 된다. 비가역적 기록이라는 블록체인의 정신에서 보면 현재의 이더리움은 가짜인 셈이다.

4-4 드러난 탈중앙화의 민낯

The DAO 사건은 많은 이들에게 블록체인의 민낯을 보여주었다. 그동안 블록체인은 독립적이고 투명하며 한번 기록된 것은 절대 변경되지 않는다고 주장했던 것들이 모두 거짓이라는 것이 만천하에 드러난 사건이었다.

블록체인에서는 기록의 변경이 힘든 것이 사실이다. 그러나 채굴꾼들이 규합만 한다면 언제든 기록을 변경할 수 있다. 현재 비트코인과 이더리움의 개발은 각 재단이 장악하고 있으며, 10여 개 채굴업자가 전체 블록 생산의 90% 이상을 독점하고 있다.

5 탈중앙화 vs. 통제 불능

모든 소프트웨어는 사람이 만들고 사람이 운영한다. 그 누구도 개입되지 않는 투명하고 독립적인 환경이란 존재할 수 없다. 소프트웨어는 개발자가 임의로 바꿀 수 있으며, 이는 블록체인도 예외가 아니다. 소프트웨어 하나 설치한다고 해서 독립적이고 투명한 환경이 조성되는 일은 결코 일어나지 않는다. 그리고 블록체인의 기록은 절대 변경되지 않는다는 주장도 심한 과장이다. 소프트웨어로 할 수 있는 일은 작업에 드는 시간을 지수(Exponential) 시간으로 늘려 저항성(Resistance)을 늘리는 것뿐이라는 점을 명심하자. 적어도 비트코인과 이더리움으로 대변되는 현재의 블록체인은 독립과 투명과는 반대로 소수의 개발자들이 장악한 통제 불능의 시스템에 더 가깝다는 비난을 면치 못하고 있다.

[독립과 투명의 진실] 사집단의 배타적 운영

비트코인은 bitcoin.org라는 도메인을 소유한 자가 코드를 독점적으로 관리 · 운영하고 있고 대부분의 운영자금을 또 다른 단체인 비트코인 재단에 의존하고 있다. 이더리움 역시 이더리움 재단이 배타적으로 관리 · 운영하고 있다. 이들 재단의 주 구성원은 가상자산 개발자, 중개소, 그리고 채굴업자들이다. 블록체인은 독립되고 투명한 운영체제가 아니라 사적인 단체가 자신들의 이익을 위해 임의로 변경 · 수정하며 운영하는 시스템이다.

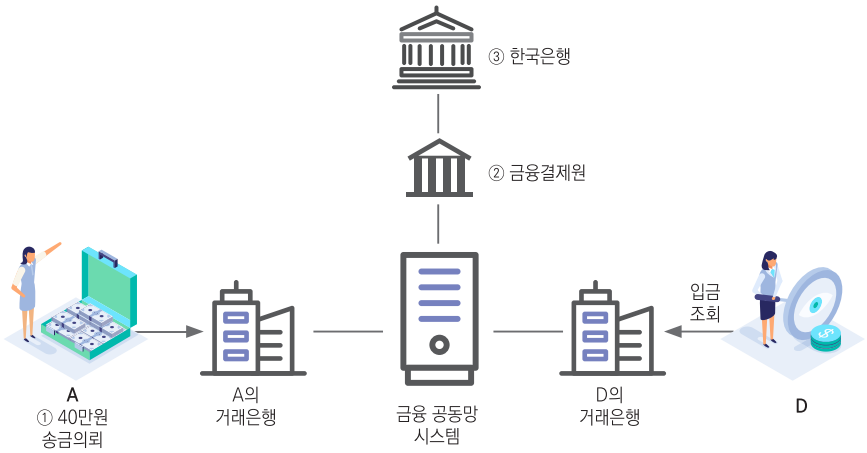
제5절

블록체인과 지급결제 시스템

1 비트코인과 지급결제 시스템

우리나라 금융기관은 금융결제원이 제공하는 은행공동망을 사용해 금융 거래의 편의를 도모한다. 다음 그림을 보자.

〈그림 Ⅷ-12〉 지급결제 시스템



〈그림 Ⅷ-12〉는 각각 다른 은행에 계좌를 가지고 있는 A와 D 사이의 금융거래를 보여준다. 그림에서 A가 D에게 40만원을 계좌이체하면, D의 은행은 A의 은행을 대신해 D에게 40만원을 지급해 준다. 이 절차를 지급(Payment)이라고 한다. 이때 A은행은 D은행에게 40만원을 빚지게 된 셈이므로, 이 돈을 갚아야 한다. 금융결제원은 각 금융기관별로 갚아야

할 금액을 기록해 두는데 이를 청산(Clearing) 절차라 한다. 한국은행은 금융결제원의 청산자료를 토대로 각 금융기관이 한국은행에 개설해 둔 당좌계좌에서 최종 금액을 결산하는데 이를 결제(Settlement)라고 한다. 이렇게 지급/청산/결제가 처리되는 시스템을 지급결제 시스템이라 한다. 한 나라의 지급결제 시스템은 그 나라의 금융 선진화 정도를 보여주는 핵심적인 척도이다. 미국도 Fed-Wire라 불리는 시스템이 우리의 금융공동망과 같은 역할을 한다.

1-1 비트코인의 지급청산

비트코인은 청산 기능을 하는 금융결제원이나 결제 기능을 하는 한국은행 같은 기관이 필요 없다. 비트코인은 이전을 위한 트랜잭션 자체가 청산과 결제를 포함하고 있으므로 별도의 청산과 결제 기관이 개입될 필요가 없기 때문이다. 한국은행을 포함한 각국의 중앙은행들은 비트코인과 같이 디지털로만 존재하는 결제 수단의 여러 특성에 대해 다양한 실험을 하고 있다. 중앙은행이 발행하는 비트코인이라는 아이디어는 CBDC라는 개념으로 확장되어 갔다.

1-2 CBDC(Central Bank Digital Currency)

CBDC는 중앙은행이 발행하는 디지털 법화의 개념이다. 실물을 찍지 않고 디지털로만 존재하는 법화를 생각하면 된다. 현재 CBDC에 가장 적극적인 나라는 중국이며 디지털로만 존재하는 법화에 대해 각국은 그 장단점에 대해 다양한 연구를 하고 있다. 한 가지 유념할 사항은 CBDC는 블록체인이나 가상자산과는 관련이 없다는 사실이다. 시중에는 이를 블록체인이나 가상자산과 연계된 것처럼 호도하는 이들이 많지만 이는 모두 사실이 아니다.

5만원권이 시중에 나올 때까지 8개 과정을 거치며 40여 일이 걸리므로 실물 화폐를 인쇄하지 않아도 된다는 것 자체가 큰 장점이 되겠지만 사실 CBDC의 가장 흥미로운 점은 고객 신원확인을 기반으로 유통된다는 것이다. 즉 완벽한 익명지급이 어렵다는 의미가 된다. 이 점은 감독당국입장에서는 가장 큰 장점이지만 프라이버시 보호라는 측면에서는 가장 큰 단점이기도 하다.

CBDC가 실제로 등장하기 위해서는 넘어야 할 산이 많이 있는데, 그중 하나는 실물 화폐만큼 사용이 편리한 디지털 단말기를 공급할 수 있느냐 하는 것이다. 이미 디지털화된 법화를 매우 편리하게 사용하고 있는 사람들에게 그보다 더 편리한 사용이 가능한 디지털 거래가 가능할 것인가는 매우 중요한 과제이다.

이 관점에서는 CBDC를 런칭하는 데 있어 가장 유리한 조건을 가진 나라는 IT 선진국인 대한민국일 것이다. 각국이 CBDC의 장단점을 연구하고 중국은 한시라도 빨리 런칭할 것처럼 선전하지만 제대로 기능을 갖춘 안정적이고 보편적 CBDC가 조만간 등장할 가능성은 낮아 보인다. 그러나 특수 목적으로만 제한된 CBDC, 예컨대 한국은행의 결제전용 CBDC는 그리 멀지 않은 시점에 발행될 수 있는 충분한 잠재력이 있다. 그 후 점차 보편적인 목적으로 확대되도록 진화해 나갈 수 있을 것이다.

핵심정리

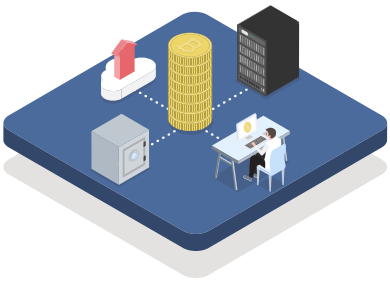
- 블록체인의 작동원리와 효용
  - 블록체인은 발생한 모든 데이터를 브로드캐스팅을 통해 공유하기 때문에 모든 노드가 항상 동일한 정보를 가진다. 따라서 모든 노드는 동등한 의무와 권한을 가지게 된다.

  - 중앙집중 시스템에서는 중앙서버의 단일 소프트웨어에 접속한 모든 사람이 동일한 서비스와 규칙을 이용하지만 블록체인은 각각 개별 접속 사용자가 스스로 다운받은 프로그램을 사용하므로 서로 버전이 다를 수 있어서 소프트 포크와 하드 포크라는 비일관성의 문제가 발생한다.

  - 비트코인 블록체인의 여러 제약을 극복하기 위해 이더리움과 하이퍼레저 등의 변형이 생긴다. 그러나 이들 변형 중 일부는 비트코인의 제약을 극복하기보다는 그 원형과는 전혀 상관없는 새로운 아케텍처로 바뀐 것으로서 그 속성 또한 정반대라는 논란이 있다.

  - 블록체인의 효용으로 널리 알려져 있는 수수료의 절감, 보안, 안전한 데이터베이스, 독립적 운용 등은 모두 사실이 아니거나 특정 요소가 과장된 측면이 있다.

헬로, 핀테크!(보안인증 · 블록체인)



HELLO, FINTECH!

8장

블록체인과 가상자산

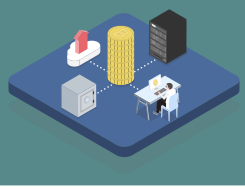
제1절 가상자산과 토큰

제2절 자산 유동화 토큰

제3절 다크코인과 자금세탁

제4절 가상자산과 금융사고

8장 블록체인과 가상자산



학습목표

1. 가상자산과 토큰을 구분할 수 있다.
2. 다크코인과 가상자산의 자금세탁 위험성을 이해하고 설명할 수 있다.
3. 자산유동와 토큰의 개념을 설명할 수 있다.

학습개요

이더리움은 새로운 커뮤니티의 구성 없이도 손쉽게 가상자산을 발행할 수 있는 표준인 ERC-20을 발표하면서 가상자산의 개수는 폭발적으로 늘어나게 된다. 한편 토큰을 통해 자산 유동화라는 새로운 아이디어의 표출과 함께 다양한 자금세탁 기능을 탑재한 암호화폐가 등장하기에 이른다.

이 장에서는 비트코인에서 촉발된 투자 목적물로서의 가상자산의 명암과 함께 FATF 권고에 따른 가상자산의 명확한 정의에 대한 의무 그리고 자금세탁 기능을 탑재한 코인과 이에 대한 추적 등 투자 목적물로서 그 용도가 파생된 블록체인의 여러 측면을 살펴본다.

용어해설

❶ ERC-20

Ethereum Request for Proposal의 약자로서 일반적인 RFC 형식을 이더리움 커뮤니티에서 사용하는 것을 말한다.

❷ 마켓 메이커(Market Maker)

시장조성자라고도 한다. 시장조성자 제도란 거래소와 시장조성 계약을 체결한 시장조성자가 매도, 매수 지정가 호가를 유동성이 필요한 상품에 제출하여 투자자가 원활하게 파생상품을 거래할 수 있도록 시장을 조성하는 제도인데, 2017년 9월부터 주식시장에도 정해진 종목에 한해 시장조성자 제도가 시행되고 있다.

❸ FATF

Financial Action Task Force의 약자이며, 1989년 G7에서 자금세탁방지를 위해 설립한 국제 조직을 말한다.

제1절

가상자산과 토큰

2021년 5월 30일 기점으로 전 세계 중개소를 통해 거래되고 있는 암호화폐 개수는 10,157개에 이르고 중개소 수는 수만여개에 이른다.[130)]

중개소는 하루 20여 개씩 생겨나고 암호화폐는 하루 50여 개씩 새로 중개소에 등록되는 현황이다. 이처럼 중개소와 가상자산이 넘쳐나는 이유는 그 개발에 있어서는 전문 지식이 크게 필요 없기 때문이다.

1 가상자산과 이더리움 토큰

가상자산을 만든다는 것은 디지털 목적물을 주고받는 내역을 기록할 수 있는 네트워크 프로그램을 만든다는 의미이다. 이러한 프로그램은 비트코인을 포함해 통상 그 소스 코드가 완전히 공개돼 있다. 따라서 누구나 그대로 이용할 수 있으며 경우에 따라 자신의 입맛대로 바꿀 수도 있다. 그러므로 프로그래밍 자체의 부담은 별로 없다. 정작 힘든 것은 생성된 가상자산이 원활하게 운영될 수 있는 생태계인 네트워크 참여자를 구성하는 일이다. 이는 웹사이트 구축은 어렵지 않으나 일정 규모 이상의 방문자를 모으는 것은 지극히 힘든 것에 비유할 수 있다.

130) CoinMarketCap.com 기준, 2021년 5월 10일

1-1 이더리움 스마트 컨트랙트와 토큰

이러한 점을 간파한 이더리움 재단은 별도의 네트워크를 구축하지 않고도 기존의 암호화폐와 거의 동일한 기능 즉, 발행, 이전 등이 가능한 새로운 방식을 제시했는데 바로 이더리움의 스마트 컨트랙트를 이용하여 가상자산을 발행하는 방법에 관한 것이다.

블록에 저장되는 프로그램의 내용을 단순히 가상자산의 발행과 이전에 관한 것으로 구성하면 이를 이용하는 사람들은 이더리움 네트워크를 그대로 활용할 수 있으므로 별도의 네트워크를 구성하는 번거로움을 피할 수 있다. 이더리움은 두 가지 표준적 스크립트 템플릿을 제공하고 각각 ERC-20과 ERC-721이란 명칭을 부여했고 이를 자체적으로 네트워크를 구축하고 있는 다른 암호화폐와 구분하기 위해 '토큰(Token)'이라는 별칭을 사용하기 시작했다. 즉 가상자산은 자체 네트워크를 구축한 것을 지칭하고 토큰은 자체 네트워크 없이 프로그램으로만 작동한다는 의미로 구분해서 부르기 시작한 것이다.

1-2 ERC-20

ERC는 Ethereum Request For Comment의 약어로서 이는 이더리움 커뮤니티에서 사용하는 RFC를 의미한다. ERC-20은 이더리움에서 만든 암호화폐 발행 프로그램의 표준이며 기본 템플릿과 함께 제공되어 숙련된 전문가의 경우 10분 정도면 새로운 암호화폐를 만들 수 있을 정도로 간단하다. 이 표준적 방법을 사용할 때의 가장 큰 이점은 별도의 네트워크를 구성하지 않아도 된다는 것이지만 그와 함께 ERC-20으로 발행된 토큰은 동일한 지갑을 사용해 주고받을 수 있다는 장점도 생긴다. 현재 ERC-20 표준에는 심각한 결함이 발견되어 새로운 표준인 ERC-223이 제안된 상태지만 기존에 발행된 대부분의 토큰은 ERC-20으로 되어 있다. 2020년 5월 11일 기준으로, 이더리움에 존재하는 ERC-20 토큰은 무려 262,234개에 달한다.[131]

131) Etherscan, https://etherscan.io

1-3 ERC-721

화폐는 액면이 그 가치를 결정한다. 모든 1만원권 지폐는 서로 맞교환이 가능한 동일한 가치를 가지고 있다. 즉 어디에 있는 누구의 1만원권이든 그 가치가 동일하다. 그러나 고려청자는 그 자체로 고유하며 맞교환 가치가 동일한 대상 같은 것은 존재하지 않는다. 이처럼 실물세계의 고유 목적물을 디지털 목적물로 흉내 낸 것이 바로 ERC-721이다. ERC-20이 일반 화폐와 유사하게 그 액면으로 가치가 결정되는 것에 비해 ERC-721은 각각이 고유물이며 그 가치가 모두 다르다. 대표적인 것이 크립토키티(Crypto Kitty)라는 가상의 고양이를 생성하는 프로그램이다. 단순한 게임이기도 한 크립토키티는 ERC-721 표준을 사용해 가상의 고양이를 생성한다. 이 고양이는 이전이 가능하다. 그러나 모든 고양이는 고유해서 그 가치는 늘 변동된다. 고양이가 팔리니 고유 목적물로서 돌과 공룡도 등장했고, 시간이 지나면서 더욱 다양한 형태의 가상의 고유물이 ERC-721로 구현되기 시작했다. 2020년 5월 11일 기점으로 이더리움에 있는 ERC-721은 무려 5,369개에 달한다. ERC-721은 NFT(Non-Fungible Token) 즉 대체 불가능 토큰으로도 불리는데 이 점은 다음 절에서 자세히 알아보도록 하자.

2 NFT(Non-Fungible Token)

내가 가진 1만원권 지폐와 타인의 1만원권 지폐는 분명히 다른 종이로 만들어진 서로 구분되는 목적물이다. 예를 들어 내가 가진 지폐는 낡고 접혔을 수 있고, 타인의 것은 빳빳한 신권일 수 있다. 그러나 이 둘이 가진 가치는 동일하다. 1만원이라는 화폐는 액면이 그 가치를 강제하기 때문이다. 우리가 쓰는 종이 돈은 법이 그 가치를 강제한 것이다. 그래서 '법정화폐(legal tender)'라고 부른다, '법'이 '정'한 강제 통용 화폐라는 의미이다. 화폐를 흉내 낸 비트코인도 마찬가지이다. 나의 1비트코인과 타인의 1비트코인은 서로 구분되는 '다른' 디지털 숫자로 기록되지만 그 가치는 동일하게 취급받는다.

만약 액면의 개념이 사라지면 어떻게 될까? 이제 그 가치는 각자 별도로 형성될 수도 있을 것이다. 앞서 예로 든 1만원권 지폐에 액면개념이 없다면 빳빳한 지폐는 낡은 지폐보다 더

가치를 받을지도 모르겠다. 실제로 1998년도의 500원 동전은 단 8,000개만 발행되었고, 그 때문에 액면과 상관없는 희귀함으로 인해 100만 원 이상에 팔리기도 한다고 알려져 있다.

이 개념을 디지털에서 흉내낸 것이 바로 NFT이다. NFT는 약자로서 통상 "대체 불가능(Non-Fungible)한 토큰(Token)"으로 번역된다. '대체 불가능'이라는 말이 다소 어려워 보이고 대단한 것처럼 들릴지 몰라도 그냥 '서로 구분할 수 있다'라는 의미로 이해하면 된다. 즉 모든 1만원권은 그 가치를 (적어도 액면으로는) 서로 '완전히 대체'할 수 있지만, 액면을 없애고 각각을 고유물로 구분하기 시작하면 그 가치를 완전히 대체할 수 없다는 의미이다.

원리는 매우 간단하다. 저장된 디지털 기호를 액면이 아닌, 식별번호로 구분하는 것이다. 비유를 해보자. 원래 비트코인에는 서로를 구분할 수 있는 식별자의 개념이 없다. 그런데 액면을 없애고 1번 비트코인, 2번 코인이라는 식으로 식별자를 부여해 구분하기 시작하면 비트코인이 NFT가 되는 것이다.

또 다른 예를 보자. 디지털 사진은 무한정 "복제"할 수 있고, 복제품의 품질은 동일하므로 굳이 서로를 구분할 실익이 없다. 그런데 복제한 디지털 사진에 일련번호 등의 고유 식별자를 부여하면 얘기가 달라질 수 있다. 누군가가 '가장 먼저' 복제한 사진이 더 의미 있다고 주장하고, 이 주장을 인정하는 사람이 있다면 거래가 성사될 수 있을 것이다. 물론 복제한 순서와 사진의 품질은 아무런 차이가 없는데도 말이다.

크리스티 경매에서 최근 이와 유사한 일이 일어났다. 디지털 그림에 연계되었다고 주장하는 NFT가 무려 6,900만 달러(한화 약 780억 원)에 거래된 것이다. 물론 경매에서 팔린 디지털 그림은 얼마든지 복제해서 그와 동일한 디지털 그림을 추가로 만들 수 있다. 다만 식별번호를 부여해 두었으므로, 경매에서 팔린 것과 나머지 복제품은 구분이 가능하다. 고유하다면 무엇이든 수백억에 팔릴 수 있을까? 하지만 다음 설명을 들으면 좀 이상하다는 생각이 들 것이다.

사실 크리스티 경매에서 팔린 NFT는 그림 자체가 아니다. NFT에는 그런 데이터를 담지 못한다. 경매에서 팔린 NFT는 그림을 샀다는 '영수증'에 불과하다. 이 NFT는 타인에게 판매할 수 있지만, 그 역시 디지털 그림 자체가 아닌 구매 영수증이 재판매되는 것이다! NFT에는 해당 작품이 있는 URL 주소나 그와 유사한 정보만 기록할 수 있을 뿐 소유자에 대한 어떠한 정보나 권리에 대한 기록도 담을 수 없다.

정리하면 다음과 같다.

1) A가 자신이 만든 디지털 그림을 어떤 서버에 저장해 두고 그 위치 URL을 담아 NFT를 발행한 후, 해당 NFT를 구매하면 보관된 디지털 그림의 유일한 소유자로 인정해 주겠다고 "말한다."

2) 그리고 NFT를 경매에서 팔았더니, B가 나타나 780억 원에 구매했다는 것이다.

A가 부주의로 서버를 고장 내면 원 그림은 완전히 사라질 수도 있다. NFT는 소유권을 주장할 수 있는 영수증일 뿐 실제 권리는 NFT를 발행한 자가 "약속을 지켜야만" 발생한다. 자동으로 소유권을 집행해 주는 프로그램이나 기관 따위는 없다. 오로지 A를 믿어야만 소유권이 인정되는 방식이다.

사실 고유한 디지털 그림을 거래하고자 한다면, 영수증만 주고받을 수 있는 블록체인이나 토큰이 아니라 전자서명을 이용해 실제 디지털 그림 데이터 자체를 받아야 하는 것이 상식이다. 그러므로 NFT라는 원시적인 방식이 '최첨단 권리증명' 기법처럼 호도된 것은 문제가 있다.

NFT는 단순히 코인이 식별자를 부여한 것일뿐 권리를 증명해 주는 기능과는 전혀 무관하다.

3 가상자산과 중개소

가상자산 중개소는 구매자와 판매자를 연결해주는 브로커 역할을 한다. 그러나 단순 연결만 해주는 브로커형 중개소는 거의 없다. 대부분은 고객의 돈을 수탁한 다음 매매를 알선한 뒤 거래가 성사된 가상자산을 보관하는 업무까지 같이하며 이를 위해서는 앞서 〈그림 Ⅵ-10〉에서 본 것처럼 거래를 알선하려는 각 가상자산의 지갑 소프트웨어를 갖추고 있어야 한다.

전 세계적으로 어느 정도 규모가 되는 중개소를 등록해서 그 정보를 보여주고 있는 CoinMarketCap 기준으로 보면 2020년 5월 11일 자로 등록되어 있는 중개소의 개수는 21,957개지만, 이곳에 등록되지 않은 것까지 합치면 그 수는 최소 열 배 이상으로 추정되며 단순 구매 대행업체까지 합치면 그 수는 훨씬 많다. 이렇듯 중개소가 우후죽순으로 생겨나는 이유는 진입장벽이 낮기 때문이다. 중개소 영업을 위해 필요한 것은 지갑 소프트웨어인데 이는 시중의 무료버전의 지갑을 사용해서도 간단히 해결할 수 있을 정도다. 현재는 중개소가 지켜야 할 별도의 소프트웨어 안전기준이 없으므로 중개소별로 그 안전도는 크게 차이가 날 수밖에 없다.

4 가상자산

FATF는 Financial Action Task Force의 약어로서 G7 미팅에서 자금세탁의 방지를 국제 협력을 통해 수행하자는 차원에서 결성한 조직으로서 파리에 본부를 두고 있다. 우리나라도 FATF의 회원국이며 2021년 36개국 39개의 회원이 있다. FATF의 권고문(Recommendation)은 회원국에는 법령에 해당하는 효력을 지닌다.

가상자산(Virtual Asset)이라는 용어는 암호화폐의 '화폐'라는 단어가 대중에게 잘못된 인식을 주지 못하게 하도록 FATF에서 각국에 암호화폐 대신 사용하도록 추천한 단어이다. 대부분의 국가는 FATF의 추천을 따라 가상자산이라는 단어를 사용하고 있으나 일본의 경우는 암호자산(Crypto Asset)이라는 용어를 쓰고 있다. 현재 각국은 FATF의 권고에 따라

가상자산의 범위와 정의를 규정하고 있다. 각국의 가상자산의 정의에 기존의 암호화폐가 들어갈 것은 자명하지만 나라별로 그 범위와 속성은 조금씩 다를 수 있다.

FATF는 2018년 10월 회원국들에게 가상자산의 정의와 규제 대상 취급업소의 범위 그리고 자금세탁방지 의무를 부과하도록 권고문을 개정했으며 같은 해 11월에는 G20 정상회의에서 FATF가 제정한 가상자산 자금세탁방지 국제기준을 각국이 이행할 것이라 결의하기도 했다.

우리나라는 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」(약칭: 특정금융정보법)을 개정하여 동 법 내에 가상자산의 정의를 새로이 신설하였는데 이 개정안은 2020년 3월 국회를 통과했고 2021년 3월 시행됐다. 「특정금융정보법」의 개정을 암호화폐의 제도권 진입이라 호도하는 이들도 있지만 이는 「특정금융정보법」 개정의 본질을 잘못 이해한 것이다. FATF의 권고는 가상자산의 정체를 규정하고 적절히 규제하여 자금세탁을 방지하는 데 그 목적이 있으며 가상자산 사업의 장려나 투자자의 보호와는 무관하며 오히려 자금세탁방지 장치를 적절히 마련하지 못하면 가상자산 사업을 금지해야 한다는 의미가 내포돼 있다. 가상자산은 암호화폐의 다른 말이 아니다. 가상자산은 암호화폐를 포함하는 보다 폭넓은 개념이다. 본서에서는 일괄적으로 가상자산으로 통일해서 쓴다. 정확한 문맥에서 가상자산과 암호화폐는 조금 다를 수 있다는 점을 이해하시기 바란다.

제2절

자산 유동화 토큰

1 자산 유동화와 토큰

자산 유동화(Asset Securization)란 자산보유자로부터 유동화 자산을 (i) 양도받은 유동화 전문회사 또는 (ii) 신탁받은 「자본시장과 금융투자업에 관한 법률」(약칭: 자본시장법)상의 신탁업자가 이를 기초로 유동화 증권(ABS; Asset Backed Securities)을 발행하고 이의 관리, 운용, 처분에 의한 수익이나 차입금 등으로 원리금 또는 배당금을 지급하는 일련의 행위를 말한다. 현재는 주로 은행, 증권회사, 자산운용사가 신탁업자 역할을 하고 「자본시장과 금융투자업에 관한 법률」 (이하, "자본시장법"이라 한다) 제296조에 의거 예탁결제원이 집합투자 재산의 취득, 처분 등에 관한 지시를 처리하는 업무에 관여하고 있다. 최근 ERC-20 토큰을 자산 유동화에 접목하려는 시도가 많이 등장하고 있다. 이 방식은 ABS 대신 토큰을 이용한다는 점을 제외하면 자산 유동화 과정과 개념적으로 거의 같다. 예컨대, 특정 부동산을 기초 자산으로 하여 토큰을 발행해 유동화를 한다면 개념적으로 다음의 과정을 거치게 된다.

1) 새로운 토큰(예 ERC-20)을 n개 발행한다.
2) 토큰 발행 회사는 각 토큰에 대해 그 기초 자산(예제의 경우는 부동산)에 대한 1/n의 권리를 보장하기로 구매자와 약속한다.
3) 발행된 토큰을 일반인에게 판매한다.

2 자산 유동화 토큰의 유의사항

우리나라는 2019년 9월 16일자로 「주식 · 사채 등의 전자등록에 관한 법률」(약칭: 전자증권법)이 시행되었다. 이 전자증권제도에 따라 주식 등 증권은 전자적으로만 발행하고 관리함으로써 그 위변조를 방지하는 등 소유자의 권리를 보호하도록 하고 있다. 이때 전자적으로 증권을 등록하고 관리할 수 있는 자격은 동 법에 의해 엄격히 규정되어 있다.

증권을 발행하고 이를 전자적으로 기록할 수 있는 자의 자격을 엄격히 규정하는 이유는 해당 증권에 대한 소유권 또는 담보권을 안전하게 보장해 주기 위함이다. 그러나 이러한 증권 대신 토큰을 이용하게 되면 여러 가지 문제가 파생되므로 주의할 필요가 있다.

첫째, 토큰에는 소유에 권한 그 어떠한 권리도 기록할 수 없다. 따라서 토큰과 기초 자산에 대한 권리를 매칭시키는 별도의 서버가 필요하므로 이에 따라 관리가 이원화되는 등 기존 데이터베이스 방식에 비해 안전성과 효용성이 크게 떨어질 수 있다.

둘째, 전자증권법상에는 전자등록업의 허가 조건에 관해 인적, 물적 요건, 사업계획, 이해상충방지 등의 엄격한 기준을 정하고 있다. 그러나 전자등록업 허가를 받지 않은 자가 토큰을 발행해 기초 자산을 관리하게 되면 이러한 기준을 따르지 않아도 되므로 투자자 보호가 크게 약화될 수 있다.

셋째, 발행된 토큰을 구매한 자가 해당 암호화 키를 분실할 경우 이를 복구할 수 있는 방법이 없고 임의로 토큰을 이전한 경우 이를 기초 자산과 매칭시키는 것이 불가능할 수 있다.

넷째, 부동산 등이 그 기초 자산일 경우 향후 매각을 위해 토큰을 모두 회수해야 할 필요성이 생길 때 이를 통제할 수 있는 방법이 없다. 경우에 따라 그 소유자를 특정할 수 없고 각각의 개인키로만 접근할 수 있는 토큰을 일괄 관리할 방법도 없기 때문이다.

다섯째, 발행된 토큰을 다양한 중개소에서 거래하게 되면 그 가격이 실제 가격과 심하게 괴리될 수 있고, 그마저도 중개소별로 상이하여 기초 자산과의 연계성 자체가 무의미해질 수 있다.

결국 기획된 자산 유동화의 원 취지가 좋더라도 그 방법론에 있어서 토큰을 선택한다면 오히려 불필요한 다른 여러 문제점을 야기 시킬 수 있으므로 유의해야 한다. 최근에는 그 기초 자산의 대상으로 미술품, 저작권 등으로 확대하고 있으며 일부는 감독의 사각지대에서 무분별한 발행을 통해 구매자를 호도하고 있으므로, 반드시 토큰 발행회사의 신뢰성을 잘 따져보아야 한다.

3 자산 유동화의 핵심

자산 유동화를 통한 이점을 살리기 위해서는 발행된 증권 또는 증표의 안전한 등록을 통해 소비자 권리의 보장에 만전을 기해야 함은 물론 그 거래 가격이 기초 자산의 실제 가치와 괴리되지 않게끔 감독할 필요도 있다. 이 때문에 토큰을 이용한 방식은 여러 관점에서 주의를 요한다. 이를 보완할 수 있는 적절한 대안이 제시되지 않는다면 토큰을 이용한 방식은 피해야 할 것이며, 전자등록업 허가를 받은 자가 사용하는 데이터베이스 방식이 훨씬 더 안전하고 편리하다. 자산 유동화의 핵심은 신뢰할 수 있는 기관이 발행된 증권과 권리의 등가성을 보장해 주는 것이다.

제3절

다크코인과 자금세탁

1 자금세탁의 진화

비트코인은 절대 익명을 추구하여 구현되었지만, 기술적 관점에서는 몇 가지 단서를 통해 신원을 특정할 수도 있다.[132)]

첫째, 비트코인을 거래한 당사자들이 사용한 비트코인 주소는 누구나 열람할 수 있도록 공개되어 있다.

둘째, 비트코인 트래픽은 암호화되지 않은 상태에서 네트워크에 전송되므로, 특정 발신지를 계속 모니터링하면 IP추적을 통해 비트코인 주소의 소유자를 알아낼 수 있는 가능성도 존재한다.[133)]

따라서 중개소를 통한 거래를 포함해 특정 비트코인 주소가 누구의 것인지 알 수 있다면(물론, 이것이 제일 힘든 일이지만) 거래의 흐름을 추적하는 것이 이론적으로 가능하다.

한편, 비트코인 이후에 나온 일부 가상자산은 추가적인 자금세탁 장치를 내장시켜 절대 익명성을 더욱 보강함으로써 거래의 추적을 무력화하려는 시도를 했다.

모네로는 소위 링 시그니처(Ring Signature)를 통해 코인 주소의 소유자를 특정하기 힘들게 만들었다. 비트코인은 그 거래 당사자들의 비트코인 주소만 기록되어 있지만 모네로는

132) 이러한 이유로 비트코인도 슈도니머스에 가깝다고 주장하는 사람도 있다.
133) 최근에는 Tor를 통해 IP 은닉을 시도하는 별도의 클라이언트도 배부된다.

당사자의 가상자산 주소와 함께 의도적으로 다수의 제3자를 한데 섞어 그중 누가 실제 거래 당사자인지 모르게 하는 모호성을 개입시켰다. 이와 함께 일회성 가상자산 주소를 사용하는 스텔스(Stealth) 주소를 지원하는 등 거래 당사자를 모호하게 하는 다양한 기능을 지원한다.

ZCash는 비트코인에 프라이버시를 보호하는 계층을 더 추가하여 만든 코인이다. 이는 소위 제로-지식(Zero Knowledgement) 증명을 이용하여 발신지를 드러내지 않는 전송을 구현했다고 주장하는 zk-SNARKs 방식으로 소유자의 특정을 방해한다. 제로-지식 증명을 비유를 통해 쉽게 설명하자면 비밀번호를 누르지 않고도 방문을 열 수 있게 한다는 것인데, 비밀번호를 직접 말하는 대신 비밀번호를 '알고 있다는 사실을 증명'하는 것으로 대체함으로써 비밀번호 자체가 누출되는 것을 방지한다는 기술이다.

Dash[134]는 PrivateSend라는 기능을 통해 거래 당사자를 특정하기 어렵게 해 준다. PrivateSend는 소위 CoinJoin이라는 기법을 이용하는 것인데, CoinJoin이란 여러 발신 당사자를 한데 묶어 그 총합을 만든 뒤 그 금액을 여러 갈래로 쪼개서 다수의 수신자에게 전달함으로써 거래 당사자들을 특정하기 힘들게 하는 기술이다. 말 그대로 자금세탁을 위한 기법을 버젓이 구현해 놓은 셈이다. Dash는 CoinJoin을 위해 마스터 노드라 불리는 '중앙' 서버를 운영하고 있어 '탈중앙화'라는 말을 무색하게 하고 있다. Dash는 모두 5개의 유동성 공급자를 제공하고 있으며 PrivateSend로 CoinJoin을 통해 자금세탁을 하려면 이 중앙화 서버들을 유료로 이용해야 하므로 탈중앙화나 독립 등과는 거리가 멀다. 일본 금융당국은 2018년에 이미 모네로, Dash, ZCash를 중개업소에서 취급하지 못하도록 금지하는 조치를 취했다.[135]

134) Dash는 원래 2014년 Xcoin이란 이름으로 비트코인에서 하드 포크 되었다가, 후에 DarkCoin으로 이름을 바꾼 뒤 2015년에 지금의 이름인 Dash로 또 바꾸었다.

135) Investopedia, https://www.investopedia.com/news/japans-fsa-bans-private-cryptocurrencies/

2 가상자산 거래 추적

범죄자들이 자금을 주고받는 주된 도구로 가상자산을 사용하는 비율이 날로 확대되어 가는 이유는 그만큼 자금세탁과 은닉이 용이하기 때문이다. 이들은 특히 모네로와 대시 등의 다크코인류를 선호하는데 가상자산이 기존에 가지고 있던 익명성에 더해 더 강력한 자금세탁 기능을 제공하기 때문이다. 최근에는 코인개발자들이 수없이 많은 아류코인들 사이에서 더 주목받기 위해 경쟁적으로 보다 강력한 자금세탁 기능을 탑재하며 이를 선전하기도 한다. 이러한 자금세탁 기법은 크게 두 가지 방식을 사용해 거래 추적을 막으려 하고 있다.

첫째, 거래 당사자의 가상자산 주소를 숨기는 방법을 쓴다. 대표적인 방법이 여러 송신자와 수신자 들을 묶으며 경우에 따라 허위 송수신자 들도 섞는 방법을 사용하여 실제 거래 당사자들이 누군지 특정하기 힘들게 만든다.

둘째, 가상자산 거래를 위해 접속한 IP 주소를 숨길 수 있는 방법을 동원한다. 대표적인 것이 Tor 등 IP 주소 추적을 방해하는 소프트웨어를 이용한다.

이 때문에 범죄에 가상자산이 이용되는 일은 더욱 확대될 것이고 그에 따라 범죄에 이용된 가상자산의 거래를 추적하는 기술과 이에 대한 적절한 서비스를 제공할 수 있는 업체의 필요성 또한 더욱 커지고 있다. 향후에는 가상자산 추적기술이 더욱 필요해 질 것이다.

제4절 가상자산과 금융사고

2017년 말 비즈니스 인사이더는 텔레그램(Telegram)에 존재하는 상위 5개의 펌프 앤 덤프(Pump & Dump) 채팅 그룹을 발표한 바 있다. 이들은 100여 명부터 많게는 1만 4천여 명까지 세력을 구축한 후 희생양들을 조직적으로 유인하기 위해 SNS와 블로그, 게시판들을 적극 활용해 시세를 부풀렸고, 각종 허위 소식 등을 퍼뜨리며 동시에 가격 축을 상(上) 방향으로 흔든 후 희생양들이 몰려들면 시세 정점에서 한꺼번에 털어낸다.[136]

'펌프 앤 덤프'는 이렇게 시세 조종을 하는 그들의 행동을 묘사한 것이다. 가상자산과 관련한 금융사고가 빈번한 이유는 신원을 특정하기 힘든 속성 때문이다. 비트코인 광풍의 이면에도 시세를 조종하기 위한 테더(Tether)[137]와 비트파이넥스(Bitfinex)의 음모가 있었다고 보는 것이 현재 뉴욕검찰의 입장이다. 테더는 현재 뉴욕주에서 두 가지 혐의로 재판 중에 있는데, 하나는 비트파이넥스가 보유한 비트코인의 가격을 조작한 것이고 다른 하나는 자신들의 주장과 달리 달러를 적절히 예치하지 않은 혐의이다.[138] 2018년 비트코인이 20,000달러를 넘은 광풍의 이면에는 테더와 비트파이넥스가 합작하여 시세를 조종했기 때문이라는 것이 그 주된 혐의인데, 이는 비트코인 거래의 70% 이상이 테더로 이루어진다는 점과, 수익구조가 전무하다시피 한 테더를 많은 비용을 들여 굳이 발행하고 운영하고 있는 점을 감안하면 합리적 의심을 가능케 한다.[139]

136) BISINESSINSIDER, https://www.parsintl.com/publication/business-insider

137) 테더는 달러와의 태환을 보장한다고 주장하는 코인이다.

138) Bloomberg, https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether, 블룸버그 2018년 11월 20일 자 기사(최종 접속 2020년 3월 14일)

139) Newsweek. https://www.newsweek.com/bitcoin-bitfinex-tether-cryptocurrency-market-manipulation-historic-value-fraud-1469640, 뉴스위크 2019년 11월 4일 자 기사(최종 접속 2020년 3월 15일)

1 마켓 메이커(Market Maker) vs. 시세조종

2018년 12월 검찰은 업비트[140]의 전 대표이사를 포함 임직원 3명을 시세조작 등의 혐의로 기소했다. 검찰은 업비트가 시세조작으로 1500억을 빼돌린 것으로 보고 있다.[141] 이에 대해 업비트는 자신들은 마켓 메이커(시장조성자) 역할을 했을 뿐이라고 강변하고 있다.

시장조성자 제도는 자본시장법에 근거해 2016년 1월부터 도입한 합법적 시장 활성화 제도이다. 한국거래소는 시장조성자 제도를 통해 유동성을 공급하여 거래 활성화를 꾀하고 있으며 주식에서도 지속적으로 해당 종목을 확대하며 유동성 공급을 하고 있다. 그러나 시장조성자의 자격조건과 시장 개입조건(종목 및 개입 조건)은 규정으로 엄격히 통제하고 있다.

규제를 받지 않는 시장조성자는 시세조종자와 다름없다. 한국거래소 내의 합법적 시장조성자조차 자전거래(Cross Trading) 등을 통한 간접적 시세 조종의 가능성을 내포하고 있다.

업비트는 스스로 거래에 참여하며 (ⅰ) 가짜 계정을 만들어 자산을 예치한 것으로 조작 (ⅱ) 254조 5,348억 규모의 허수 주문 (ⅲ) 4조 2,670억 규모의 가장매매 (ⅳ) 비트코인 거짓 거래를 통해 회원 26,000명에게 총 1,491억원을 갈취한 혐의로 현재 재판 중이다.

이처럼 현재 가상자산을 둘러싼 여러 가지 문제점이 빈번하게 발생하는 것은 적절한 통제 규정의 미비 때문이다. 빠른 시기에 그 규정이 정비되어야 할 것이며 그 첫 신호탄이 바로 「특정금융정보법」 개정에 따른 가상자산 취급업소에 대한 의무부과가 될 것이다.

---

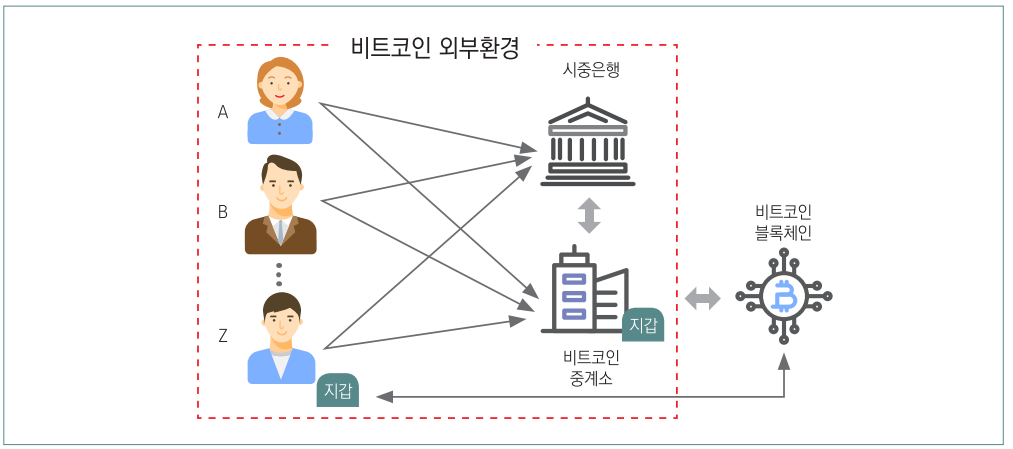
140) 업비트는 국내 코인 중개소이다.
141) 업비트, 검찰발표에 대한 업비트의 입장 공지사항(2018.12.21), https://upbit.com

2 가상자산과 해킹

2018년 12월 빗썸[142]이 해킹 당해 4억 7,000만원을 도난당한 박 모 씨가 빗썸을 상대로 낸 손해 배상 청구소송에서 국내 법원은 빗썸의 배상 책임이 없다는 판결을 내렸다. 재판부는 가상화폐는 「전자금융거래법」을 적용할 수 없다고 판시하였다.[143]

그러나 이 판결은 관점에 따라 문제의 소지가 있다. 고객은 법화를 빗썸에 송금하고 가상자산을 구매했지만 자신의 명의로 된 가상자산을 단 한 번도 실제로 가진 적이 없기 때문이다. 이제 중개소에서 해킹이 빈번하게 발생하는 이유와 중개소에서 가상자산 거래 시 어떤 일이 발생하는지 간단히 살펴보자.

〈그림 Ⅷ-1〉 가상자산 거래와 중개소



〈그림 Ⅷ-1〉은 중개소와 블록체인과의 관계를 보여준다. A와 B가 가상자산을 구매하면, 중개소들은 구매가 일어난 것처럼 중앙 서버 장부에 숫자만 조작해 표시할 뿐 실제 블록체인 거래는 일어나지 않는다. A, B는 자신들이 구매한 가상자산이 그들 명의의 주소로 블록체인에

142) 빗썸은 국내 코인 중개소이다.
143) 서울중앙지법 2018.12.20., 선고 2017가합585293 판결

보관된다고 생각하지만, 모든 가상자산은 중개소의 주소에 일괄 보관될 뿐이다. 이때 그림의 Z처럼 별도로 지갑을 설치 후 지정한 주소로 이전을 요청하면, 중개소는 그제야 일괄 보관하던 것 중 일부를 실제 블록체인 거래를 통해 이전한다. 중개소들의 보안 수준은 천차만별이지만, 적절한 관리감독은 이루어지지 않고 있다.

해커들은 비교적 손쉽게 중개소를 해킹한 다음, 가상자산을 절취할 수 있다. 다시 앞 그림을 보자. 그림 중 Z가 해커라고 가정하자. Z는 이제 다음의 과정을 거쳐 A의 가상자산을 절취할 수 있다.

① Z는 중개소를 해킹한 다음, 자신의 신원이 A인 것처럼 속인다.
② Z는 해킹한 중개소에 자신이 지정한 가상자산 주소로 A가 위탁한 모든 가상자산을 송금할 것을 요청한다.
③ 해킹을 당해 Z를 A로 오인하고 있는 중개소는 A가 위탁한 모든 가상자산을 중개소 명의의 주소에서 Z가 지정한 주소로 이전한다.

[중개소의 해킹]

경찰청 자료에 따르면 2016년 7월부터 2019년 3월까지 알려진 것만 해도 국내 중개소는 8번의 해킹을 당해 총 1,635억원을 도난당했으며, 이 중 국내 최대 규모 중개소인 빗썸은 3건의 해킹을 통해 무려 793억원의 손실을 입은 것으로 파악됐다.

핵심정리

- 블록체인과 가상자산
  - 이더리움은 자체 네트워크의 구성없이 쉽게 가상자산을 발행할 수 있는 프로그램 표준인 ERC-20과 ERC-721을 발표하면서 가상자산 개수는 기하급수로 증가한다. 이들은 토큰이라는 별도의 명칭으로 불리며 단순히 가상자산을 발행하고 거래하는 기능만 가지고 있다.

  - 자산 유동화 토큰이라는 명목으로 기존 ABS 대신 ERC-20 토큰을 발행하려는 시도가 많은데, 이는 소유권의 보장 약화 등의 여러 문제를 야기할 수 있다. 한편 5,000여 개가 넘는 여러 가상자산 중 자신이 더욱 주목받기 위해 자금세탁 기능을 탑재하는 코인들이 개발되고 있고, 이는 건전한 금융에 대한 새로운 위협이 되고 있다.

  - 가상자산의 개념은 FATF의 권고에 따라 각국에서 현재 나름대로의 정의를 내리는 중에 있으며 그 핵심은 자금세탁 위협의 방지에 있다.

헬로, 핀테크!(보안인증 · 블록체인)

HELLO, FINTECH!

9장

블록체인 정책 및 산업 동향

9장 블록체인 정책 및 산업 동향

학습목표

1. 금융위원회와 과학기술정보통신부의 정책 기조를 이해하고 설명할 수 있다.
2. 정부의 핀테크 육성 방안에 대해 설명할 수 있다.
3. 업계 사례를 통해 프로젝트의 적절성을 논할 수 있다.

학습개요

금융위원회는 핀테크 육성에 대해 적극적인 정책을 펴고 있고, 과학기술정보통신부는 블록체인 기술의 육성에 적극적이다. 이 장에서는 금융위원회와 과기정통부의 정책기조에 대해 살펴본 다음 시중의 몇 가지 블록체인 프로젝트에 대해 평가해본다.

용어해설

❶ 규제 샌드박스

신제품, 신서비스 등을 출시할 때 일정 기간 기존 규제를 면제해주는 제도다. 모래 놀이터처럼 '규제 프리존'에서 새로운 산업이 더 발전할 수 있다는 취지로 2016년 영국에서 핀테크 산업을 육성하면서 처음 등장하였다.

❷ 규제 프리존

2015년 12월 16일 발표. 정부가 27개 전략산업을 육성하기 위해 규제를 대폭완화하기로 한 14개 도시를 말한다. 정부가 '2016년 경제정책방향'에서 핵심 콘텐츠로 내세운 것으로서 신성장 산업 기반 마련과 지역경제 발전을 도모하기 위해 지정하였다.

제1절

블록체인 관련 정부 정책 동향

금융위원회는 다각도로 핀테크 사업을 지원하고 있다. 2015년 3월 30일에는 핀테크 기업과 금융회사의 현장 접점 역할을 위한 핀테크 지원센터를 설립하기도 했다. 또, 2018년 10월 19일에는 당시 김용범 부위원장 주재로 핀테크 등 금융혁신을 위한 규제개혁 T/F를 구성했으며, 2019년 10월 15일에는 손병두 부위원장 주재로 핀테크 활성화를 위한 규제혁신 전담 TF를 구성했다. 또한 「금융혁신지원 특별법」의 시행 준비를 비롯한 핀테크 활성화를 추진 중이며 최근에는 실질적인 지원을 위한 펀드를 조성하기 위한 계획도 발표했다.

1 한국핀테크지원센터

2015년 3월 30일 개소된 한국핀테크지원센터는 10개 시중은행, 5개 카드사, 11개 증권, 보험사 및 코스콤, 금융결제원, 금융보안원 등 유관기관 핀테크 관련 업무 전문 실무자들이 스타트업/예비창업자들의 핀테크 사업에 대한 상담을 그 주목적으로 하고 있다. 주요 기능으로는 핀테크 스타트업 및 기술벤처 육성, 정책금융기관을 통한 핀테크 기업 자금조달 및 다각적 지원, 핀테크 분야 핵심기술 연구개발이 있으며 창업절차, 아이디어 실용화, 시장성 평가, 보안수준제고 방안 등 종합 상담 서비스를 제공하고 있다.

특히 다양한 혁신 서비스가 등장하며 기존 법령과 충돌 가능성이 높은 분야인 핀테크의 지원을 위해 정부는 국정과제인 8대 혁신성장 선도사업의 일환으로 핀테크 산업 활성화를 위한 규제샌드박스 도입을 통해 예산지원을 추진해 왔고 이를 법제화한 「금융혁신지원 특별법」 제정안은 2018년 12월 7일 국회 본회의를 통과했다.

2020년 5월 12일 '대한상공회의소 규제 샌드박스 지원센터' 출범식에서는 그동안 공공기관에서만 운영되던 규제 샌드박스 지원기능을 민간 영역으로 확대하고 5대 전담기관을 지정하였는데, 한국핀테크지원센터는 혁신금융 전담지원센터로 지정되었다.

2 핀테크 혁신펀드

2019년 12월 23일 은행권과 금융유관 기업이 참여한 핀테크 혁신펀드가 조성되었다. 이는 KB, NH, 신한, 우리, 하나 등 주요 금융그룹과 BNK, DGB 등 지방은행, 코스콤, 은행권 청년창업재단이 참여한 민간 주도 펀드로서 운용규모는 2020년 ~ 2023년까지의 4개년간 총 3,000억원이며 혁신적 핀테크 기업에 집중 투자된다. 펀드의 운용사로는 한국투자파트너스와 KB 인베스트먼트가 3월 23일에 선정되었다.

이 펀드는 창업 초기(창업 5년 이내 초기) 핀테크 스타트업과 초기 이후의 스케일업, 해외진출 지원투자로 구분되어 각각 1,500억원씩 투자된다. 또한 자금운용 추이와 시장수요를 감안하여 6년간 5,000억원으로 확대할 것이라 발표했다. 2020년에 총 855억원 이상의 자금이 배정되고 핀테크 빅데이터, 블록체인, 해외소재 금융 플랫폼에 200억원 규모의 투자를 최초로 집행했다.

3 금융회사의 핀테크 투자 등에 관한 가이드라인

2018년 11월 16일 이낙연 국무총리가 은행장 간담회에서 금융회사의 핀테크 기업 출자 허용을 추진할 것을 지시함에 따라 금융위원회는 금융회사가 디지털 전환 흐름에 능동적으로 대응할 수 있도록 핀테크 투자 규제 관련 가이드라인을 마련하고 2019년 10월 4일 발표하게 된다.

이 가이드라인을 살펴보면 금융회사가 출자 가능한 핀테크 회사 유형에 인공지능이나 사물인터넷 등은 구체적으로 적시되어 있지만 블록체인은 언급되지 않는다. 다만 블록체인 기업이 핀테크 기업에 포함될 수 있다고 해석해 볼 수 있는 항목으로는 제2조 제2호의 핀테크 기업의 정의 부분 중 '자'목에서 (ⅰ) 인공지능, (ⅱ) 빅데이터의 분석 및 이용, (ⅲ) 사물인터넷, (ⅳ) 그밖에 (ⅰ)부터 (ⅲ)까지와 유사한 기술로서 금융위원회가 인정하는 기술이라는 부분과 '카'목에서 그 밖에 정보통신 기술, 그 밖의 디지털 신기술을 활용하여 금융 산업 또는 금융소비자에 기여하거나 기여할 것으로 예상되는 사업을 하는 기업으로서 금융위원회가 인정하는 기업이라고 되어 있다. 따라서 금융위원회가 정의하는 핀테크 기업과 연계된 블록체인이란 디지털과 관련된 기술이며 가상자산을 유통하는 등의 사업자는 포함되기 힘들다는 점을 유추해 볼 수 있다.

제2절

블록체인과 핀테크

2020년 5월 11일 기점으로 전 세계 중개소를 통해 거래되고 있는 가상자산 개수는 5,439개에 이르고 중개소 수는 21,957개에 이른다.[144)]

중개소는 하루 20여 개씩 생겨나고 가상자산은 하루 50여 개씩 새로 중개소에 등록되는 현황이다. 이처럼 중개소와 가상자산이 넘쳐나는 이유는 그 개발에 있어서는 전문 지식이 크게 필요 없기 때문이다.

블록체인에 대한 정부의 정책 동향은 크게 두 가지 측면에서 구분해 볼 수 있다. 하나는 가상자산의 실체 규명과 관련된 금융 당국의 정책 방향이며 다른 하나는 과학기술정보통신부가 중심이 된 블록체인 기술 육성 사업이다.

1 금융당국의 가상자산에 대한 규정 정비

앞서 제8장에서 살펴본 것처럼 현재 FATF의 권고문에 따라 각국에서는 가상자산의 정의와 함께 그 취급업자의 정의 그리고 의무규정을 정비 중에 있다. 이러한 규정은 국제적 공조 하에 이루어질 것이며 그 결과에 따라 향후 가상자산에 대한 금융당국의 정책도 많은 영향을 받게 될 것이다. 현재까지 각국의 일반적인 동향은 가상자산의 범위를 폭넓게 정의하여 가급적 많은 유형의 디지털 관련 자산을 규제의 틀 속에 포함하려고 하고 있다.

자금세탁방지를 위한 가상자산 거래 추적기술이나 각국 규정에 따른 취급업소의 의무사항을 준수하기 위해 가상자산 취급업소들은 관련한 기술을 확보할 필요성이 생겼다. 가상자산과 관련한 국제적인 규정의 정비와 함께 다양하고 새로운 형태의 유관 기술 시장이 생성될 것으로 보인다.

144) CoinMarketCap.com 기준, 2020년 5월 10일

2 과학기술정보통신부의 정책 동향

과학기술정보통신부(이하, 과기정통부)는 2018년 정부출연 4,282억원, 기업체 출연 1,284 등 총 5,566억원 규모의 블록체인 중장기 기술개발 사업을 위한 예산을 기획하고 예비타당성 조사를 신청했다. 이 금액은 2020년부터 2026년 사업기간에 집행할 목적으로 책정되었다.

〈그림 Ⅸ-1〉 과기정통부 블록체인 사업 예비타당성 조사 결과

과학기술정보통신부의 블록체인 중장기기술개발 사업 예비타당성 조사 결과

사업비(정부)	5,566억원(4,282억원)
사업기간	2020~2026년
비용편익(B/C) 비율	0.16%
종합평가(AFP) 시행점수	0.293(0.5 이상이면 시행)
비고	• 과제우선순위 설정과정에 문제점이 존재 • 사업목표가 적절히 설정되지 못함 • 장기간 연구개발(R&D) 추진을 통해 확보하고자 하는 핵심원천기술의 실체가 불명확함 • 선도 서비스 구축계획의 구체성이 미흡하고 관련 부처와의 협업이 부족함 • 경제성 확보 가능성 낮음

출처: 한국과학기술기획평가원(KISTEP) 보고서

그러나 이 사업은 한국과학기술평가원에 의해 사업목표의 구체성이 떨어지고 핵심원천기술의 실체가 불명확하다는 사유로 기준점 이하의 점수를 받아 보류되었다(〈그림 Ⅸ-1〉). 과기정통부는 2020년 1월 17일, 이 계획을 일부 수정하여 2021년부터 2025년까지 5년간 총 4,000억원 규모의 국비를 투자하는 '블록체인 R&D 연구사업'에 대한 예비타당성 조사를 한다고 밝혔다. 과기정통부는 데이터, 네트워크, 인공지능 기반의 디지털 선도국가로 나아가기 위해 핵심 응용기술로서 블록체인을 연구하겠다고 밝히고 있다.

한편, 블록체인의 실증적 사례를 찾기 위한 과기정통부의 투자는 지속될 것으로 전망되며 유관 예산도 계속 집행될 것이다. 실례(實例)로 과기정통부는 2020년 3월 16일 정보통신산업진흥원(NIPA)과 함께 9개 프로젝트를 선정하여 45억원을 지원하는 블록체인 기술 검증지원 시범 프로그램을 추진하고 있다.

제3절

블록체인 시장 현황

시중에는 다양한 형태의 블록체인 프로젝트가 진행 중에 있다. 여기서 '블록체인'이라 함은 주로 패브릭 기반으로 구성된 SI 사업과 연계된 시장을 의미한다. 시중에는 향후 세계 블록체인 시장의 규모를 최소 수십 조달러에서 최대 수천 억달러 규모로 예측하고 있지만, 대부분은 가상자산 시장의 단순 거래 규모와 현재의 가상자산 평가액을 합산하는 등 그 예측의 정확도가 높지 않다.

국내에서의 전망을 살펴보면 정보통신산업진흥원(NIPA)이 한국과학기술정보연구원(KISTI)의 보고서를 인용해 발표한 자료에서 국내 블록체인 시장 규모를 2019년 846억원, 2020년 1,366억원, 2021년 2,206억원, 2022년 3,562억원으로 매우 구체적인 수치로 전망하고 있다. 그러나 이 규모 자체는 클라우드 등 타 산업에 비하면 미미한 수치이면서 동시에 대부분이 시범사업에 그치고 있으므로 그 의미가 그리 크지 않다. 한편 NIPA가 외국의 전망을 인용해 발표한 세계시장규모는 2020년 46억달러, 2022년 108.6억달러로서 이 역시 자료의 신뢰성은 미지수다.

블록체인 시장의 상당수는 시범사업이며 일반적 디지털 SI 사업이 그저 블록체인이라는 명칭을 사용하고 있는 것도 적지 않으므로 이 분야에 대한 보다 정확한 예측을 위해서는 좀 더 시간이 필요해 보인다.

소프트웨어 개발용역 시장(SI, System Integration)으로 대변되는 블록체인 시장과 다대다의 투기시장으로 변화된 가상자산 중심의 시장은 연관성이 없는 개별 시장이다. 기술 과제와 관련한 다양한 기회가 있을 수 있지만 블록체인이라는 용어에 매몰되는 것은 좋지 않다. 현재 시범사업이 대부분인 블록체인 사업의 내부를 들여다보면 안전한 분산저장, 정보의 공유, 컨소시엄을 이룬 회사 간 고도의 협업 등이 그 핵심이다. 특히 마이데이터, 오픈 API 등은 협업을 통한 데이터의 활용을 지원해 줄 수 있으므로 컨소시엄 형태의 네트워크 필요성이 증대될 것이다.

뚜렷한 목적성 없이 블록체인이라는 마케팅 용어만 내세운 일회성 · 단발성 시장은 도태될 것이지만, 그 핵심 개념을 연구하는 디지털 금융 시장은 지속적으로 확대될 것이다.

결국 블록체인이라는 용어에 매몰되지 않고 그 핵심 개념을 분리해 보면 향후 시장의 방향을 살펴볼 수 있을 것이다.

제4절

가상자산 시장

가상자산 거래 시장은 2020년 5월 기준으로 최소 하루 110조 원이고 5,500여 개 가상자산의 전체 평가액은 300조 원 정도였으며, 가상자산 중 비트코인이 차지하는 비중이 무려 66%에 달했다. 그러던 것이 2021년 초부터 다시 치솟기 시작하여 2021년 4월 14일 기준 비트코인은 무려 64,650달러까지 상승했고 국내 가격은 8,000만 원을 넘어섰다. 이 광풍은 다시 5월 8일을 기점으로 가파르게 하락하여 2021년 6월 8일 기점으로 33,000달러까지 폭락했다. 몇 달 새 그야말로 롤러코스트를 타고 있는 것이다. 테슬라의 일론 머스크는 트위터를 통해 대중을 선동하는 듯한 글로 시세조종이라는 비난에 휩싸이기도 했다. 각국에 가상자산을 거래하는 시장이 엄연히 존재하지만, 사실 이러한 광풍은 미국과 한국에 특히 국한된다.

이처럼 가상자산 시장 규모를 거론하는 것은 사실 큰 의미가 없다. 자산의 성장에 따른 주식시장과 달리 가상자산은 클릭 한 번이면 바로 두 배, 세 배로 늘수 있는 데다 그 변동성도 심하기 때문이다.

이러한 시장에서 일부 기업은 크게 다음과 같은 네 가지 유형으로 수익을 탐색한다.

1 가상자산 중개업

가상자산 중개업은 가상자산을 사거나 팔려는 사람을 중개해서 그 수수료를 수입으로 얻는 사업이다. 대개 증권사의 HTS를 흉내 낸 시스템을 갖추고, 각종 가상자산의 입출금이 가능한 소위 '지갑' 소프트웨어를 차려두고 영업을 한다.

가상자산 중개업은 대부분 전문 중개업체에 의해 이루어지고 있고 코인베이스나 바이낸스 등 일부 대형 중개소가 거의 대부분 시장을 차지하고 있으나, 최근에는 다양한 업종에서 이 시장을 넘보고 있다. 대표적인 것이 페이팔과 싱가포르의 최대 상업 은행인 DBS이다. 이들은 이미 확보한 자사의 다수 회원을 대상으로 손쉬운 가상자산 매매를 알선하여 수수료를 챙기려는 목적을 가지고 있다.

페이팔은 자사 고객이 물품을 살 때 비트코인으로 바로 결제할 수 있는 서비스를 제공하겠다고 밝혔다. 그러나 물품 판매자는 당연히 법정화폐를 절대적으로 더 선호할 것이며, 비트코인 등을 사용할 경우의 불편함과 비용의 과도함, 가격의 불안정 등을 고려하면 비트코인을 결제용으로 사용하는 것은 사실상 실효성도 없고 합리적이지도 않다. 이 때문에 사실상 페이팔이 제공하는 서비스는 단순히 비트코인을 달러 등 법정화폐로 환전하는 서비스를 제공하는 것으로 마케팅에 불과하며, 판매자나 구매자 모두에게 비합리적인 수단일 뿐이다. 이들이 기존 중개소 시장에 어떤 영향을 끼칠 수 있을지는 미지수이다. 결제수단으로써 더 편리하고 뛰어나서 비트코인을 사용하는 것이 아니라, 많은 불편과 비용을 감수해야 하기 때문이다.

2 커스터디 서비스

두 번째 유형은 가상자산의 보관 및 관리 서비스이다. 이를 보통 커스터디(Custody) 서비스라고 부르며, 우리말로는 수탁 서비스라고 할 수 있다. 주된 비즈니스 모델은 고객의 가상자산을 비교적 안전하게 보관하고 관리하는 서비스를 제공하는 것이다. 이런 서비스가 필요한 이유는 통상 중개소의 보안이 허술한 데다 가상자산의 경우 해당 키를 분실하면 다시는 회복할 수 없다는 치명적인 약점이 있기 때문이다. 커스터디 서비스에서는 대개 소위 콜드 월렛[145]을 제공하여 해킹으로부터 비교적 안전하게 가상자산을 보관한다.

145) 콜드 월렛은 6장 마지막 부분을 참고하라.

국내 은행들은 은행법상 법정화폐가 아닌 가상자산을 직접 수탁하지는 못하므로, 직접적으로 커스터디 서비스를 제공하는 대신 커스터디 서비스를 제공하는 회사에 우회적으로 지분을 투자하는 방식을 택했다. 한편 커스터디는 단순 보관 이외에도 보관 기간에 따라 이자를 코인으로 지급하기도 한다.

이러한 서비스는 중개서비스에 비해 자금 세탁 등의 시빗거리가 없어 제공자 입장에서는 비교적 위험 부담이 덜한 편이지만, 각국의 관계 법령과 가상자산 시장의 변동성에 즉각적으로 영향을 받을 수 있다.

3 코인의 직접 발행

또 다른 유형은 직접 코인을 발행하는 것이다. 국내에서도 대기업의 자회사를 비롯한 많은 중소 기업이 코인을 발행했다. 이들이 코인을 발행한 후 중개소를 통해 어느 정도의 자금을 조달했는지는 명확하지 않으나, 이러한 방식의 자금 조달은 불로소득에 해당하므로 향후 문제의 소지가 될 수 있다.

현재 기업들이 코인을 발행하는 것에 관한 별도의 규정은 없다. 2021년 6월 미국에서는 증권거래위원회(SEC)가 소위 알트코인의 대표 격인 리플을 상대로 증권법 위반 혐의에 대해 소송을 진행하고 있다. 그 판결 결과에 따라 대부분의 코인이 증권법 위반으로 처벌될 가능성도 배제할 수 없으며 그 경우 국내에도 큰 영향이 미칠 수 있다.

4 직접 투자

기업들이 가상자산을 통해 이익을 취하는 네 번째 방법은 직접 혹은 간접 투자를 하는 것이다. 앞서 잠시 언급한 일론 머스크의 테슬라가 비트코인에 투자했다는 이야기는 다들 들어

보았을 것이다. 그러나 변동성이 극심한 가상자산에 기업의 자금을 투자하는 것에 대해서는 여전히 찬반 의견이 분분하며 가상자산 시장의 사회적 가치에 대한 논란도 뜨겁기에, 경우에 따라서는 기업의 가상자산 투자가 평판 리스크로 이어질 수도 있다.

한편, 가상자산과 관련된 사업은 가상자산을 직접 개발하거나 이를 유통 또는 중개하는 업이 대부분이다. 일부 국가에서는 가상자산을 기초자산으로 하는 파생상품도 판매하는 등 가상자산의 금융상품화를 시도하기도 하였다. 그러나 이 분야는 전술한 대로 각국이 가상자산에 대한 법령을 어떻게 정비하느냐에 많은 영향을 받을 수밖에 없다.

또한 가상자산의 단순거래에만 머물던 시장에서 이를 다양한 용도로 활용하려는 시도도 있다. 대표적인 것이 소위 유틸리티 토큰 등인데, 발행된 토큰의 용도를 특정 서비스의 구매용으로만 제한하는 경우이다. 유틸리티 토큰은 중개소를 통한 무분별한 거래에 따른 부작용은 사라지고 공급되는 서비스나 재화의 구매용으로서 가치를 가지게 되므로 기존의 가상자산과는 기능이 다를 수 있다. 영국은 유틸리티 토큰을 가상자산의 범위에서 제외하고 있다.

향후 디지털 관련 자산 시장은 크게 두 가지 시장으로 분류될 수 있고 이들에 대한 전망은 크게 다를 수 있다.

첫째는 블록체인을 사용하고 중개소를 통해 유통하는 것을 목적으로 하는 가상자산 시장이다. 이러한 가상자산은 내재가치가 0이며 오로지 수요와 공급에 의해 외부에서 가치가 주입되어야 한다. 이 시장은 각국의 가상자산의 규제방향에 따라 크게 영향을 받을 것이다.

둘째는, 지역화폐, 유틸리티 토큰, 기타 선불 토큰처럼 미리 정해진 가치를 가지고 잘 정비된 중앙 서버의 데이터베이스를 통해 발행되는 디지털화 자산이다. 이 형태는 핀테크의 전형적인 형태이므로 각국의 가상자산 법령 정비와 관련 없이 보다 다양한 형태로 나타나며 금융당국의 지원을 받을 것이다. 다만 각국의 가상자산 정의에 따라 이러한 디지털화 자산을 가상자산이라는 범주에 포함시키지 않는 국가도 상당수 있을 것이다.

[가상자산의 범위] 특정금융정보법상의 범위

현행 특정금융정보법은 가상자산을 '경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자증표'라는 포괄적 의미로 규정한 다음, 여기서 제외되는 항목을 6가지 목을 통해 열거하고 있다. 예컨대 선불카드, 전자화폐, 전자증권, 전자어음, 전자선하증권, 게임 아이템은 제외한다고 되어 있다. 이 법은 향후 시행령 제정 등을 통해 보다 세분화될 것이며 그에 따라 가상자산의 범위도 보다 구체화될 것이다.

제5절

블록체인 사례분석

시중에서 블록체인 프로젝트로 알려진 몇 가지 사례를 통해 그 의의와 맥락을 살펴보도록 하자.

1-1 뱅크사인

뱅크사인은 블록체인을 기반으로 은행권 공동 인증 서비스 구축을 표방하면서 2018년 8월 27일 공식 출범한 서비스이다. 이 프로젝트의 핵심은 기존의 공인인증서를 대신하여 범은행권에서 사용할 수 있는 새로운 공용 인증 서비스였고 18개 시중 은행 중 15개 은행이 참여했고, 카카오뱅크, 시티뱅크, 산업은행은 참여하지 않았다. 2021년 6월 기점으로는 산업은행도 참여하여 모두 16개 기업으로 늘었다.

아키텍처의 형태는 소위 컨소시엄 블록체인으로서 패브릭에 기반한 삼성의 넥스레저를 사용한 것으로 알려졌다. 이 프로젝트는 은행권이 컨소시엄을 이루어 공동으로 사용할 인증서를 관리하자는 데 합의했다는 점에서 그 의의를 찾아볼 수 있다. 그러나 금융결제원이 제공하는 생체인증을 통한 공동 인증 서비스 또는 오픈 API를 통한 컨소시엄 형태의 공동 인증 등 다양한 대체 수단이 존재한다는 점에서는 이 프로젝트의 상대적 장점이 무엇인지 서로 비교해 보는 것도 필요해 보인다. 또한 이 프로젝트는 블록체인 프로젝트라는 명칭보다는 오히려 컨소시엄 네트워크 프로젝트라는 것이 기술적으로 더 적절한 용어로 보인다는 지적도 있다.

1-2 K생명의 소액 보험금 지급시스템

K생명은 2017년 말 소액보험금을 간편 지급하기 위해 블록체인을 사용한다고 홍보했다. 이 프로젝트의 의의는 그간 보험사가 소극적으로 꺼려하던 보험금 지급을 자발적으로 간소화하는 시도를 했다는 측면이다.

그러나 소액 보험금 지급의 핵심은 진료 데이터라는 개인정보를 보험사로 바로 전송할 수 있느냐와 그 데이터를 보험사가 신뢰할 것인가에 관한 것이며, 이는 디지털기술보다는 법이나 보험사 사내 보험금 지급 규정과 깊은 관련이 있다. 따라서 이를 블록체인으로 어떻게 개선했다는 것인지에 대해서는 다소 모호해 보인다. K생명은 간편 인증기술을 위해 블록체인과 IoT를 활용했다고 설명했는데, 그것만으로는 보편적이고 안전한 기존 방식과의 차이가 무엇인지 알기 쉽지 않다.

여하간 그 기저 아키텍처와 상관없이 금융권에서 먼저 소비자를 위해 디지털기술을 이용해 각종 절차를 간소화하려는 적극적이고 다양한 시도가 보다 많이 나와야 할 것으로 보인다.

1-3 호주의 전력 직거래

호주의 P사는 블록체인을 활용해 전력 직거래 비용을 획기적으로 낮추었다고 주장한다. 이 회사가 발행한 백서를 살펴보면 자신들의 시스템을 하이브리드 블록체인으로 설명하고 있는데 퍼블릭 블록체인은 이더리움의 ERC-20 토큰을 발행한 부분이고, 나머지 부분은 프라이빗/컨소시엄 블록체인으로 구성됐다고 설명하고 있다. 그러나 이 회사가 직거래 비용을 낮출 수 있게 된 이유는 백서나 회사 홈페이지에서는 찾아보기 힘들다.

이 회사는 POWR이라는 코인을 10억 개 발행하여 중개소에서 판매 중이며 홈페이지를 통해서는 코인을 할인판매하고 있다. 이 토큰의 상당수는 한국에서 거래되고 있다.

1-4 사례를 통해본 블록체인 프로젝트의 핵심

앞서 시중에서 많이 거론되는 3가지 블록체인 사업을 살펴보았다. '왜 보다 실증적이고 구체적인 사례를 설명해 주지 않는가' 하는 의문도 들겠지만 아쉽게도 보편적으로 인정받는 블록체인의 실제 효용 사례가 나타날 때까지는 좀 더 시간이 필요해 보인다. 월마트의 이력추적 시스템이나 국제 무역 간편화 시스템 등을 들어 봤겠지만 그들 모두 단순히 디지털화의 효용에 블록체인이라는 마케팅 용어를 붙인 것에 더 가깝다는 지적이 많다.

다양한 블록체인 프로젝트들이 시중에 등장하고 있지만 새롭게 제안된 시스템이 기존 방식보다 왜 더 우수한 것인가라는 본질에 대한 설명을 명확히 보여주는 사례는 찾아보기 힘들다.

또한 규정과 제도의 개선을 통해 문제를 해결한 것을 마치 블록체인이라는 소프트웨어로 해결한 것처럼 호도하는 경우도 적지 않다. 일부 사례집은 시범사업자들의 일방적 주장을 여과 없이 그대로 옮겨 싣는 수준에 그치는 경우도 있는데, 그러한 나열은 도움이 아니라 오히려 혼란만 더 일으킬 수 있다.

새로운 기술이 등장하고 발전하기 위해서는 건전한 비판과 토론을 통해 단점이 보완되고 장점을 살려야 하며 가장 먼저 무엇을 위한 기술인지 그 '목적성'을 뚜렷이 해야 한다. 블록체인은 지금까지 그러하지 못했다.

1-5 기술의 정확한 특정

시중에는 블록체인의 실증사례를 찾기 위한 많은 프로젝트들이 진행되고 있다. 그러나 실증사업이란 기술이 특정되었을 때 이를 증명해 보는 사업을 의미하는 것이지 정체가 모호한 기술의 용처를 찾기 위해 다양하게 응용해 보는 것을 의미하는 것이 아니다. 실체를 특정하기 전의 블록체인 실증사업이란 개념증명(Proof of Concept)이 아니라 돈 낭비가 될 수 있다. 블록체인이라는 명칭을 사용하는 기술이 있는데 그 용도를 모르겠으니 그 사례를 찾아보겠다는 식의 주객전도가 될 수 있는 것이다.

따라서 실증사업 전에 반드시 선행되어야 할 과정은 먼저 블록체인의 정의를 명확히 내리고 육성해야 할 '기술'이 무엇인지 최대한 구체적으로 특정하는 것이다. 이러한 선제적인 과정을 거치지 않은 상태에서의 블록체인 프로젝트는 그 의미가 퇴색될 수 있다.

가상자산의 광풍과 블록체인이라는 기술 거품을 겪으면서 우리는 사람들이 원하는 진정한 효용이 무엇인지에 대해 많이 알게 되었다. 필요한 것은 사람들이 원하는 것을 해결해 주는

기술을 찾는 것이다. 블록체인이라는 단어에 매몰되지 말고 사람들이 원하는 '니즈'라는 관점과 그를 해결해 줄 수 있는 구체적인 기술에 보다 집중해야 할 것이다.

기술은 그 자체가 목적이 아니라 효용을 위한 수단일 뿐이다. 수단과 목적을 구분하고 사람들이 원하는 효용의 해결이라는 본질에 집중할 때 비로소 블록체인의 본질을 찾을 수 있을 것이다.

핵심정리

- 블록체인 정책 및 산업동향
  - 금융위원회 주도의 한국핀테크지원센터를 통한 다양한 정부 지원사업과 과학기술정보통신부의 블록체인 중장기 기술개발 지원사업이 진행 중이다.
  - 산업계에서의 블록체인은 SI를 근간으로 하는 개발부분이 주를 이루고 있고, 금융계에서는 비트코인으로부터 촉발된 여러 유관 개념들의 파생이 주가 되고 있으며 그 대표적인 것이 디지털화된 자산과 디지털 자산이다.
  - 향후에 블록체인의 기술적 정의가 보다 명확해지고, 가상자산에 대한 정의가 보다 뚜렷해지면 각 산업계에서 다양한 아이디어가 등장하게 될 것이다.
  - 블록체인이라는 단어에 매몰되지 말고 고객의 필요성에 집중하여 기술은 그 자체가 목적이 아니라 효용을 위한 수단이라는 점을 잊지 말고 보다 구체적인 기술에 집중해야 인류를 위한 보다 진보된 기술이 등장할 것이다.

헬로, 핀테크!(보안인증 · 블록체인)

10장

전통적 관점의 컴플라이언스 이해

제1절 전통적 관점의 금융회사 컴플라이언스 개념

제2절 금융회사 컴플라이언스 업무 특징

제3절 컴플라이언스 업무체계 및 시스템화

제4절 컴플라이언스 실무

10장 전통적 관점의 컴플라이언스 이해

학습목표

1. 컴플라이언스(Compliance)의 역할과 책임을 설명할 수 있다.
2. 내부감사(Internal Audit)와 컴플라이언스의 차이를 설명할 수 있다.
3. 컴플라이언스 실무 프로세스를 이행할 수 있다.

학습개요

금융회사는 전통적으로 국가 재정의 대동맥 임무를 수행해 왔다. 그래서 다른 어떤 산업부문보다 신뢰가 중요하며, 그 신뢰의 밑바탕은 컴플라이언스 업무에 의해 이루어졌다 하여도 과언이 아니다. 컴플라이언스는 기업의 영속을 위해 반드시 필요하며, 최근에 강조되고 있는 윤리경영 및 사회적 책임을 고려할 때도 중요하다. 또한, 컴플라이언스 부서는 금융회사 내의 이사회, 감사위원회, 경영진과 준법감시인 등 회사 내 거버넌스(Governance) 조직과 협력하여 기업의 건전성을 지켜내야 한다. 이 장에서는 컴플라이언스의 개념을 알아보고, 컴플라이언스의 유형 및 특징, 컴플라이언스 구조(Structure)와 업무 등에 대해 개괄적으로 알아본다.

용어해설

❶ 컴플라이언스

기업이나 단체가 사업 연속성과 경영 투명성을 확보하기 위하여 자율적 · 법률적으로 여러 가지 규제(Regulations)를 준수하는 것을 말한다. 최근에는 일반적인 규제 준수 외에도 기업 윤리(Ethics)와 사회적 책임(CSR; Corporate Social Responsibility)까지도 컴플라이언스 영역에 포함한다.

❷ 준법감시인(Compliance Officer)제도

금융회사 등은 「금융회사의 지배구조에 관한 법률」(약칭: 금융사 지배구조법) 제25조(준법감시인의 임면 등)에 의거하여 내부통제기준의 준수 여부를 점검하고 내부통제기준을 위반하는 경우 이를 조사하는 등 내부통제 관련 업무를 총괄하는 사람(준법감시인)을 1명 이상 두어야 한다.

❸ 내부통제기준

내부통제기준으로는 '윤리강령 및 행동강령', '선량한 관리자로서의 주의 의무'와 기타 명칭에 상관없이 위에서 규정하지 아니한 모든 규정(Regulations)을 말한다.

제1절

전통적 관점의 금융회사 컴플라이언스 개념

1 컴플라이언스 개념

1-1 컴플라이언스 정의와 도입 배경

가. 컴플라이언스의 정의

● 컴플라이언스 일반적 정의

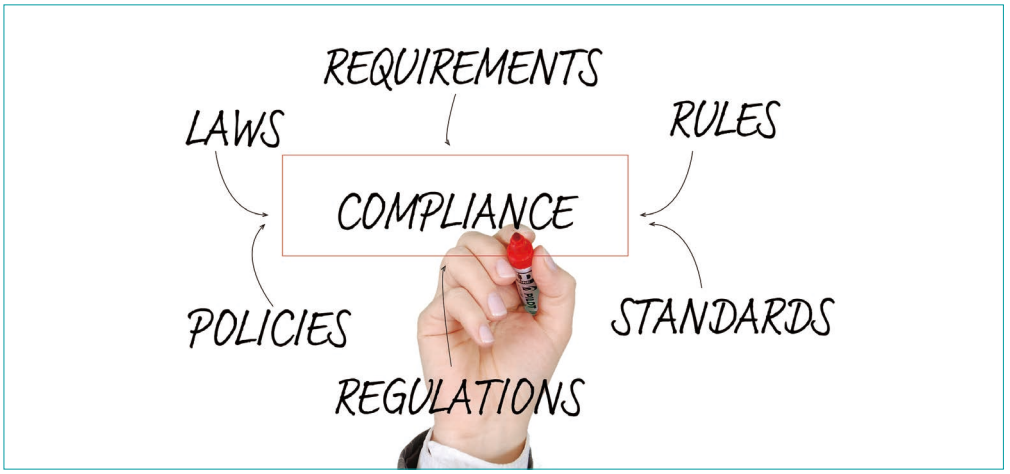
기업이나 단체가 사업 연속성과 경영 투명성을 확보하기 위하여 자율적 · 법률적으로 여러 가지 규제(Regulations)를 준수하는 것을 말한다. 최근에는 일반적인 규제준수 외에도 기업윤리(Ethics)와 사회적 책임(CSR; Corporate Social Responsibility)까지도 컴플라이언스 영역에 포함한다.

● 컴플라이언스의 정의

금융감독원에서 제정한 '은행 준법감시인 제도운영 모범규준'에 의하면, 준법감시(Compliance)란 일반적으로 고객자산의 선량한 관리자로서 회사의 임직원 모두가 제반 법규를 철저히 준수하도록 사전 또는 상식적으로 통제 · 감독하는 것을 말한다.[146)]

146) 금융감독원, 은행 준법감시인 제도운영 모범규준, 2006, p. 3

〈그림 X-1〉 컴플라이언스



출처: 픽사베이(Pixabay)

나. 컴플라이언스 오피서(Compliance Officer, 준법감시인) 제도의 도입 배경

● IMF 외환위기에 대한 반성

우리나라는 1997년 IMF 외환위기를 겪으면서 이에 대한 원인이 기업경영과 금융부실에 있다는 것이 드러나게 되었다. 이에 따라 금융기관에 대한 효과적인 감독체계가 중요함을 인식하고 금융 전(全) 부분에 대한 규제의 완화 · 구조조정 및 개방화가 진전되면서 금융기관의 내부통제 강화를 위한 선진화된 준법감시제도를 국내 도입하려는 분위기가 조성되었다[147].

● 준법감시인 제도

금융회사 등은 「금융회사의 지배구조에 관한 법률」(약칭: 금융사 지배구조법) 제25조(준법감시인의 임면 등)에 의거하여 내부통제기준의 준수 여부를 점검하고 내부통제기준을 위반하는 경우 이를 조사하는 등 내부통제 관련 업무를 총괄하는 사람(준법감시인)을 1명 이상 두어야 한다. 준법감시인은 필요하다고 판단하는 경우 조사 결과를 감사위원회 또는 감사에게 보고할 수 있으며, 금융사 지배구조법에 따라 임기를 2년 이상 보장받고 있다.

147) 정병석, 사법제도 개혁추진위원회 자료집, 기업의 준법관리제도 도입방안, 2007, p. 268

2 컴플라이언스 부서의 역할과 책임

2-1 조언(Advice & Guidance)

가. 법률 및 감독규정(법규) 제정 및 개정 내용을 조사한다.

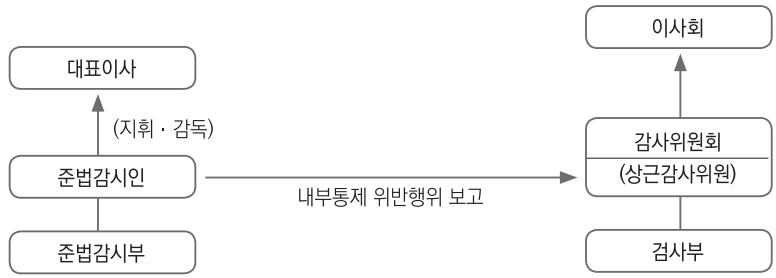
나. 법규 분석 및 내규에 적용한다.

다. 업무절차를 개선한다.

라. 법률 검토 및 해석한다.

마. 법규준수를 위한 자가진단 절차를 운영한다.

〈그림 X-2〉 시중 A 은행의 상근감사위원과 준법감시인의 위치



2-2 교육(Training & Education)

법규준수를 위한 교육 프로그램 마련 및 운영

2-3 사전검토 및 모니터링(Review & Monitoring)

가. 일상 업무 관련 내부통제 또는 법규준수 측면에서 사전검토를 수행한다.

나. 사전검토 의견 제시 및 피드백을 수행한다.

다. 임직원의 내부통제기준 위반 여부를 점검하고 조사한다.

2-4 보고(Reporting)

가. 준법감시 활동계획 및 실적을 경영진과 감사위원회에 보고한다.

나. 감독기관에 보고한다.

3 컴플라이언스 업무 영역

3-1 모범규준상 준법감시인의 직무

가. 준법감시인은 내부 통제기준의 준수 여부를 점검하고, 동 업무의 원활한 수행을 위하여 적정한 준법감시 조직 및 인력을 확충하여야 한다.

나. 활동 결과를 상근감사위원(감사위원회)에 보고하여야 한다.

3-2 『내부통제기준』의 해석

가. 법령준수

법령준수는 '법률'과 '명령'을 준수하는 것을 말한다. '법률'에는 법령, 해당 법의 시행령과 시행세칙을 말한다. '명령'은 명령과 조례 등으로 구성되며 정부 또는 지방자치단체가 제정한 모든 제한 규정을 말한다.

나. 법규준수

법규준수는 '감독규정'과 '내규'의 준수를 말한다. '감독규정'에는 규정, 시행세칙, 지도 공문 및 요구 등 그 명칭에 상관없이 감사원, 공정거래위원회, 감독기관, 국회 또는 한국은행 등 금융회사 등에 대하여 감독기관의 성격을 가지고 있는 모든 기구의 규정(Regulations)을 말한다. 또한, '내규'는 회사나 조직 내부에서 정한 내규, 지침과 업무 편람 등을 의미한다.

다. 내부통제 기준준수

내부통제 기준으로는 '윤리강령 및 행동강령', '선량한 관리자로서의 주의 의무'와 기타 명칭에 상관없이 위에서 규정하지 아니한 모든 규정(Regulations)을 말한다.

제2절

금융회사 컴플라이언스 업무 특징

1 컴플라이언스 일반론

1-1 통제 원칙

가. 업무의 기능적 분리, 책임의 명확화, 회계자료의 정확성 및 신뢰성 확보, 복수 관리, 상호대사가 이루어져야 한다.

나. 신상품 등 새로운 업무를 개발 또는 취급하는 경우 법규준수 및 내부통제의 적정 여부가 사전에 검토되어야 한다.

다. 관계 법령, 감독규정 등이 변경될 경우 관련 내용을 신속하고 적절하게 내규에 반영하여야 한다.

1-2 관련 책임

가. 전제: 이사회와 경영진의 지배구조를 가진 은행에 적용(The Basel Committee, 2005)

나. 은행의 컴플라이언스에 대한 1차 책임은 경영진과 사업본부장(Management and Line Manager)에게 있다.

다. 소관부서의 관련 법규 인식 및 질의에 대한 해석의 책임은 법규 부서(법무팀; Legal Service 부서)가 담당한다.

라. 은행의 재무 위험(신용, 시장, 유동성 리스크) 모니터링과 각 정책과 한도 준수 여부 확인은 위험통제 부서가 담당한다.

2 컴플라이언스와 내부감사 업무의 비교

2-1 범위와 업무 형태

컴플라이언스 업무는 「금융회사의 지배구조에 관한 법률」(약칭: 금융사 지배구조법)에 의거하여 수행하며, 감사와 감사위원회 업무는 「상법」을 근거 법으로 한다. 아울러, 컴플라이언스는 사고 예방에 무게중심을 두고 있지만, 내부감사는 엄격한 내부징계를 통해 사고억제(Deterrence)에 무게중심을 두고 있다.

〈표 X-1〉 제무제표감사, 업무감사, 준법감사의 상호 비교

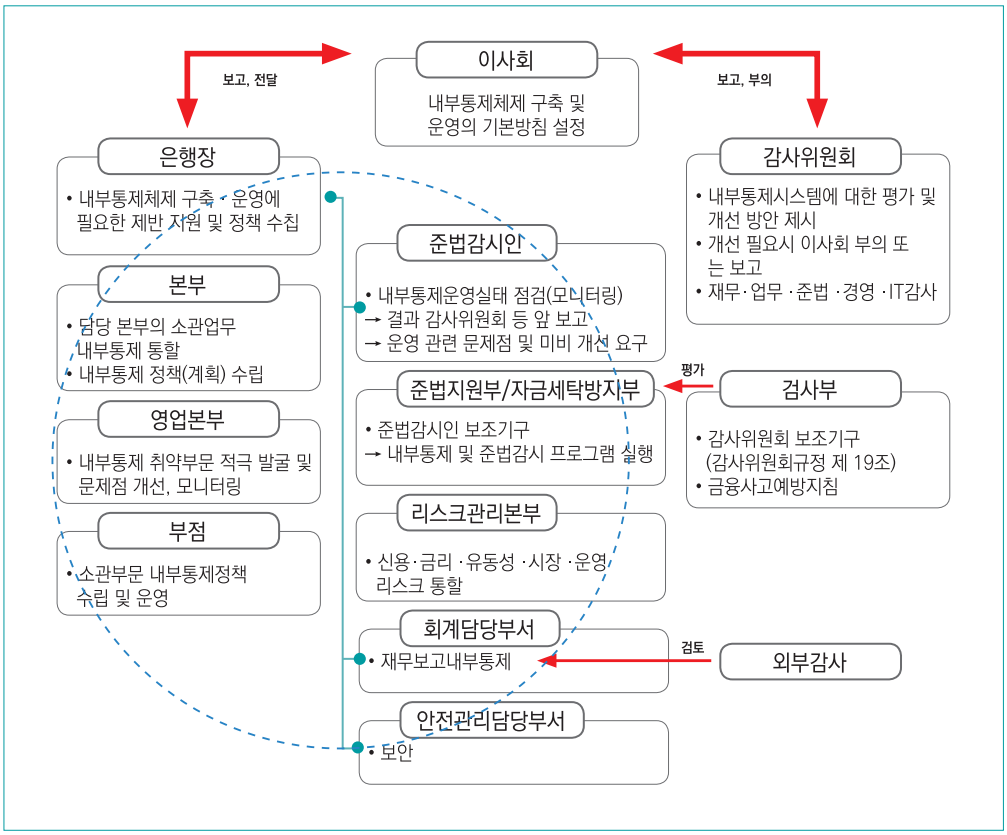
	재무제표감사 (audit of financial statements)	업무감사 (operational audit)	준법감사 (compliance audit)
감사목적	재무제표의 공정표시 여부를 결정 (fair presentation)	업무의 효율성과 효과성을 평가 (efficiency and effectiveness)	법규·규정 사항의 준수여부를 결정 (compliance)
평가기준	일반적으로 인정된 회계원칙	사전에 정해진 업무목표	법규·절차·규정의 내용
감사인	독립성을 갖춘 전문감사인, 주로 공인회계사	외부·내부감사인	외부·내부감사인
감사보고서이용자	불특정 다수	주로 내부경영진	주로 내부경영진 및 상급규제기관
주감사기능	비판적 기능	지도적 기증	감시적 기능
사례	회계법인의 상장회사에 대한 재무제표감사	기획재정부의 공기업 경영평가	국세청의 법인세 세무조사

출처: 이효익 · 김한수 · 이종은(2018), New ISA 회계감사, 신영사

2-2 거버넌스의 3중 구조

일반적인 금융회사 등의 거버넌스는 〈그림 X-3〉에서 보는 것처럼 「주식회사 등의 외부감사에 관한 법률」(약칭: 외부감사법)에 따른 '감사인'과 「은행법」에 따른 '감사위원회'와 「금융회사의 지배구조에 관한 법률」(약칭: 금융사 지배구조법)에 따른 '준법감시인'의 3중 구조로 되어 있다.

〈그림 X-3〉 거버넌스 부서의 업무 및 보고 체계



3 리스크 유형별 컴플라이언스 역할

3-1 단위 리스크(Risk)별 대응 조직

가. 재무(Finance) 리스크

재무 리스크는 '시장 및 금리 위험', '유동성 위험', '신용 및 신용편중 위험', '결제 위험', '운영 위험' 등이 있으며, 조직 내에서 리스크관리그룹 및 자금시장 그룹이 담당한다.

나. 전산 시스템(IT System) 리스크

전산 시스템의 개발 및 관리에 대한 모든 위험을 말하며, 조직 내에서 전산 담당(ICT; Information and Communications Technologies) 그룹이 담당한다.

다. 법률적 리스크(Regulation Risk)

조직 내의 모든 법률적 위험의 사전적 자문과 사후적 송무(訟務)에 수반되는 모든 위험을 말하며, 준법지원부와 법무부서가 담당한다. 법무부서는 독립된 부서 또는 준법지원부 소속 법무팀으로 존재하기도 한다.

라. 평판 리스크(Reputation Risk)

모든 언론 및 인터넷 등 소셜 네트워크상에서 조직에 대한 부정적인 평판위험을 말하며, 홍보부와 관련 유관부서에서 담당한다.

마. 재무보고(내부회계) 통제 리스크(Accounting Risk)

외부에 공시하는 사업보고서 등의 재무 자료뿐만 아니라, 내부 관리 회계가 부정확함으로써 발생하는 위험을 말한다. 주로 회계(Accounting)부서에서 담당한다.

바. 부정 리스크(Fraud Risk)

조직 내 구성원들의 조직적 또는 개인적 일탈 행위로 발생하는 부정(Fraud)에 관한 위험으로서 발생 시 평판위험은 물론 재무 위험도 발생할 수 있다. 담당 부서는 검사부, 감찰부, 인사부 및 준법지원부 등이 있다.

사. 보안 리스크(Security Risk)

은행 등과 같이 조직 내에 물리적 재화를 보관하는 기업뿐만 아니라, 특허 및 음원 자료 등 디지털 자산을 보관할 경우 발생하는 위험으로서 안전관리부 및 정보보호부 등이 담당한다.

제3절

컴플라이언스 업무체계 및 시스템화

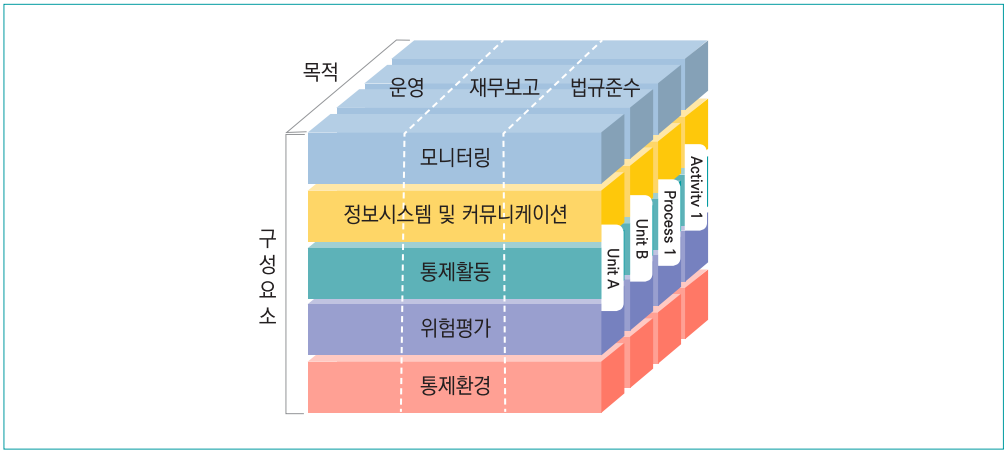
1 컴플라이언스와 내부통제 업무체계

제1절에서 모범규준상 준법감시인의 직무 중 준법감시인은 '내부통제' 기준의 준수 여부를 점검하여야 한다고 기술했다. 제3절에서는 내부통제는 무엇이며 무엇을 목적으로 하고 내부통제를 달성하기 위한 구성 체계 및 시스템에 대하여 알아본다.

1-1 내부통제의 정의

내부통제는 재무 보고의 신뢰성, 경영의 효과성 및 효율성, 관련 법규준수에 관련된 기업의 목적달성에 관한 합리적인 확신을 제공할 목적으로 지배기구, 경영진 및 기타 인원이 설계, 실행, 유지하는 모든 절차를 말한다.

〈그림 X-4〉 내부통제의 구성요소



출처: COSO(Committee of Sponsoring Organizations of the Treadway Commission)

1-2 내부통제의 목적

가. 기업경영의 효과성과 효율성

기업의 컴플라이언스 목표 달성을 위한 효과성과 기업 자원의 중복 및 자원 낭비 및 비능률을 사전에 방비하고 조정한다.

나. 재무 보고의 신뢰성

정교하고 정확한 재무 시스템의 설계와 운용을 통하여 대내외적인 이해관계자에게 보고하는 재무 보고서의 정확한 기록 및 문서를 통제한다.

다. 관련 법규의 준수

조직과 관련된 다수의 법규준수를 위한 통제 절차 설계와 운영을 수행한다.

1-3 내부통제의 한계

가. 인적 오류(Human Error): 의사 결정 과정에서 사람의 판단이 잘못될 가능성을 말한다.

나. 개인적 부주의(Personal Carelessness): 개인적 부주의로 인해 내부통제가 와해할 위험을 말한다.

다. 공모(Collusion): 2명 이상이 공모할 가능성을 말한다.

라. 경영진의 무시(Management Override): 경영진의 내부통제 유린으로 인하여 무력화될 가능성이 존재한다.

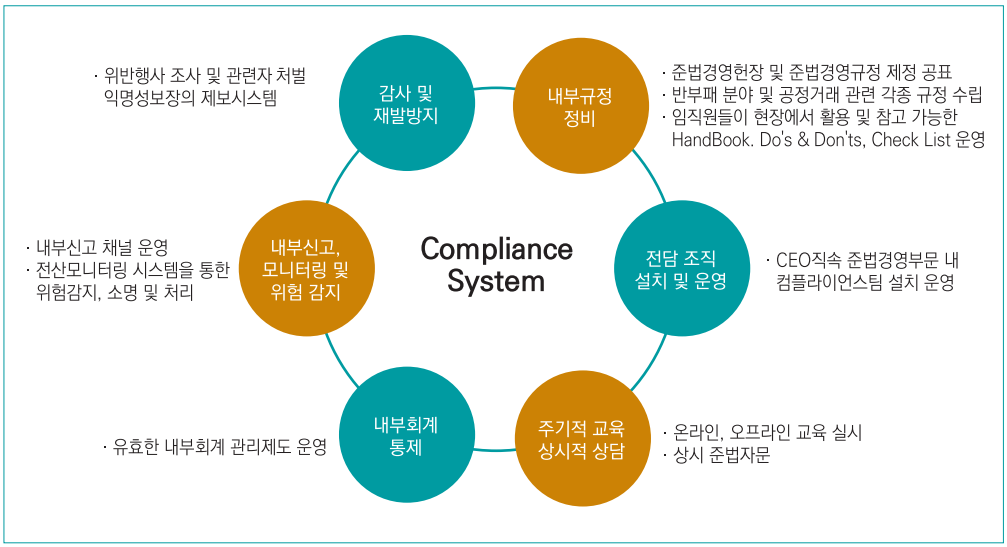
마 일상화(Routinization): 대부분의 내부통제는 일상적인 거래를 대상으로 한다.

바. 진부화(Obsolescence): 거래 여건은 변화하는데 기존의 통제 절차는 오래되거나 부적절하게 되어서 통제 준수가 쉽지 않게 될 가능성이 존재한다.

2 컴플라이언스 업무의 시스템화

컴플라이언스 시스템을 그림으로 표현하면 다음과 같다. 국내 기업 L회사의 예시이다.

〈그림 X-5〉 컴플라이언스 시스템 예시



출처: L케미칼 홈페이지,
https://www.lottechem.com/kor/management/compliance/contentsid/872/index.do

2-1 컴플라이언스 시스템의 구축 목적

컴플라이언스 시스템의 구축 목적은 조직 내의 모든 임직원이 준수해야 할 내부통제 절차를 종합적으로 관리할 시스템을 만들어 조직 구성원의 위법행위를 사전에 예방하는 것이다.

2-2 컴플라이언스 시스템의 6요소

가. 내부통제 규정 수립

부서별 업무 및 관련 규정을 검토하여 임직원이 준수해야 할 내부통제 기준을 수립한다.

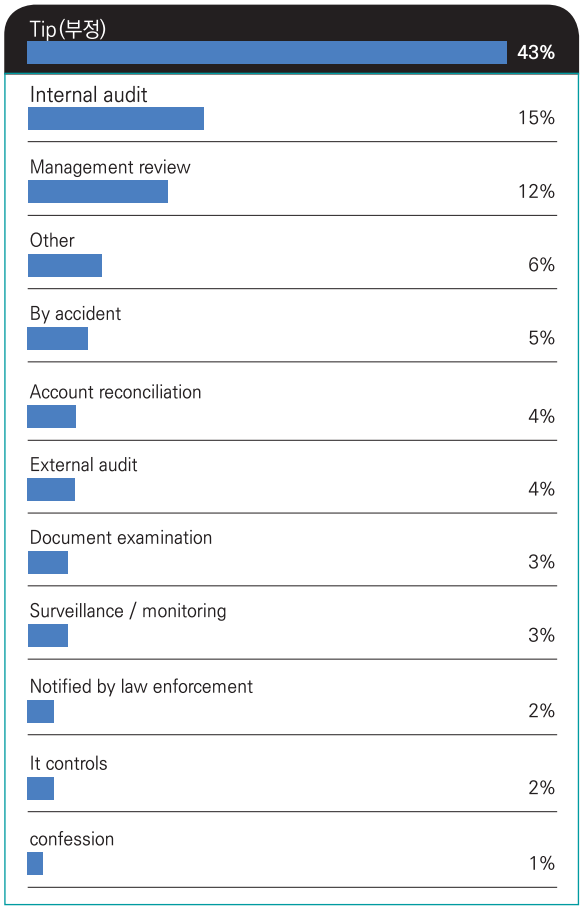
나. 임직원을 위한 교육 및 상담 프로그램 운영

임직원이 내부통제 기준을 숙지하고 이를 준수할 수 있도록 지속적인 교육 및 상담 프로그램을 운영한다.

다. 내부신고(Tip), 모니터링 시스템 구축 및 운영

내부통제 기준에 따라 모니터링 시스템을 구축하여, 임직원들이 내부통제 기준과 법규를 준수하는지를 시스템으로 종합 관리한다.

〈그림 X-6〉 부정이 최초에 어떻게 발견되는가?



출처: REPORT TO THE NATIONS 2020 GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE

라. 감사 및 위반 직원에 대한 제재

내부통제 위반 직원에 대해서는 제재와 시정을 요구하고, 관련된 사항을 이사회에 주기적으로 보고한다.

마. 전담조직 설치 및 운영

새로운 상품 및 서비스 출시 등 신규 사업내용 및 내외부 문서의 법규준수 여부 등을 사전 심의하고, 내부통제 기준 및 일상 업무 등에 대하여 법규 자문 역할을 수행한다.

바. 내부회계 통제

유효한 내부회계 관리 제도를 운용한다.

제4절 컴플라이언스 실무

1 준법감시담당자의 직무

1-1 준법감시담당자

가. 역할

준법감시담당자는 준법감시인 또는 각 조직 단위 부서장의 준법감시업무를 보좌하는 역할을 담당한다. 준법감시담당자는 소속 본부에 대한 내부통제 책임을 진 그룹장과 본부장이 소관 업무와 관련하여 법규의 적합성 점검 및 내규정비 업무를 보좌하여야 한다. 주요 업무는 다음과 같다.

- **내부통제계획 수립 및 점검**

  준법감시인 및 각 본부의 내부통제 계획의 수립 및 점검에 협조하여야 한다.

- **내부통제기준 준수 여부 점검**

  매주 1회 이상 내부통제 체크리스트를 점검하고 교육을 한다. 또한, 내부통제 위반을 발견하면 '내부통제(기준) 위반 보고서'를 제출한다.

- **내부통제 위반 발견 시 보고**

  내부통제를 위반한 사실을 발견하면 본부장 또는 준법감시인에게 보고하여야 한다. 미보고 시는 행위자와 동일하게 제재를 받을 수 있으니 주의하여야 한다. 내부통제 위반에는 '소송 발생, 윤리강령 위반, 법규위반과 위반이 우려되는 경우 또는 위반의 강요'도 포함된다. 금융사고의 유형에는 '횡령, 유용, 배임, 사기 도난, 피탈 등의 금전사고'와 '실명제 위반, 사금융알선, 금품수수, 사적 금전대차 등 금융질서 문란행위도 포함된다.

● 직원 상담 및 대응

준법감시담당자는 법규준수 의무 위반을 강요받거나, 위험을 인식한 직원을 대상으로 하여 구체적인 행동요령의 지도와 직원 법규상담 및 지도를 하여야 한다.

● 내부통제 또는 법규준수 1차 사전검토

준법감시담당자는 감독기관에 제출하는 서류의 일차적인 사전검토를 한다. 또한, 공시담당자가 공시대상 여부를 확인하였는지를 점검하여야 한다.

2 은행 준법감시인 제도 모범규준 개정(2015년 9월 시행)

2-1 준법감시인의 임기 및 지위

가. 사내이사 또는 업무집행 책임자 중에서 선임하고, 그 임기는 2년 이상 보장하여야 한다.

나. 준법감시인에게 발견된 위법사항에 대하여 업무정지 요구 권한 및 의무를 부여한다.

다. 필요시 이사회를 포함한 모든 업무 회의에 참여하여 적법성 등에 대하여 의견을 발언할 수 있다.

2-2 준법감시인의 독립성 확보

가. 준법감시인이 내부통제기준을 잘 지키고 있는지 점검하고 위반한 사실을 조사하여 감사위원회와 감사에게 보고할 수 있다.

나. 준법감시인은 원칙적으로 자산 운용에 관한 업무 등과 같이 이행상충 문제가 발생할 수 있는 업무와 내부통제 업무에 전념하기 어려운 업무는 겸직이 금지되어 있다.

2-3 전담조직 및 인력 지원

가. 은행은 준법감시인의 효과적 업무 수행을 위하여 적정수준의 내부통제 전담인력을 확보하여야 하며, 해당 인력을 은행 및 은행연합회 홈페이지를 통하여 알려야 한다.

나. 은행은 준법감시부서 직원의 인사발령 시 사전에 준법감시인과 협의하여야 하고, 준법감시부서에서 정당하게 수행한 컴플라이언스 업무를 이유로 인사상 불이익을 주어서는 안 된다.

2-4 내부통제위원회 구성 및 운영

가. 대표이사 직속으로 내부통제 조직(예 이사회, 대표이사, 준법감시인 및 준법감시부서 등) 간 협력 및 조정 업무를 수행하는 "내부통제위원회"를 설치하고 운영하여야 한다.

나. 대표이사는 준법감시인으로 하여금 이사회에 내부통제기준과 준법감시정책을 연 1회 이상 보고하도록 하여야 한다.

2-5 준법감시체제 구축 및 운영

가. 준법감시인은 자점검사와 금융사고 예방을 위한 상시감시시스템 구축하고 운영하여 각 부점에서 처리한 업무가 법규에 준하여 바르게 처리되었는지를 상시적으로 점검하여야 한다.

나. 영업점 자점검사 업무의 주관부서를 검사부에서 준법감시인 소속의 준법지원부로 변경하여 준법감시인의 준법감시업무의 효율성을 높였다.

다. 아울러, 준법감시인이 영업점의 자점검사 담당 직원에 대한 인사평가권을 부여하여 실질적인 영업점 준법감시 통제를 가능하게 하였다.

3 영업점 준법감시 모니터링

3-1 영업점 모니터링 목적

영업점은 모든 영업행위가 일어나는 장소이며 동시에 금융소비자와 만나는 접점이다. 즉, 영업점 모니터링은 내부통제의 시작이자 마지막 장소이다. 내부통제 부서뿐만 아니라 영업점 관리자(지점장)와 준법감시 담당자는 내부통제의 최일선 책임자이며 실행자임을 명심하고 최선을 다하여 영업점 모니터링과 주요 점검 항목을 점검하여야 한다.

3-2 영업점 모니터링 실시 및 주요 점검 항목

- □ ① 준법감시 체크리스트 점검
- □ ② 준법감시 교육보고서 제출
- □ ③ 내부통제의 날 실시 결과 보고서 제출
- □ ④ 재산상 이익 제공/수령 보고서 제출
- □ ⑤ 광고(홍보물) 제작 시 유의사항 점검
- □ ⑥ 임직원 윤리 · 법규준수 자가진단 수행
- □ ⑦ 임직원 금융투자상품 매매 신고서 제출
- □ ⑧ 미공개 중요정보 이용행위의 금지 점검
- □ ⑨ 내규에 따른 주요사안 보고
- □ ⑩ 내부자 제보 제도
- □ ⑪ 특이 거래 등 보고 절차 준수
- □ ⑫ 공시 관련 유의사항 점검
- □ ⑬ 임직원의 대외매체 등 접촉에 관한 내규 준수 점검
- □ ⑭ 불건전 영업행위 금지
- □ ⑮ 불공정 영업행위 금지

- ☐ ⑯ 신용공여 한도 및 절차 준수
- ☐ ⑰ 금융실명거래 및 비밀보장법 준수
- ☐ ⑱ 외환 업무 시 유의사항 점검
- ☐ ⑲ 방카슈랑스 판매인 법규 준수사항 점검
- ☐ ⑳ ISA 영업 관련 내부통제 절차 준수
- ☐ ㉑ 특정금전신탁 업무 시 유의사항 점검
- ☐ ㉒ 펀드(집합투자상품) 판매 시 유의 사항 점검
- ☐ ㉓ 퇴직연금 업무 유의사항 점검
- ☐ ㉔ 대출모집인(대출상담사) 업무처리 유의사항 점검
- ☐ ㉕ 카드 모집 관련 유의사항 점검
- ☐ ㉖ 행정정보 공동이용 유의사항 점검
- ☐ ㉗대외 제출 제 증명서 발급 시 유의사항 점검
- ☐ ㉘ 비정형 계약(약정)서 사용 시 유의사항 점검
- ☐ ㉙ 채권추심 관련 유의사항 점검

핵심정리

1. 전통적 관점의 금융회사 컴플라이언스 개념

- 컴플라이언스(Compliance)

  컴플라이언스란 기업이나 단체가 사업 연속성과 경영 투명성을 확보하기 위하여 자율적 · 법률적으로 여러 가지 규제(Regulations)를 준수하는 것을 말한다. 최근에는 일반적인 규제 준수 외에도 기업 윤리(Ethics)와 사회적 책임(CSR; Corporate Social Responsibility)까지도 컴플라이언스 영역에 포함한다.

- 컴플라이언스 통제 원칙

  업무의 기능적 분리, 책임의 명확화, 회계자료의 정확성 및 신뢰성 확보, 복수 관리, 상호대사가 이루어져야 하며, 신상품 등 새로운 업무를 개발 또는 취급하는 경우 법규준수 및 내부통제의 적정 여부가 사전에 검토되어야 한다. 아울러, 관계 법령과 감독규정 등이 변경될 경우 관련 내용을 신속하고 적절하게 내규에 반영하여야 한다.

- 내부감사와 컴플라이언스의 차이

  컴플라이언스 업무는 「금융회사의 지배구조에 관한 법률」(약칭: 금융사 지배구조법)에 의거하여 수행하며, 감사와 감사위원회 업무는 「상법」을 근거 법으로 한다. 아울러, 컴플라이언스는 사고 예방에 무게중심을 두고 있지만, 내부감사는 엄격한 내부징계를 통해 사고억제(Deterrence)에 무게중심을 두고 있다.

2. 금융회사 컴플라이언스 업무 특징

- 거버넌스의 3중 구조

  일반적인 금융회사 등의 거버넌스는 「주식회사 등의 외부감사에 관한 법률」(약칭: 외부감사법)에 따른 '감사인'과 「은행법」에 따른 '감사위원회'와 「금융회사의 지배구조에 관한 법률」(약칭: 금융사 지배구조법)에 따른 '준법감시인'의 3중 구조로 되어 있다.

3 컴플라이언스 업무체계 및 시스템화

- **내부통제의 정의**

  내부통제는 재무 보고의 신뢰성, 경영의 효과성 및 효율성, 관련 법규준수에 관련된 기업의 목적달성에 관한 합리적인 확신을 제공할 목적으로 지배기구, 경영진 및 기타 인원이 설계, 실행, 유지하는 모든 절차를 말한다.

- **내부통제의 3대 목적**

  내부통제의 3대 목적은 첫째, '기업경영(운영)의 효과성과 효율성', 둘째는 '재무 보고의 신뢰성'이며, 셋째는 '관련 법규의 준수'이다.

- **컴플라이언스 시스템(Compliance System)의 6요소**

  컴플라이언스 시스템을 구성하는 6요소는 다음과 같다. '내부통제 규정 수립', '임직원을 위한 교육 및 상담 프로그램 운영', '내부신고, 모니터링 시스템 구축 및 운영', '감사 및 위반 직원에 대한 제재', '전담조직 설치 및 운영', '내부회계 통제' 등으로 구성될 수 있다.

4. 컴플라이언스 실무

- **준법감시담당자의 역할**

  준법감시담당자는 준법감시인 또는 각 조직 단위 부서장의 준법 감시업무를 보좌하는 역할을 담당한다. 준법감시담당자는 소속본부에 대한 내부통제 통할 책임을 진 그룹장과 본부장이 소관 업무와 관련하여 법규의 적합성 점검 및 내규정비 업무를 보좌하여야 한다.

헬로, 핀테크!(보안인증 · 블록체인)

HELLO, FINTECH!

11장

레그테크 개요

제1절 레그테크 개념

제2절 레그테크 등장 배경

제3절 레그테크 구조 및 특징, 비즈니스 모델

제4절 국내외 레그테크 부문 핀테크 기업의 서비스 사례 분석

11장 레그테크 개요

학습목표

1. 레그테크(RegTech)를 정의할 수 있다.
2. 레그테크가 등장하게 된 배경을 설명할 수 있다.
3. 레그테크와 핀테크 산업과의 관계를 이해하고, 혁신기술이 어떻게 컴플라이언스 업무를 변화시킬 수 있는지 이해하고 설명할 수 있다.

학습개요

레그테크란, 규제(Regulation)와 기술(Technology)의 합성어로 규제 준수 및 규제 관련 활동을 기술로 혁신하고자 하는 움직임 또는 산업을 의미한다. 레그테크는 기술, 규제, 금융서비스와 핀테크(FinTech)를 상호 연결하여 각각의 강점을 살릴 수 있는 기술을 의미한다. 이 장에서는 이러한 레그테크의 정의에 대하여 알아보고, 국내외 추진 사례와 레그테크의 등장 배경 및 국내외 주요 레그테크 산업에 대해 알아본다.

용어해설

❶ 핀테크(FinTech)

핀테크란, 금융(Finance)과 기술(Technology)의 합성어로, 금융과 IT의 융합을 통한 금융서비스 및 산업의 변화를 통칭한다.

❷ FATCA(Foreign Account Tax Compliance Act)

미국의 해외금융계좌신고법. 미국 납세의무자의 역외탈세 방지를 위하여 2010년 도입한 법으로, 세계 금융회사들은 미국 납세자가 보유한 5만달러 이상의 계좌에 대한 정보를 미국의 국세청(IRS)에 의무적으로 보고하도록 하고 있다.

❸ 자금세탁방지제도(Anti-Money Laundering)

자금세탁방지제도란, 자금세탁과 밀접한 관련이 있는 전제범죄(前提犯罪, Predicate Offense)와 관련된 불법 자금세탁의 적발 및 예방을 하기 위한 법적, 제도적 장치를 말한다.

제1절

레그테크 개념

1 레그테크의 정의

1-1 사전적 정의

레그테크(RegTech)란, 규제(Regulation)와 기술(Technology)의 합성어로 규제 준수 및 규제 관련 활동에 초점을 맞춘 기술을 말한다. 레그테크는 기술, 규제, 금융서비스와 핀테크를 상호 연결하여 각각의 강점을 살려 AI를 활용해 복잡한 금융규제 준수 관련 업무를 자동화 · 효율화하는 기술이다.

〈그림 XI -1〉 레그테크 구성 요소

출처: Bloomberg, How RegTech closes the gap between technology and financial services

1-2 산업적 정의

가. '레그테크'는 규제와 기술의 단축어로 규제 모니터링, 보고와 준수 분야에 IT 기술을 사용하는 것을 말한다. - 크리스토프 샤죠 -

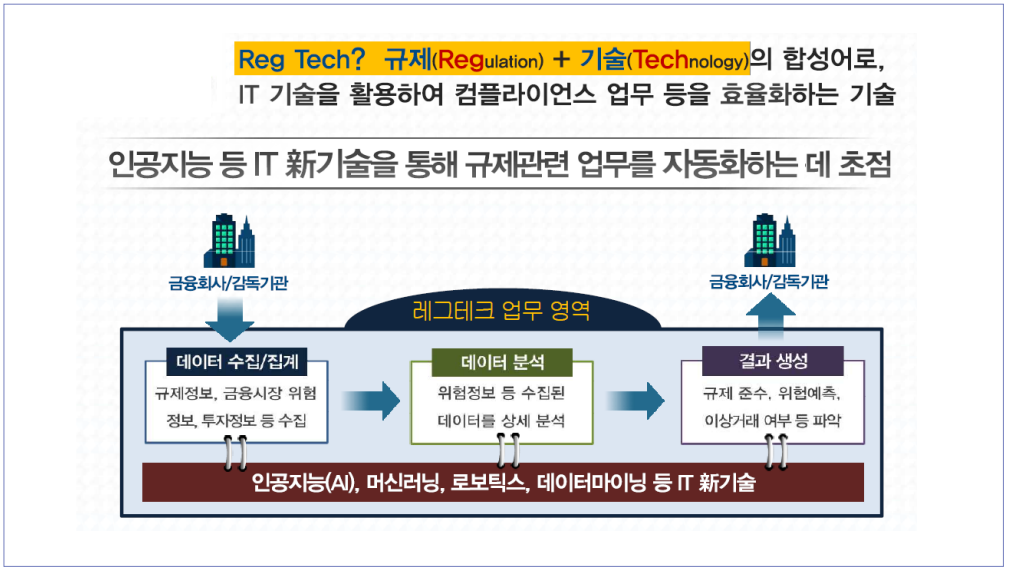
"

'RegTech' is a contraction of the terms 'regulatory' and 'technology', and describes the use of technology, particularly information technology('IT'), in the context of regulatory monitoring, reporting and compliance.

출처: Christophe Chazot, Institute of International Finance, RegTech: Exploring Solutions for Regulatory Challenges

"

〈그림 XI-2〉 레그테크의 정의



출처: 금융보안원, 금융보안 분야 레그테크 도입 방향, 금감원 레그테크 포럼 발표자료, 2017, 1면

나. 프로세스 자동화를 통해 위험 요소 파악 및 규정 준수를 더 잘 그리고 더욱 효율적으로 수행하는 것을 말한다. – 산티아고 페르난데스 드 리스 –

> Automation of processes allows for better
> and more efficient risk identification and regulatory compliance.
>
> 출처: Santiago Fernandez De Lis, ET AL., REGTECH,THE NEW MAGIC WORD IN FINTECH 1

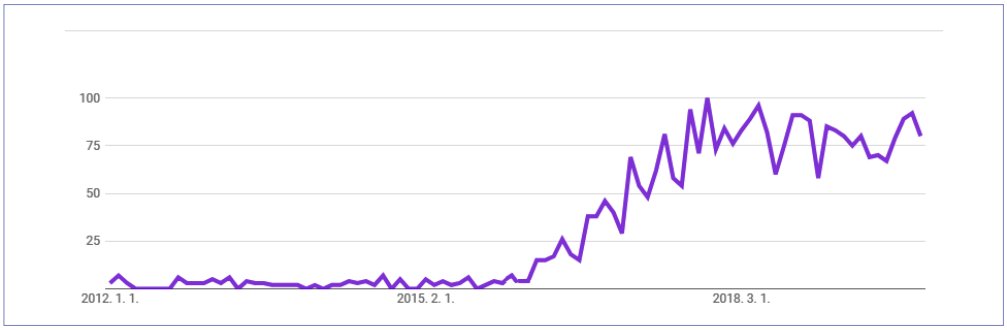
다. 일반적인 레그테크의 정의가 협소하게 시스템적 관점으로 한정되는 측면이 있다. 본 서에서는 금융회사의 컴플라이언스 종사자, 핀테크 기업, 금융정책기관 등의 이해관계자를 포함한 생태계로서의 레그테크로 이해하는 것이 필요하다.

2 레그테크의 동향

2-1 국내외 추진 동향

가. 레그테크의 확산

〈그림 XI-3〉 구글(Google) RegTech 키워드 서치 트렌드



출처: 금융보안원, 금융보안 분야 레그테크 도입 방향, 금감원 레그테크 포럼 발표자료, 2017, 1면

구글의 레그테크 주제어 검색 추세를 보면 2012년부터 2015년까지는 미약한 반응을 보이다가 2016년 하반기부터 비약적으로 발전하는 양상을 보인다. 지역별 관심도를 보면 룩셈부르크, 세인트헬레나, 싱가포르, 홍콩과 아일랜드가 두드러지게 나타난다. 관심도를 보이는 지역은 핀테크와 블록체인(Blockchain)에 관심이 많은 지역이다. 이러한 현상은 2015년 3월 영국 국립 최고 과학 자문기구가 보고서를 통해 핀테크를 활용한 새로운 규제 관리기술의 방법론으로 '레그테크'를 주창하면서 비롯되었다.

나. 감독기관 주도의 국내외 추진사례

■ 해외 추진사례

1) 2015.3. 영국 국립 최고 과학 자문기구(UK Government Chief Scientific Adviser), 'RegTech' 개념을 소개하였다.

2) 2016.2. 영국 금융감독청(FCA; Financial Conduct Authority), 레그테크를 핀테크의 한 부분으로(RegTech is a subset of FinTech)로 정의하였다.

3) 2018.1. 싱가포르 금융감독청(MAS; the Monetary Authority of Singapore) 금융회사가 신기술을 활용한 비대면 고객확인 업무(Non face to face KYC) 수행 시 해당 기술에 대한 독립적인 검증을 요구하였다.

〈그림 XI-4〉 해외와 국내 추진사례

출처: 금융보안원, 금융보안 분야 레그테크 도입 방향, 금감원 레그테크 포럼 발표자료, 2017, 2면

■ 국내 추진사례

1) 2017.4. 금융감독원 레그테크 포럼을 발족하였다. 해당 포럼에는 금융회사, 관계기관, 학계 및 전문가들로 구성하였다.

2) 2017.10. 금융위원회 · 금융감독원 · 한국금융연구원 공동으로 '레그테크 도입 및 활성화 과제' 세미나를 개최하였다.

3) 2019.7. 금융감독원은 금융산업의 핀테크 혁신을 지원하고 레그테크 활성화를 도모하기 위해 기존의 레그테크 발전협의회를 확대와 재편성하여 제1차 「핀테크 · 레그테크 포럼」을 개최하였다.

제2절

레그테크 등장 배경

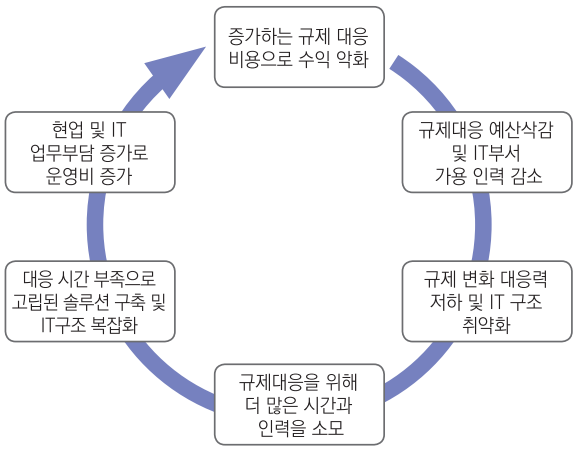
1 규제 당국 관점

1-1 데이터의 폭발적 증가와 기술 기반의 금융서비스 대응 필요

가. 디지털 기술의 비약적인 발전으로 비대면 금융거래 데이터가 기하급수적으로 증가하였다. 또한, 자금세탁방지(AML: Anti-Money Laundering) 업무, FATCA, 불공정 거래 감시 등 새로운 규제 관리를 위한 데이터 분석에 많은 자원이 투입되게 되었다.

나. 4차 산업혁명의 진행으로 인공지능(AI), 빅데이터 등 IT 발전으로 금융서비스가 지능화 및 자동화되어 이러한 환경에 대응하는 규제 당국의 능력도 요구되고 있다.

〈그림 XI-5〉 금융회사의 레그테크 필요성



출처: 박만성, RegTech 전망과 도입 필요성, 금감원 레그테크 포럼 발표자료, 2017, 10면

2 금융회사 관점

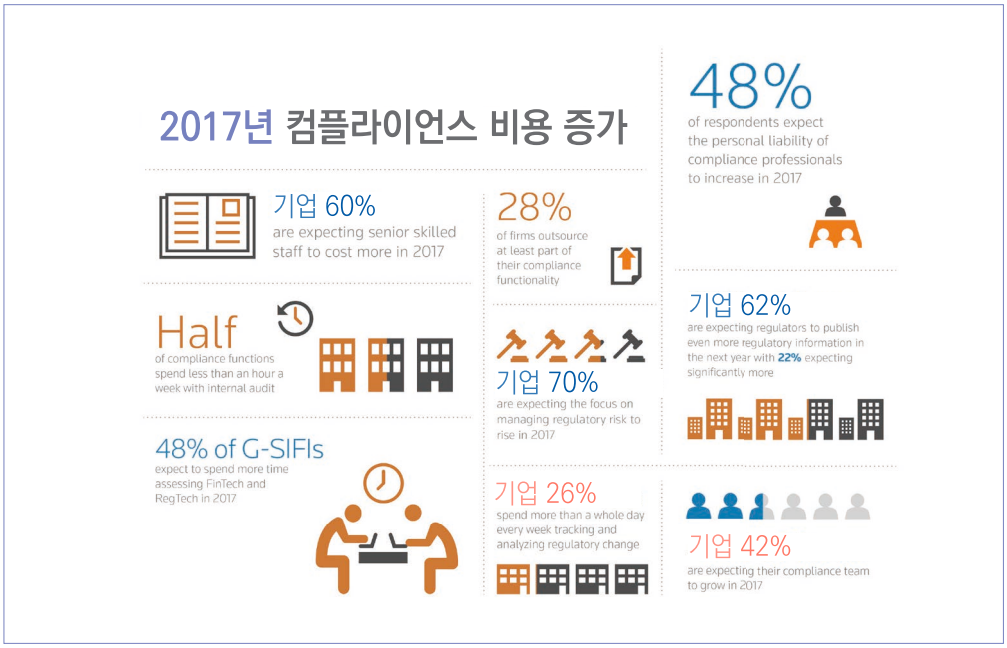
2-1 컴플라이언스 업무 비용의 증가

가. 지속적 비용 증가

1) 컨설팅 회사인 액센추어의 2017년 발표에 따르면 금융회사는 새로운 법규의 신설 및 금융소비자 보호를 위하여 당기순이익의 5% 이상을 컴플라이언스 비용으로 지출하고 있으며, 매년 40%씩 증가하고 있는 추세이다.

2) 금융 리서치 그룹인 메디치(Medici) 그룹의 2016년 보고서에 따르면, 세계적 금융회사들이 규제 준수에 사용하고 있는 비용은 약 80조원에 이르며, 2020년에는 세계적 규제 준수를 위한 소프트웨어 시장은 약 130조원 규모로 증가할 것으로 예상되었다.

〈그림 XI-6〉 컴플라이언스 비용의 증가



출처: Thomson Reuters, Cost of Compliance 2017

나. 레그테크 수요의 증가 예상

1) 레그테크의 핵심은 AI 등을 활용하여 데이터 분석 · 예측에 따른 의사결정을 하는 것이므로, 이를 위한 데이터 수집 · 보관 · 분석역량 확보 등이 우선되어야 한다. 이에 바젤 은행 감독위원회(BCBS; Basel Committee on Banking Supervision)는 2010년 9월에 '효과적인 리스크 데이터 수집과 리스크 보고 원칙(BCBS#239)'을 발표하고, 글로벌 은행은 리스크 데이터 수집 능력을 제고하고, IT 등의 인프라를 구축할 것을 요구하였다.

2) 세계경제포럼(WORLD ECONOMIC FORUM)에 따르면 2025년에는 기업의 회계감사의 30%를 인공지능(AI) 기반의 레그테크 시스템이 수행할 것이라고 예상하고 있다.

〈그림 XI-7〉 세계 주요 은행의 규제 준수 비용 현황

출처: Financial Times, 2016

3) 급변하는 4차 산업혁명 시대 속에서 금융회사 등이 생존하려면 시시각각으로 변하는 규제와 고객의 요구(Needs)에 대해 최신 기술인 인공지능(AI), 빅데이터 분석(Big Data Analysis), 블록체인(Blockchain) 등을 활용한 신속하고 정확하며 지속적인 대응이 필요하다.

3 금융소비자 관점

3-1 금융소비자의 편익 증대

가. 민원 조기 예방

레그테크를 활용하면 금융소비자의 민원을 조기에 탐지하고 해결할 수 있게 된다. 금융당국이나 금융회사 등에 문의하는 민원 및 상담 전화 대화는 자동응답 서비스(ARS; Automatic Response Service)시스템에 의해 모두 녹취된다. 녹취된 음성파일은 인공지능을 활용하여 모두 텍스트로 전환(Voice to Text)하고 그 전환한 내용 중에 고객의 불편과 금융회사 직원의 부적절한 대응이 있었다면 민원담당 책임자나 준법감시 책임자에게 자동으로 통지되어 민원을 조기에 차단 및 최소화할 수 있다. 여기서 한 발짝 더 나아가 인공지능을 활용하여 뉴스뿐 아니라 소셜네트워크 서비스상 금융소비자의 불만과 피해를 예방할 수 있다.

특히, 최근에 사회적으로 문제가 되었던 사모펀드 등에 대한 이상 징후와 금융소비자의 불만이 표면화되기 6개월 전부터 비실명 커뮤니티에서 회자하였던 점은 시사점이 크다.

나. 금융 법규 위반 예방

금융 관련 법규는 일반 금융소비자가 이해하기 어려운 점이 많다. 특히, 유학생 송금 등으로 송금할 수 있는 항목은 「외국환거래법」에 따라 제한되어 있는데 그러한 법규를 모르는 금융소비자가 유학생 송금과는 관련 없는 해외부동산 투자 목적 등으로 송금을 하여 외국환거래법규를 위반하여 처벌받는 사례 등이 있다. 이러한 위규 방지는 인공지능의 판단 트리(Decision Tree) 시스템 등을 적용하면 쉽게 예방할 수 있다.

3-2 레그테크를 활용한 금융사기 예방

가. 전화금융사기(Voice Phishing)와 대출사기 문자 방지

전화금융사기와 대출사기 문자는 금융소비자를 괴롭히는 대표적인 민생침해 범죄이다. 특히, 이 범죄에는 대포통장 등이 주로 사용된다. 대포통장은 범죄조직이 법집행기관의

자금추적을 피하려고 다른 사람의 실지명의로 만든 통장으로, 전화금융사기 또는 강력 범죄에 악용된다. 이러한 범죄예방에도 레그테크가 활용된다. 인공지능과 빅데이터를 활용하여 금융사기 범죄에 관련된 전화번호와 문자 내용 및 대포통장 번호를 요주의 목록으로 관리하여 해당 금융거래 및 통신 거래를 실시간으로 차단하는 방법이다.

〈그림 XI-8〉 금융사기 범죄 현황

분기별 메신저피싱 피해자 발생 현황(명)

	1분기	2분기	3분기	4분기
´17년	151	164	310	491
´18년	991	1,683	2,113	3,365
´19년	1,417	1,702	1,654	1,914

유형별 보이스피싱 피해자 현황

(단위: 명, %)

구분	´17년		´18년		´19년		´20년 1Q		합계	
전체	30,420		48,116		49,597		7,288		135,421	
대출빙자	25,306	(82.3)	32,649	(67.9)	38,213	(77.0)	4,990	(68.5)	103,929	(76.7)
사칭형	5,384	(17.7)	12,426	(25.8)	11,384	(23.0)	2,298	(31.5)	31,492	(23.3)
메신저	1,116	(3.7)	8,152	(16.9)	6,687	(13.5)	1,741	(23.9)	17,696	(13.1)

*( )안은 해당연도 전체피해자에서 유형별 피해자가 차지하는 비중

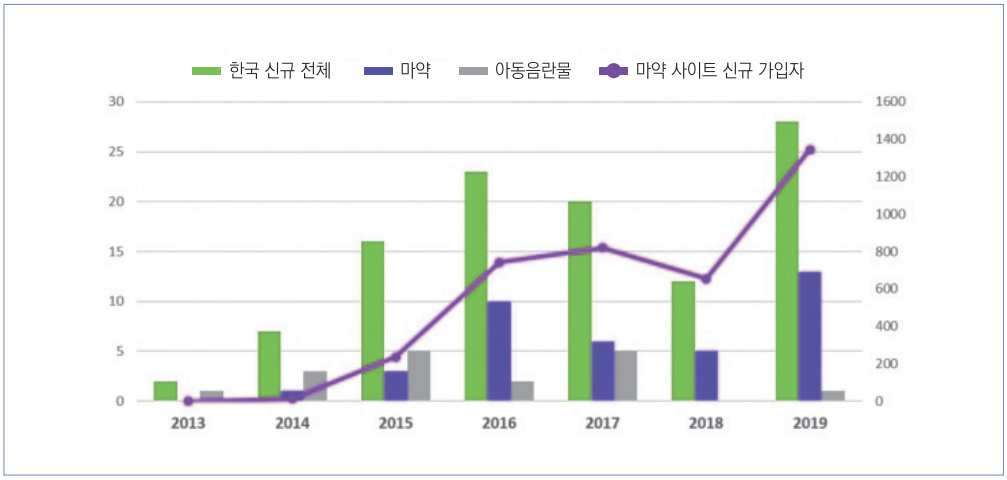
출처: 금융감독원, 보이스피싱 피해자 속성 빅데이타 분석을 통해 금융소비자 맞춤형 예방업무를 추진합니다(2020.8.10), http://www.fss.or.kr

나. 가상자산 범죄 예방

최근 들어 마약 범죄나 소위 말하는 'n번방 사건'과 같은 집단성착취 및 영상거래 사건 등 각종 범죄의 온상으로 다크웹과 텔레그램 등이 사용되고 있다. 또한, 범죄에 사용되는 자금도 가상자산 등이 사용되는 등 범죄가 지능화 및 디지털화되고 있다. 이러한 다크웹 및 텔레그램 범죄의 경우에 특히, 레그테크의 역할이 중요시된다

나아가 국제자금세탁방지기구(FATF)는 가상자산을 사용한 자금세탁방지의 국제적 공조를 위해 가상자산 사업자들에게 거래내역 보관 의무를 부여하고 있는데 축적된 데이터는 레그테크의 분석자료로 활용된다.

〈그림 XI-9〉 2019년 다크웹 신규 한국사이트 도메인



출처: NSHC(Network Security Hacking Company), https://www.nshc.net

제3절

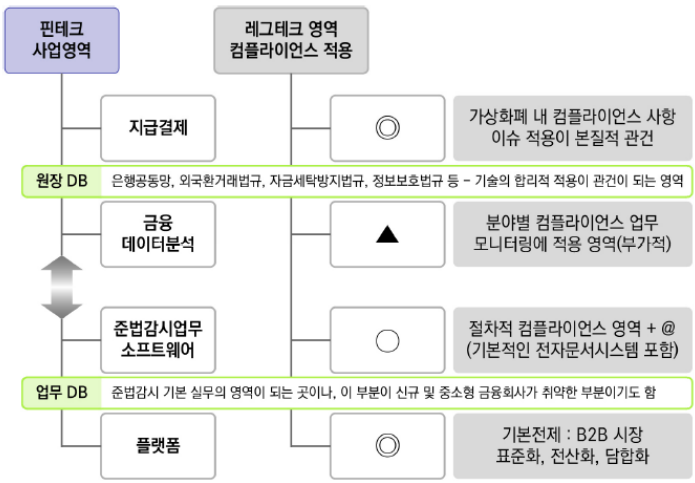
레그테크 구조 및 특징, 비즈니스 모델

1 레그테크 구조

1-1 핀테크와 레그테크의 구조 비교

핀테크와 레그테크는 용어의 정의에서 볼 수 있듯이, 핀테크는 금융(Finance)과 기술(Technology)의 합성어이며, 레그테크는 규제(Regulation)와 기술(Technology)의 합성어이다. 핀테크는 금융소비자가 금융상품과 서비스에 접근하기 손쉽게 IT기술을 활용하는 것이며, 레그테크는 제10장에서 학습한 컴플라이언스와 내부통제를 효율적으로 관리하기 위해 IT기술을 활용하는 것이다. 통상 금융회사의 내부 시스템을 데이터 관점에서 크게 구분하면 〈그림 XI-10〉과 같이 거래기록을 가지고 있는 원장 DB 계층, 리스크관리 · 완전판매 · 상품설계 등 금융서비스와 관련된 정보가 기록되는 업무 DB 계층으로 나눌 수 있고, 레그테크 역시 두 계층에 모두 적용될 수 있으며 원장 DB를 기반으로 한 업무는 주로 금융회사의 영업행위 결과를 바탕으로 한 모니터링(금지행위의 적출 등)이 대표적이고, 업무DB에 기반을 둔 업무는 금융회사의 서비스를 제공하는 절차나 종사자들의 행위가 올바르게 수행될 수 있도록 지원하는 형태에 해당한다.

〈그림 XI-10〉 핀테크와 레그테크 비교



출처: 조창훈 (2017), 국내 레그테크의 시장성 검토 및 도입 시 고려사항. 전자금융과 금융보안, 제8호, 2017-04, p. 74

2 레그테크 특징

2-1 양 방향성

레그테크는 기존 컴플라이언스 시스템과 다르게 외부와 유기적으로 연결되어 동작하는 것을 대체로 지향한다. 예로 감독기관의 시스템과 금융회사의 내부 컴플라이언스 시스템이 연동되어 필요한 데이터를 상호 간에 정해진 기술과 프로토콜로 주고받을 수 있도록 하여 효율성과 정확성을 추구하는 특성이 대표적이다.

2-2 표준화

기존의 컴플라이언스 시스템은 해당 조직이나 기업만을 위하여 독립적으로 설계되고 운영되었다면, 레그테크 시스템은 설계 단계부터 범용성을 위하여 표준화되어 개발되었다는 점이다. 이러한 표준화 특성은 법규 변경에 신속한 대응을 가능케 한다.

2-3 자동화

레그테크 사례 중 가장 대표적인 MRR(Machine Readable Regulation)은 자동화 특성을 잘 설명해준다. 수많은 법 · 제도 및 규정들이 변경될 때마다 금융회사는 변경에 따른 영향의 정도를 분석하여 필요에 따라 내부 컴플라이언스 절차 또는 내부 시스템을 변경해야 할 수도 있다. 이런 변경이 미칠 영향을 분석하고, 그에 따른 변경작업을 기술의 힘으로 자동화시켜보자는 프로젝트가 머신 리더블 레귤레이션(Machine Readable Regulation)이다. 즉, 시스템(Machine)이 변환된 금융 관련 법규를 자동으로 인식(Read)하고, 분석하여 금융회사의 컴플라이언스 절차 및 관련 시스템에 자동으로 반영을 할 수 있는지를 타진하고 있는 프로젝트이다.

2-4 신기술의 적극적 활용

레그테크는 블록체인, 빅데이터 및 클라우드 기반 등 신기술을 적극적으로 활용하는 특징을 가지고 있다. 신기술을 활용한 사례 등은 제12장에서 자세히 다루기로 한다.

3 레그테크 비즈니스 모델

3-1 제공 서비스별 비즈니스 모델

가. 유지보수

기존의 컴플라이언스 시스템의 보수유지 비즈니스 모델로 유지보수에는 관련 소프트웨어 유지보수와 업무 유지보수 및 해당 업무 전체의 아웃소싱 유지보수가 있다.

나. 소프트웨어 라이선스

컴플라이언스 패키지나 내부통제 패키지에 대한 라이선스 사업이 있다. 예를 들면 다우존스사의 요주의 인물 검색 시스템의 한국 내 라이선스 사업이나 외국 레그테크 패키지의 국내 공급 총판 사업 등이 있다.

다. 구축 서비스

관련 프로젝트를 수주하여 프로젝트를 수주하며 기존 시스템과의 인터페이스와 데이터 마트 구축 및 보고서 개발 등이 있다.

라. 컨설팅 업무

새로운 규제 발생에 대한 컨설팅과 새로운 기술의 기존 시스템에 적용하는 컨설팅 업무 등이 있다.

3-2 기능적 비즈니스 모델

가. 고객 확인 업무(Customer Journeys) ↔ 고객 수용 및 관리 업무

규제의 대상이 되는 고객 또는 기업 등의 대상물(Entity)에 대한 정보를 확인하고 검증하고 관리하는 업무를 수행하는 것을 말한다.

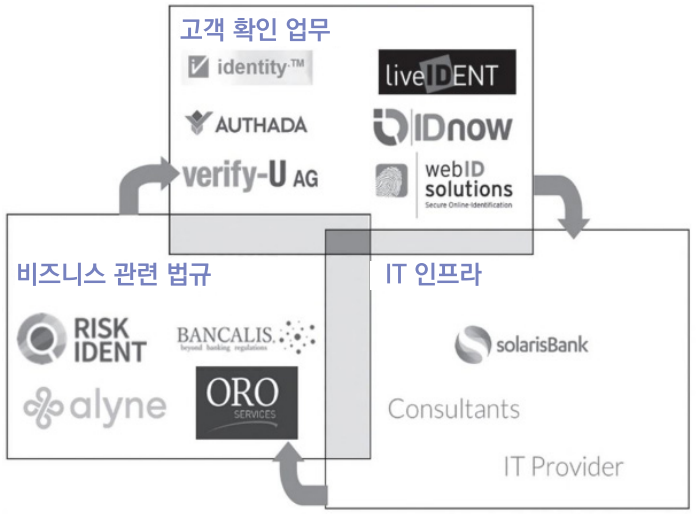
나. 사업 관련 법규(Business-Related Rules) ↔ 법률 리스크 점검 업무

고객 정보 등 분석 대상이 되는 목적물(Entity)의 정보(Journeys)를 가지고 법률 위반 리스크를 검토하는 업무를 수행하는 것을 말한다.

다. IT 기반 설비(Infrastructure) ↔ 전산시스템 구축 업무

금융당국으로부터 요구되는 법규준수를 효과적으로 지원할 수 있는 시스템 구축 사업을 말한다.

〈그림 XI-11〉 독일의 레그테크 시장 평가도(Market Evaluation Map)



출처: Janos Barberis 외 2명(2019), The REGTECH Book, John Wiley & Sons Ltd.

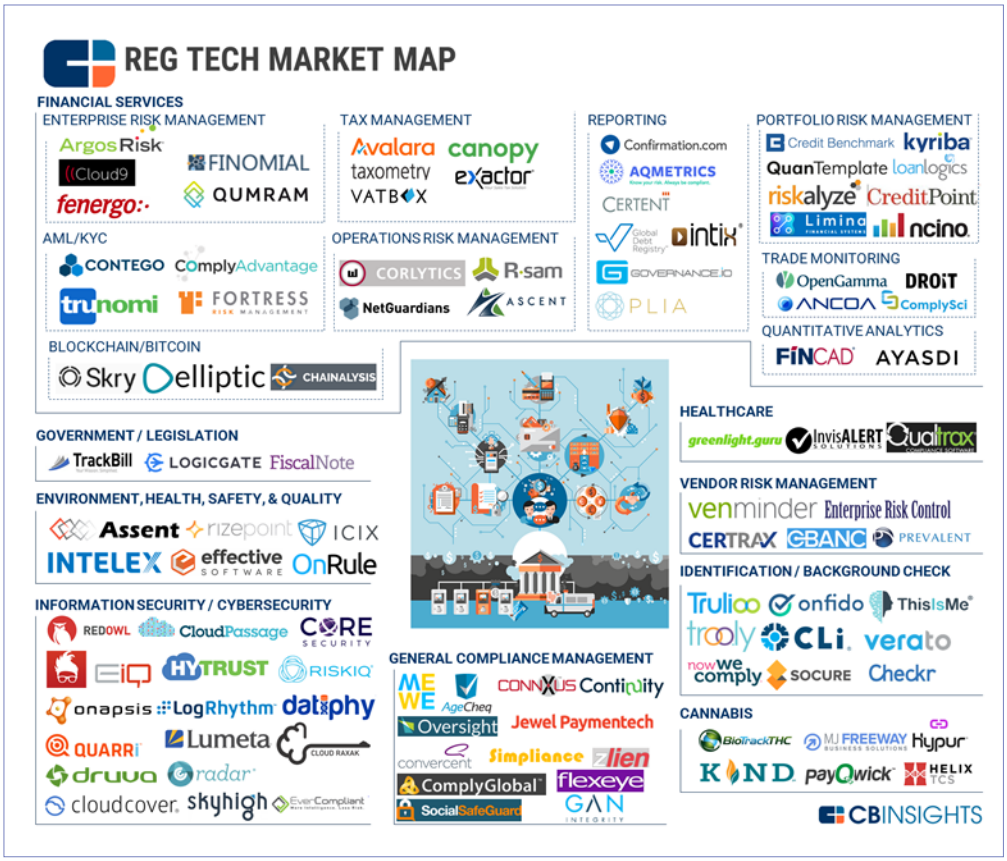
제4절

국내외 레그테크 부문 핀테크 기업의 서비스 사례 분석

1 해외 레그테크 서비스 사례

1-1 레그테크 시장 구성도

〈그림 X1-12〉 레그테크 시장 구성도



출처: CB Insights, 2017

〈그림 XI-12〉의 레그테크 시장 구성도[148]를 보면 해외에서는 매우 다양한 분야가 레그테크 시장을 구성하고 있음을 알 수가 있다. 우리가 잘 알고 있는 자금세탁방지 시스템을 구성하는 고객확인제도(KYC; Know Your Customer)를 포함한 금융서비스(Financial Service) 분야 외에도 정부/입법(Government/Legislation) 분야, 의료(Healthcare) 분야, 공급자 위험관리(Vendor risk management) 분야, 정보보호(Information Security/Cyber-security) 분야 및 검증/평판 점검(Identification/Background Check) 분야 등 매우 광범위한 분야가 레그테크 시장을 구성하고 있다.

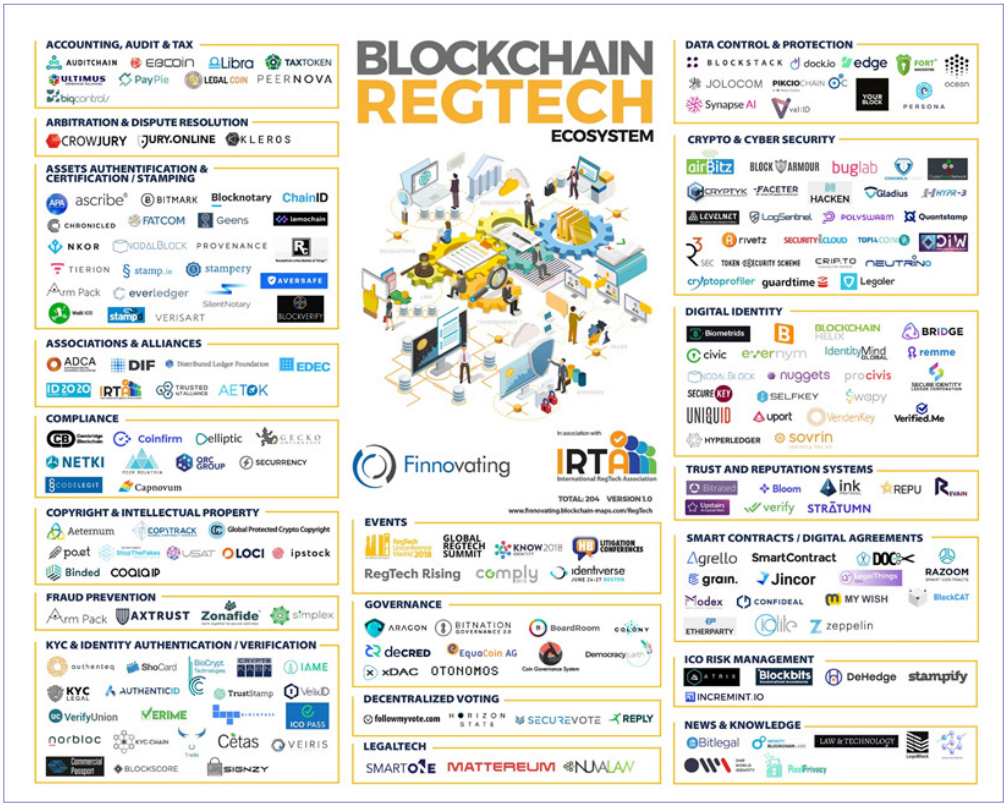
1-2 블록체인 레그테크 생태계

레그테크 서비스 시장에서 한 발짝 더 나아가 블록체인 레그테크 생태계[149]를 보면, 기존의 레그테크 업체 외에 회계, 재정거래, 분쟁, 저작권 및 지식재산권, 사기 방지, 선거, 데이터 보호, 디지털 고객 확인, 스마트 계약, 가상화폐공개 리스크 관리 등 매우 다양하고 광범위한 생태계를 구성하고 있다.

148) REGTECH MARKET MAP, CBINSIGHTS[웹사이트](2020.6.3.), https://www.cbinsights.com/research/regtech-regulation-compliance-market-map/?utm_source=CB+Insights+Newsletter&utm_campaign=d01a7281f1-TuesNL_1_31_2017&utm_medium=email&utm_term=0_9dc0513989-d01a7281f1-&utm_source=CB+Insights+Newsletter&utm_campaign=4f0080b02c-TuesNL_1_31_2017&utm_medium=email&utm_term=0_9dc0513989-4f0080b02c-88531353

149) BLOOKCHAIN REGTECH ECOSYSTEM, Finnovating[웹사이트](2020.6.3.). https://www.finnovating.com/news/finnovating-launches-the-first-regtech-blockchain-map-in-association-with-the-irta/

〈그림 XI-13〉 블록체인 레그테크 생태계



출처: 피노베이팅(Finnovating), 2018

2 국내 레그테크 서비스 사례

국내의 레그테크 업체는 '레그테크 시장 구성도'와 '블록체인 레그테크 생태계'를 고려하면 매우 많은 업체가 레그테크 업체에 포함될 것이다. 그중에 대표적인 기업은 지난 2019년 5월에 금융위원회가 개최한 '제1회 「코리아 핀테크 위크 2019」'에 참가인 6개 기업이다. 업체 중 (주)유니타스와 (주)옥타솔루션은 자금세탁방지 분야를, (주)닉컴퍼니와 (주)코스콤은 컴플라이언스 분야를, (주)에임스는 보험금 착오 지급점검 분야를, 금융보안원은 금융회사의 금융보안 레그테크 시스템 서비스를 제공하고 있다.

〈그림 XI-14〉 국내 레그테크 업체

기업명	분야	솔루션
(주)유니타스	자금세탁방지	• UNITAS CRI(Country Risk Index) Service – 마약, 테러, 제재 등과 관련된 34개 변수를 실시간 반영한 '국가위험지수(Country Risk Index)' 산출
(주)닉컴퍼니	핀테크 전문 컴플라이언스	• NIC 디지털 컴플라이언스 플렛폼 – 금융회사가 제공하는 모든 서비스를 위험지표와(스코어링)하여 시각화된 모니터링 기능 제공
(주)에임스	보험금 착오지급 점검	• 보험금 착오지급 점검업무 자동화 솔루션(Autodit) – 보험약관의 자동 알고리즘화 및 보험금 착오지급 자동 검출
(주)옥타 솔루션	자금세탁방지	• 업종별 특화 AML//RBA 솔루션 SaaS 서비스 – 가상통화 취급업소, 해외송금업자, 전자금융업자 등에게 업종 맞춤형 자금세탁방지 솔루션 제공
(주)코스콤	금융투자 컴플라이언스	• 상시모니터링서비스 시스템 KI-Guard – 금융투자회사의 데이터베이스를 실시간으로 분석 · 모니터링하여 내부직원의 횡령 · 사기 등 이상거래를 적출
금융보안원	금융보안점검	• 금융보안 레그테크 시스템 – 금융회사의 정보보호 수준 자율진단, 금융보안 관련 보고서의 자동 생성 · 리포팅 등

출처: 금융위원회(2019), 제1회 「코리아 핀테크 위크 2019」 개최 결과, 금융위원회

핵심정리

1. 레그테크의 정의

레그테크란, 규제(Regulation)와 기술(Technology)의 합성어로 규제 준수 및 규제 관련 활동에 초점을 맞춘 기술을 말한다. 레그테크는 기술, 규제, 금융서비스와 핀테크를 상호 연결하여 각각의 강점을 살릴 수 있는 기술을 의미한다. 즉, 레그테크란 '사업자가 자신의 상품 및 서비스를 시장에 공급할 때 존재하는 각종 규제를 효율적으로 관리하거나 극복하기 위해 IT 기술을 활용하는 것'을 말한다.

2. 레그테크 서비스 등장 배경

레그테크 서비스의 등장 배경은 첫째, 규제 당국 입장에서는 '금융 데이터의 폭발적 증가 및 금융서비스의 혁신 필요성'이며, 둘째, 금융회사 처지에서는 '컴플라이언스 업무 비용의 기하급수적인 증가'를 들 수 있으며, 셋째 금융소비자로서는 '금융소비자의 편익 증대'와 '레그테크를 활용한 금융사기 등의 예방'을 목적으로 한다.

3. 레그테크와 핀테크의 차이점

레그테크와 공통점은 IT기술을 활용하여 금융소비자의 편익을 증대한다는 점이다. 통상 레그테크는 핀테크의 일부(Subset)로 인식되기도 하지만 차이점으로는 핀테크는 '금융소비자의 편리와 이익의 증대'를, 레그테크는 '기업의 컴플라이언스 비용 절감과 효율성 극대화'를 목적으로 한다.

MEMO

헬로, 핀테크!(보안인증 · 블록체인)

HELLO, FINTECH!

12장

레그테크 관련 기술 현황

제1절 레그테크의 핵심기술

제2절 레그테크의 아키텍처

제3절 레그테크 적용 방식

제4절 레그테크의 미래 전망

12장 레그테크 관련 기술 현황

학습목표

1. 레그테크(RegTech)의 핵심 기술에는 어떤 것들이 있는지 설명할 수 있다.
2. 레그테크의 사례들이 전통적 컴플라이언스의 한계를 어떻게 해결하고 있는지와 향후 어떤 모습으로 발전될지 예상할 수 있다.

학습개요

레그테크의 핵심기술로는 대표적으로 '응용 프로그래밍 인터페이스(API)', '블록체인(Blockchain)', '머신러닝(Machine Learning)'과 '클라우드 컴퓨팅(Cloud Computing)' 등이 있다. 이러한 핵심 기술들을 활용하여 다양한 레그테크 서비스가 연구 및 적용되고 있다. 이번 장에서는 레그테크 시스템의 방법론으로 '로봇 프로세스 자동화(RPA)', '섭테크(SupTech)', '위험기반 접근법(RBA)' 등을 소개한다. 아울러, 방법론의 세부적인 기술로 사용되는 '외국환거래', '무역기반 자금세탁방지(TBML)', '요주의 인물 검색(WLF)'과 '보이스 피싱(Voice Phishing)에 대하여 알아본다.

용어해설

❶ 응용 프로그래밍 인터페이스(API)

API(Application Program Interface)란 정보 이용자들에게 정보를 공개하기 위해 제공하는 일정한 규약으로 외부개발자가 정보공급자(금융감독원 홈페이지 등)의 콘텐츠 데이터를 타 시스템에서 활용할 수 있도록 XML(eXtensible Markup Language), JSON(JavaScript Object Notation) 형태로 제공하는 REST(REpresentational State Transfer) 방식의 인터페이스를 말한다.

- XML: 홈페이지 구축 기능, 검색 기능 등이 개선된 웹 문서 개발 언어이다.
- JSON: 웹과 컴퓨터 프로그램에서 경량의 데이터를 교환하기 위해 자바스크립트로 개발된 데이터 교환 형식이다.
- REST: 웹(Web) 프로토콜을 통해 데이터를 교환할 수 있는 인터페이스 표준을 말한다.

❷ 블록체인(Blockchain)

블록(Block)에 정보를 담아서 체인(Chain) 형태로 연결한 분산형 데이터 저장기술이다. 중앙 집중형 컴퓨터와 달리 분산된 수많은 컴퓨터에서 동일한 원장을 분산 보관하는 기술로 탈중앙화 공공 거래 원장이라고도 부른다.

❸ 섭테크(SupTech)

감독(Supervision)과 기술(Technology)의 합성어를 말한다. 금융감독기구의 주 업무인 감독(Supervision)에 기술(Technology)을 접목해 감독과 검사를 효율적으로 수행하는 것을 말한다. 레그테크가 금융회사의 업무 효율화에 필요한 것이라면, 섭테크(SupTech)는 금융회사들의 감독자인 금융감독기구의 감독업무를 효율화하는 데 사용된다.

제1절

레그테크의 핵심기술

1 응용 프로그래밍 인터페이스(API)[150]

1-1 API 정의

API(Application Program Interface)란 정보 이용자들에게 정보를 공개하기 위해 제공하는 일정한 규약으로 외부개발자가 정보공급자(금융감독원 홈페이지 등)의 콘텐츠 데이터를 타 시스템에서 활용할 수 있도록 XML(eXtensible Markup Language), JSON(JavaScript Object Notation) 형태로 제공하는 REST(REpresentational State Transfer) 방식의 인터페이스를 말한다.

1-2 API 목적

이용자가 일방적으로 웹 검색 결과 및 사용자 인터페이스(UI) 등을 제공 받는 데 그치지 않고 공개된 데이터를 활용하여 창조적이고, 다양한 콘텐츠를 직접 개발할 수 있도록 지원한다.

150) 오픈 API 소개, 금융감독원, http://fss.or.kr/fss/kr./openApi/sumry/intrcn.jsp

〈그림 XII-1〉 레그테크와 API

레그테크	API
Semantic tech and data point models	
- Machine-readable regulation은 규정 변경으로 인한 비용과 시간을 자동화를 통해 최소화 가능 - 규정변경에 따른 불일치성을 최소화할 수 있음	각종 규정의 Machine-readable (정부 문서 Github공유, **웹사이트가 아니라 디지털 서비스)**
Application Programming interface(API)	
- 시스템 간의 통합과 데이터 교환을 용이하게 함 - 비용절감과 혁신을 위한 효율과 플랫폼을 제공할 수 있음	**- 각종 보고 방식을 API 전환** - 보고 및 교환되는 정보의 표준화 : 데이터 항목 이름 : 항목 데이터 type(숫자, 글자 등) - 사람의 개입이 적을 수록 비용절감, 데이터 정확도 향상
Shared data ontology	
- 규제관련 데이터의 구조를 설명하기 위한 데이터 타입, 속성 등을 정의하고 교환 - 효율증대, 비용절감. 중복의 최소화	
Robo-handbook	
- 상호작용이 가능한 handbook(FCA Handbook)은 금융회사의 시스템과 프로세스에 미치는 영향을 더욱 잘 이해 가능토록 함 http://www.handbook.fca.org.uk/handbook	정적이고 일방적인 guide를 다양한 관점으로 볼 수 있고, **tailoring할 수 있도록 변화 필요**

출처: Feed Statement, Call for input on supporting the development and adopters of RegTech, FCA

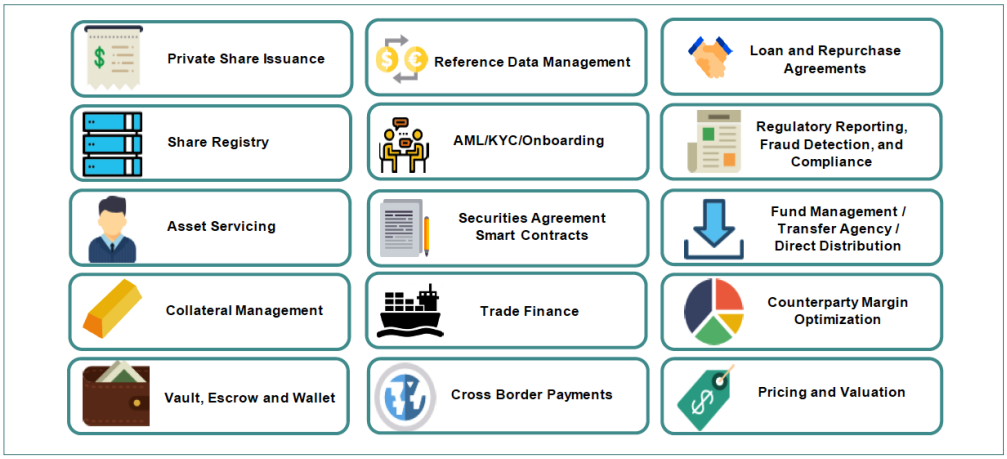
2 블록체인(Blockchain)

2-1 블록체인의 정의

블록체인(Blockchain)이란, 단어와 같이 블록(Block)에 정보를 담아서 체인(Chain) 형태로 연결한 분산형 데이터 저장기술이다. 중앙 집중형 컴퓨터와 달리 분산된 수많은 컴퓨터에서 동일한 원장을 분산 보관하는 기술로 탈중앙화 거래 원장이라고도 부른다.

블록체인은 다양한 분야에 활용될 수 있는데, 특히 탈중앙화(脫中央化)된 지분율 관리(Private Share Issuance)나 권리관계(Share Registry)를 표시할 때 매우 유용하며, 대출업무의 담보물 관리(Collateral Management), 무역거래에 있어서 신용장 및 자금관리(Trade Finance), 국가간 지급결제(Cross Border Payments) 등에도 활용될 수 있다.

〈그림 XII-2〉 블록체인의 활용도



출처: R3 Korea Members Workshop, Seoul, 28 October 2016

2-2 레그테크와 블록체인

블록체인의 가장 큰 특징은 한번 기록된 자료는 위변조가 거의 불가능한 불가역성(不可逆成)이다. 이러한 특성은 법률 공포(公布)나 계약 및 등록과 같은 분야에 가장 적합한 특징이다. 〈그림 XII-2〉와 같이 다양한 분야에 활용될 수 있는데 특히, 자금세탁방지 분야의 고객확인제도(KYC; Know Your Customer) 분야와 법률적 보고(Regulatory Reporting), 사기방지(Fraud Detection), 스마트 계약(Smart Contracts) 등 다양한 컴플라이언스 영역에서 활용될 수 있다.

3 머신러닝(Machine Learning)

머신러닝이란 컴퓨터가 스스로 학습하게 하는 것을 말한다. 예를 들면, 우리가 컴퓨터에게 감자의 크기를 정해주지 않고 단순히 큰 것과 작은 것으로 분류하라고 작업을 지시하면, 컴퓨터가 1차적으로 단순 세척과정에서 수확한 전체 감자의 크기 분포도를 만들고 2차적으로는 크기의 분류 기준을 만들어 세척 후 분류 작업을 자동적으로 수행하는 것을 예로 들 수 있다. 레그테크 분야에서도 머신러닝을 통해 1차적으로는 인간의 오류나 실수를 발견하여 알려주며, 2차적으로는 학습을 통해 사전적으로 오류 비율 또는 위험도가 높은 특정 지역이나 인물에 대한 통계학적 예측도 가능하게 한다.

3-1 머신러닝(Machine Learning)의 정의

가. 아서 사무엘(Arthur Samuel)의 정의

명시적으로 프로그램을 작성하지 않고 컴퓨터에 학습할 수 있는 능력을 부여하기 위한 연구 분야를 말한다.[151]

나. 톰 미첼(Tom M. Mitchell)의 정의

컴퓨터 프로그램이 어떤 작업 T와 평가 척도 P에 대해서 경험 E로부터 학습한다는 것은, P에 의해 평가되는 작업 T에 있어서의 성능이 경험 E에 의해 개선되는 경우를 말한다.[152]

3-2 레그테크와 머신러닝

컴플라이언스 준수를 위한 각종 규제 데이터를 학습하고 각종 분석 알고리즘을 사용하여 법규준수를 위한 단위업무를 처리한다.

---

151) Arthur Samuel(1959), Some studies in machine learning using the game of checkers, Artificial Intelligence for Games: Seminar

152) Tom M. Mitchell(1997), Machine learning. Boston: WCB/McGraw-Hill

〈그림 XII-3〉 레그테크와 머신러닝

레그테크	머신러닝
Big data analytics	
- 진보된 분석을 위해서는 방대한 정형 또는 비정형 데이터를 보관할 수 있어야 함 - 정보에 근거한 의사결정과 통찰력을 갖기 위해 - 규제기관이 대용량 데이터 분석 역량을 갖추게 되면 금융회사는 보고의 부담을 덜 수 있음	- 저비용의 고용량 데이터 보관기술 **- Raw data에 근거한 분석**
Modeling/Visualization Technology	
- 가시적으로 나타나는 상호작용 시뮬레이션을 통해 시스템에 미치는 영향을 평가 가능 - 모델링기술은 적용되기 전 규제의 영향을 이해할 수 있도록 해줌	- 데이터 간의 **상관관계 등의 가시화** - Risk management, Reporting
Risk and compliance monitoring	
- 거래, 행동 및 커뮤니케이션을 상시 감시할 수 있게 해주는 기술 - 다양한 데이터 source로부터 들어오는 사건 간의 상관관계를 실시간으로 추출 가능	- 실시간 대응력을 갖춘 데이터 분석 **- Data 간 Correlation 분석**
Machine learning and cognitive technology	
- 데이터로 학습하고 알고리즘을 스스로 개선하는 기술 - 복잡하고 대용량의 데이터를 처리하거나, 반복하는 일의 자동화	- AML 등 각종 분석 알고리즘의 **자기학습화 필요**

출처: Feed Statement, Call for input on supporting the development and adopters of RegTech, FCA

〈그림 XII-3〉 에서처럼, 레그테크에 머신러닝이 활용되는 사례는 금융회사에서 판매하는 다양한 상품과 관련된 '고객 동의서' 작성의 적정성 검증에 활용할 수 있다. 금융상품을 판매할 때를 예로 들어보자.

고객의 의사를 확인하기 위하여 여러 곳에 고객의 이름과 날인을 받도록 되어 있다. 이때 고객이 서명이나 날인을 누락했을 경우 컴퓨터가 누락 여부를 알려줄 수 있으며, 머신러닝을 통하여 고객이 본인의 이름이나 구매한 금융상품명을 잘못 작성하였을 경우 오류를 알려줄 수 있다.

4 클라우드 컴퓨팅(Cloud Computing)

4-1 클라우드의 정의(Cloud)

클라우드(Cloud)는 사전적 의미인 구름과 같이 그동안 컴퓨터와 통신업계에서 시스템 구성도상에 네트워크(Network)를 구름(Cloud)으로 표현한 것에 기인한다. 일반적인 자립형(Stand Alone) 컴퓨터에 대비되는 개념으로 네트워크상에 컴퓨터 자원을 공유하는 개념이다.

4-2 레그테크와 클라우드 컴퓨팅(Cloud Computing)

클라우드 컴퓨팅(Cloud Computing)은 레그테크 서비스 등장 배경인 '금융 데이터의 폭발적 증가 및 금융서비스의 혁신 필요성'과 '컴플라이언스 업무 비용의 증가'를 해결할 수 있는 기술로 평가된다. 기업이나 조직 내에 대량의 데이터 보관 및 처리를 위해 전산 설비를 구매하고 운영할 필요 없이 레그테크에 필요한 전산 설비 및 전산 프로그램과 데이터를 외부 자원을 활용함으로써 고성능 · 고비용 컴퓨팅 자원을 효율적으로 사용할 수 있게 된다.

〈그림 XII-4〉 레그테크와 클라우드 컴퓨팅(Cloud Computing

레그테크	클라우드 컴퓨팅
Alternative reporting methods	
- 보고를 위해 새로운 방법을 제공 (비용과 보고업무에 의한 부담 감소)하는 기술 - 엑셀, 워드 파일 등이 아닌 내부 시스템과 연결된 시스템 to 시스템 보고 체계 구축	- RPA(Robot Process Automation) **- End to End (Straight Through) Processing**
Shared Utilities	
- 서비스를 공유할 수 있게 만들어주는 기술 - 공유 가능한 서비스는 확장성과 유연성을 바탕으로 비용부담을 감소시킴	**- ASP 컴플라이언스 솔루션**
The cloud/cloud computing	
- 인터넷을 통한 On-demand 컴퓨팅 서비스 - 혁신적인 소프트웨어, 진보된 컴퓨팅 환경은 역량, 인사이트, 의사결정력을 강화 시켜줌	**- 낮은 비용의 ASP 솔루션** **- 낮은 비용의 Computing Power**
Online Platform	
- 기술은 서로 다른 기관들을 커뮤니티로 연결시켜 줄 수 있음 - Fintech 기업들을 위한 regulation, compliance 커뮤니티	- 문제점이 많이 공유되면 해결책도 하나의 솔루션(산업)으로

출처: Feed Statement, Call for input on supporting the development and adopters of RegTech, FCA

〈그림 Ⅻ-4〉와 같이 클라우드 컴퓨팅을 사용하게 되면, 각 금융회사가 금융당국에 개별적으로 보고하는 자료를 업권별 연합회에 공용 보고 클라우드시스템을 구축하여 '시스템to시스템' 보고체계를 구축할 수 있으며, 고가의 응용 프로그램 또한 공동으로 사용할 수 있으며, 온라인을 통한 자료 공유 및 커뮤니티 형성까지도 가능하게 된다.

제2절

레그테크의 아키텍처

1 로봇 프로세스 자동화(RPA)

1-1 로봇 프로세스 자동화(RPA)의 정의

로봇 프로세스 자동화는 사람이 수행하는 방식으로 다른 컴퓨터 시스템의 사용자 인터페이스를 작동시키는 도구의 포괄적인 용어이다. 로봇 프로세스 자동화는 "아웃사이드 인" 방식으로 수행된 자동화로 사람을 대체하는 것을 목표로 한다. 이것은 정보 시스템을 개선하기 위한 고전적인 "인사이드 아웃" 접근 방식과는 다르다.[153)]

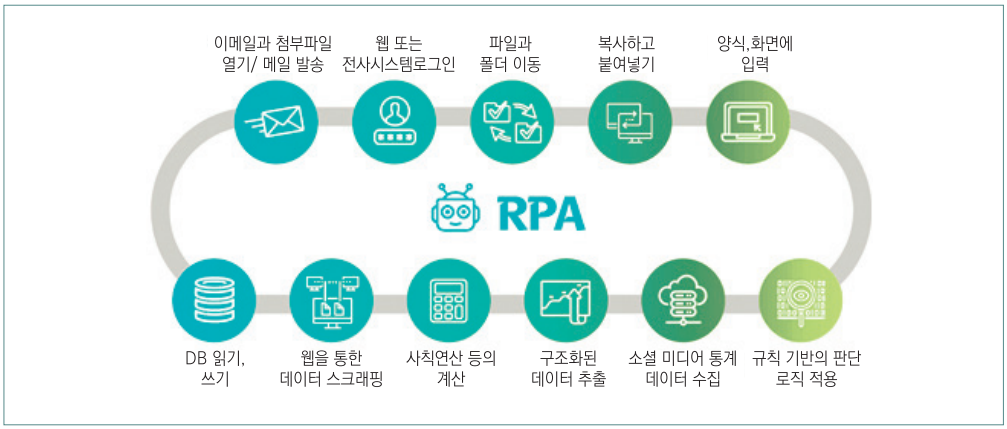
1-2 레그테크와 로봇 프로세스 자동화

금융산업은 이종 산업과 결합해 융·복합 서비스를 끊임없이 창출하고 있으며 4차 산업혁명을 바탕으로 급속하게 기술이 발달하였다. 하지만 개인정보, 리스크 관리 등 새로운 각종 과제와 맞물리게 되어 이에 대한 규제 대응과 관련 이슈는 금융권이 기술과 규제 사이에서 가장 민감하게 체감하는 과제로 부각되었음을 제10, 제11장에서 설명하였다.

이에 대응하기 위해 첨단 기술 접목으로 레크테크 활용에 접근하였고 이를 기반으로 도입한 로봇 프로세스 자동화(RPA)의 경우는 〈그림 XII-5〉에서 처럼 '인건비 절감'과 '인간의 실수'를 줄일 수 있어서 레그테크의 구현방법으로 매우 많이 사용되고 있다.

153) Wil M. P. van der Aalst 외 2명 (2018), Robotic Process Automation, Business & Information Systems Engineering volume 60, pp. 269-272(2018)

〈그림 XII-5〉 RPA가 할 수 있는 작업



출처: 한국지능정보사회진흥원, 공공기관 최초 'RPA활용'업무 혁신 추진 (2019.05.15)

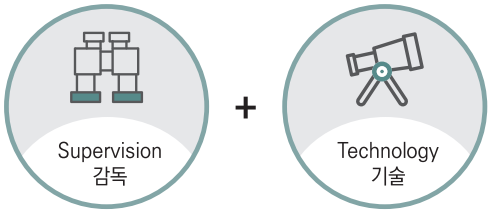
RPA 기술은 금융, 제조 등 민간 기업을 중심으로 외부사이트 신용등급 조회, 엑셀 보고서 작성, 법인카드 및 출장비 처리 등 시간이 오래 걸리고 단순 반복되는 업무를 자동화해 업무 효율성 증대 및 규칙적인 반복 업무를 자동화하여 개발기간이 짧고 즉시 효과를 얻을 수 있다는 장점이 있다. RPA 기술은 중복집행, 오류집행 등 또한 줄일 수 있다. 이러한 장점들은 생산성 향상, 신속성, 일관성 있는 업무 적용에 활용된다.

2 섭테크(SupTech)

2-1 섭테크(SupTech)의 정의

섭테크(SupTech)란, 감독(Supervision)과 기술(Technology)의 합성어를 말한다. 금융감독기구의 주 업무인 감독(Supervision)에 기술(Technology)을 접목해 감독과 검사를 효율적으로 수행하는 것을 말한다. 레그테크가 금융회사의 업무 효율화에 필요한 것이라면, 섭테크(SupTech)는 금융회사들의 감독자인 금융감독기구의 감독업무를 효율화하는 데 사용된다.

〈그림 XII-6〉 감독과 기술의 융합, 섭테크

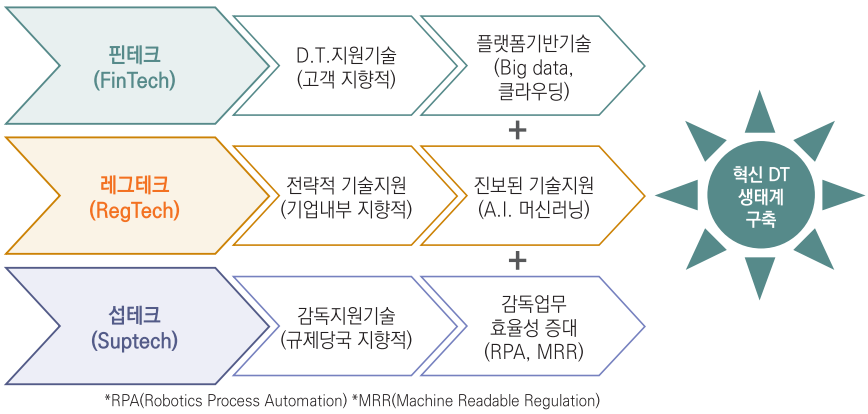


현재 금융회사 등의 핵심적인 업무는 대부분 전산화되어 있으며, 또한 관련 자료도 전자문서 형태로 보관한다. 감독과 검사업무의 대상 자체가 대체로 전산화된 디지털 자료이며 또한 양도 방대하기 때문에 전산화되지 않으면 효율적인 감독업무가 불가능하다. 이러한 현실적 필요에 의해 그림처럼 AI · 빅데이터 기술 등을 통해 규정 위반, 소비자 권익 침해 여부 등을 일차적으로 분석 · 심사한 후 적정성을 판단한다. 이렇게 자동화된 조사를 통해 금융당국은 기계가 대체할 수 없는 고난도 판단이 요구되는 업무에 집중할 수 있게 해준다.

2-2 레그테크와 섭테크(SupTech)

제11, 12장에서 핀테크와 레그테크 및 섭테크를 학습하였다. 공통점은 모두 최신 IT 기술을 이용하여 편리성과 효율성을 증대한다. 차이점은 '해당 기술이 누구를 중심으로 이루어졌는가'이다. 핀테크는 금융소비자인 고객을, 레그테크는 기업을, 섭테크는 규제당국을 지향한다.

〈그림 XII-7〉 핀테크, 레그테크, 섭테크



특히, 금융감독원은 다양한 시스템을 도입하여 섭테크 활용에 노력해 왔다. 예를 들면 '대부업 불법 추심 판별지원' 및 '보험 TM(텔레마케팅) 불완전판매 식별지원'에 음성변환 기술(Speech to Text)을 사용하여 의심되는 통화를 신속하게 식별할 수 있으며, 빅데이터와 인공지능(AI) 및 기계독해(MRC; Machine Reading Comprehension)를 통하여 불법 광고 및 이에 대한 민원 제기를 사전에 예방하는 등 금융감독원의 심사업무 효율화에 활용하고 있다.

2020년 4월 기준, 섭테크 관련 금융감독시스템 현황 및 효과는 다음과 같다.

〈그림 XII-8〉 섭테크 관련 금융감독 시스템 현황 및 효과

섭테크 관련 금융감독시스템 현황

시스템명	가동시기	주요 적용기술
대부업 불법 추심 판별 지원	2019.5.	음성변환
보험 TM(텔레마케팅) 불완전판매 식별 지원	2020.3.	
인터넷 불법 금융광고 감시*	2020.7.	빅데이터
민원 분류 추천	2019.5.	AI, 기계독해
AI 사모펀드 심사 지원	2020.2.	

(자료: 금융감독원, 인공지능(AI)과 빅데이터를 활용한 금융감독 디지털 전환 추진)
*20.3.부터 시범운영중

금융감독 업무에 AI, 빅데이터 등 최신기술을 활용함으로써 다음과 같은 효과를 기대할 수 있습니다.

활용기술	효과
AI	AI의 감독·심사업무 지원을 통한 업무효율 제고
빅데이터	외부 불법 금융 광고 관련 빅데이터를 수집해 조기에 적발·차단함으로써 피해 예방
음성변환	단순 반복적 업무를 자동하하여 업무부담 경감
	불법 추심 불완전판매 사례를 적발하여 금융소비자의 권익 제고

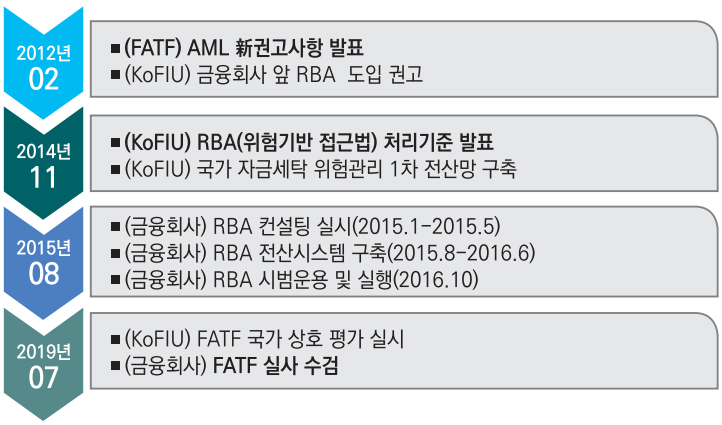
출처: 금융감독원

3 위험기반 접근법(RBA)

3-1 위험기반 접근법(RBA)의 정의

위험기반 접근법(RBA; Risk Based Approach)은 자금세탁방지시스템의 구성 요소 중 위험을 측정하는 방법론 중의 하나이다. FATF(국제자금세탁방지기구)의 2012년 기준 개정 시, 국가적 차원에서 금융회사에 대한 전사적 자금세탁 위험을 효과적으로 통제하기 위해, 전사적 위험기반접근법(RBA) 시스템 도입을 의무화하였고, 2019년 FATF의 한국에 대한 국가 상호 평가 시 점검을 시행하였다.

〈그림 XII-9〉 위험기반 접근법(RBA) 연혁



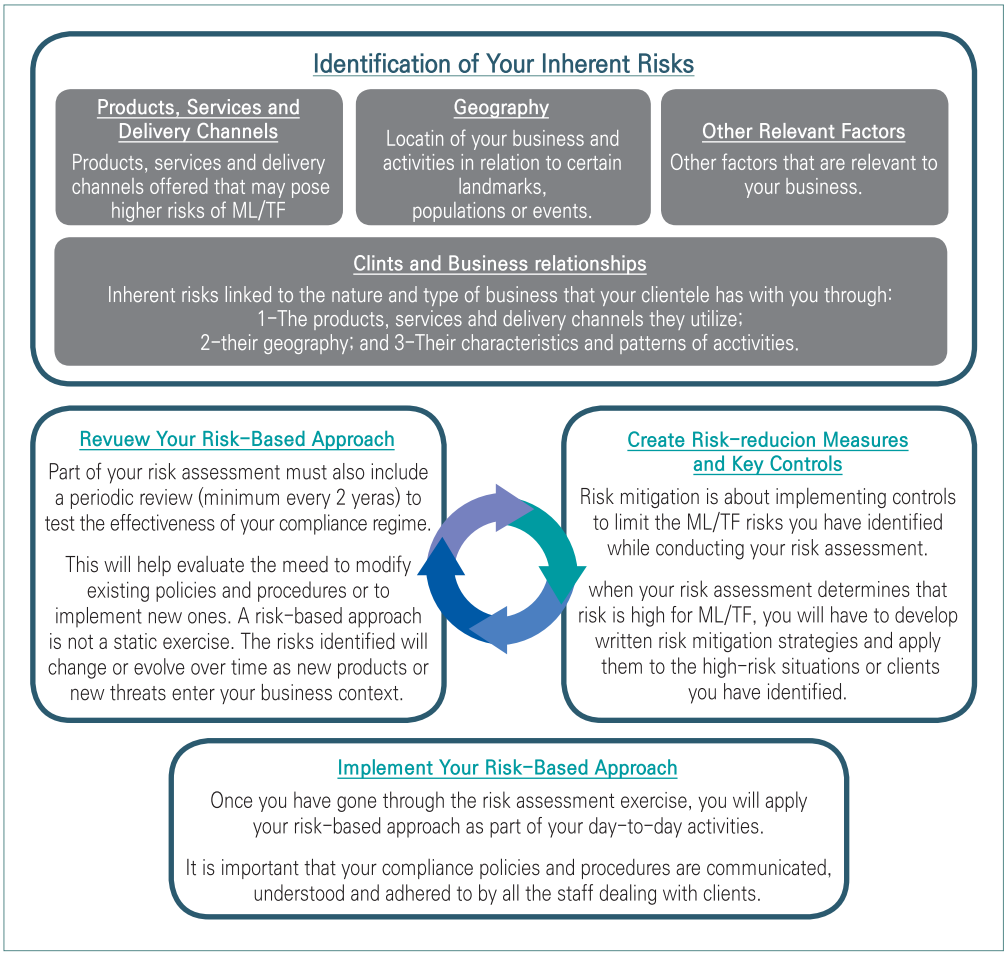
3-2 위험기반 접근법(RBA)의 목적

가. 금융당국과 금융회사 등은 한정된 자원으로 복잡한 자금세탁방지 및 테러자금확산방지(AML/CFT) 체계에 대한 효율적인 감독을 위하여 위험기반 접근법(RBA)을 기반으로 한 평가시스템 구축을 완료하고 '17년부터 본격 운영 중이다.

나. 국제기구 권고기준 준수 및 주기적 평가 대응을 위해 위험평가 시스템을 지속 활용한 위험기반 접근법(RBA)의 감독 체계(평가 · 검사 · 교육)의 확립이 필요하였다.

다. 전사적 자금세탁 위험요인을 식별하고 평가하여 저 위험 영역에는 간소화된 조치를, 고위험 영역에는 강화된 조치를 통한 효율적 위험 감소를 목적으로 한다.

〈그림 XII-10〉 위험기반 접근법



출처: 캐나다 금융거래분석센터(FINTRAC), https://www.fintrac-canafe.gc.ca

위험기반 접근법은 기업의 한정된 자원을 가지고 효율적인 법규 준수를 위하여 위험이 높은 부문에 집중적으로 자원을 투입하는 것이다. 그렇게 하기 위하여 〈그림 XII-10〉과 같이 먼저 법규에 따른 '위험평가 기준을 수립'하고, 그 기준에 따라 기업의 각 부문의 '위험을 식별'하고 새로운 위험의 경우에는 새로운 '위험지표로 정의'한다. 위험지표의 정의가 완료되면 운영위험과 고유위험으로 구성된 '위험평가모형을 정의'한다. 기업은 완성된 이 모형을 가지고 해당 기업의 '위험관리 이행 평가'를 수행한다. 그 결과 고위험으로 분류된 부문에 검사와 교육 등의 자원을 집중적으로 투입하여 개선한다.

제3절

레그테크 적용 방식

1 외국환거래

1-1 핀테크 업체의 법률적 오해

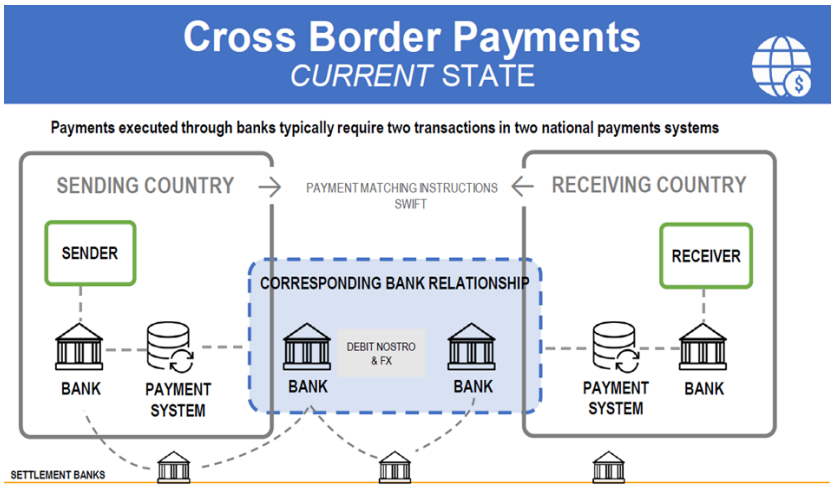
핀테크 업체는 해외송금업에 비교하여 상대적으로 시장진입이 용이했던 국내 송금업에 대해서는 일찍부터 시장에 참가하여 활동해왔다. 전자금융업자는 2006년 4월 28일 제정된 「전자금융거래법」을 근거로 다양한 방법의 국내이체 서비스를 제공해 왔다. 그 이후 세계 유수의 핀테크 업체가 국경 간 자유로운 해외송금 서비스를 제공하자 국내법과 해외 법에 관한 연구 및 대비 없이 기술적으로 구현 가능한 서비스를 금융소비자에게 제공하기에 이르렀다.

특히, 2015년 7월 1일 「외국환거래법 시행령」 개정으로 국내 전자지급결제대행업자(Payment Gateway社)들이 전자상거래에 따른 지급 · 결제 대행 업무를 수행하게 됨에 따라 전자상거래의 범위를 자의적으로 확대하여 해석하거나, 전자상거래가 수반되지 않은 지급 · 결제 업무까지 금융당국의 허가 및 신고 없이 수행하는 지경에 이르렀다.

1-2 금융당국의 고민

이러한 핀테크 업체의 자의적 시장진입 및 서비스 제공에 대하여 정부는 대응이 필요하였다. 2016년 11월 기획재정부는 전자금융업자인 센트비를 비롯하여 13개 업체가 「외국환거래법」을 위반하였다고 보고 금융감독원에 조사를 요청하게 되었다. 이에 2017년 2월에는 일부 핀테크 업체와 유관 협회 등에서 강한 유감의 뜻을 표하기도 하였다. 이러한, 업계의 의견을 수렴하여 금융당국은 제도 개선을 고민하게 되었다.

〈그림 XII-11〉 해외 결제 망을 통한 해외 송금 처리 방식



출처: R3 Korea Members Workshop, Seoul 28 October 2016

1-3 금융당국의 방안 제시

2017년 2월 22일 기획재정부는 소액 해외송금업 제도 구체화 및 외환거래 편의성 제고를 위한 「외국환거래법 시행령」 및 「외국환거래규정」 '개정안 입법 예고'를 발표하였다. 기획재정부는 이 입법 예고를 통하여 소액 해외송금업 제도를 구체화하였으며, 해당 소액 해외송금업의 등록요건, 업무 범위, 거래 안전성 확보 및 소비자 보호방안을 발표하였다. 그중 등록요건 상에 시설 · 인력 요건을 보면 '전산 시설 및 자금세탁방지 체계를 구축하고, 한국은행과 외환 전산망 연결, 외환 전문인력을 확보해야 한다.'라고 등록요건을 명시하고 있다.

2 무역기반 자금세탁방지(TBML)

2-1 정의

세계자금세탁방지 국제기구(FATF)에서는 무역기반 자금세탁방지(TBML; Trade-based Money Laundering)를 "불법적 자금원천을 합법화하기 위하여 정상적인 무역거래로 가장하여 범죄행위를 위장하고 관련 자금을 세탁하는 행위를 말한다."라고 정의하고 있다.

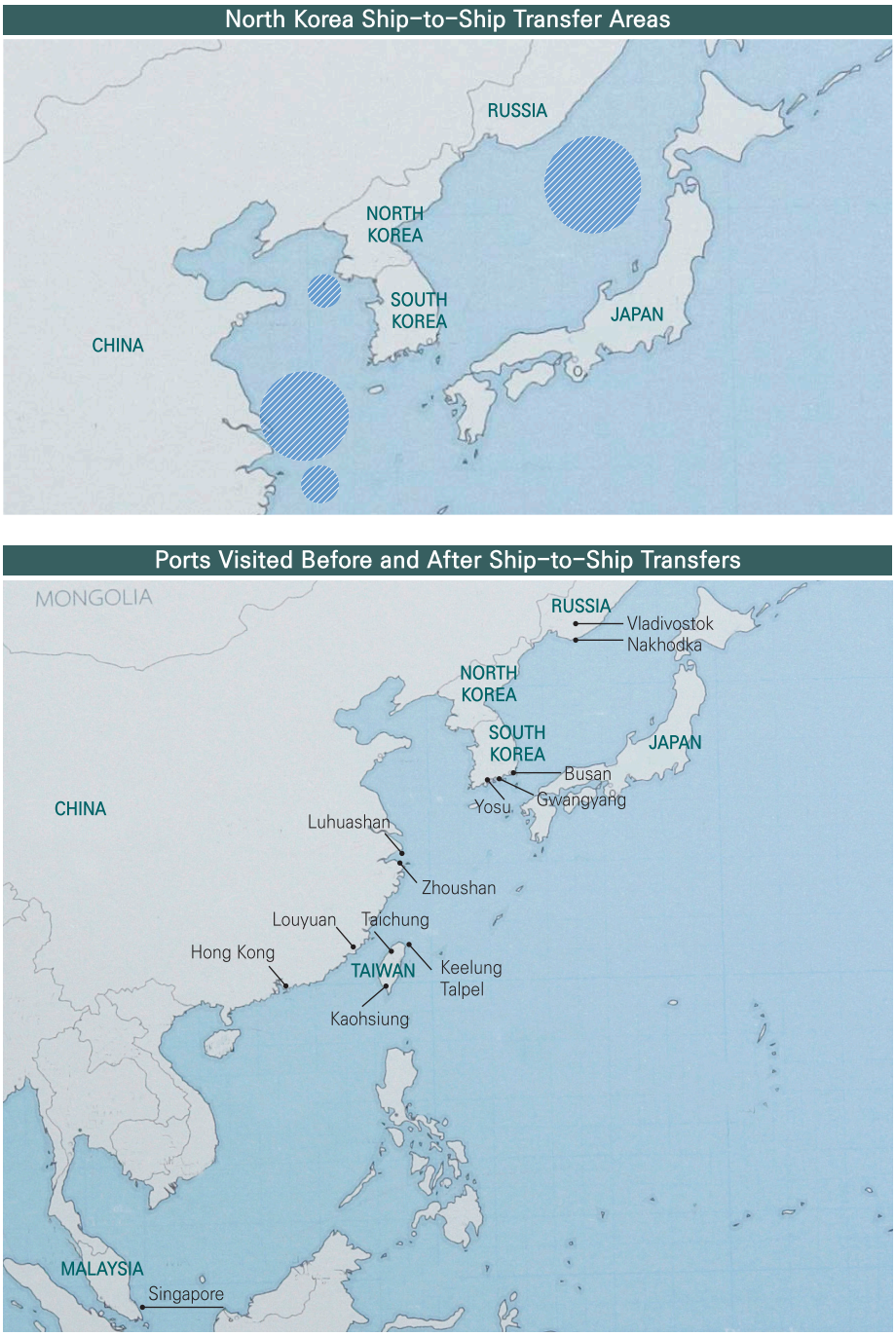
2-2 레그테크 적용 필요성

2019년 3월 12일 유엔 안보리 산하 대북제재위원회의 전문가 패널 연례보고서에 따르면, 2018년 북한은 정제유 수입이 제한되자 유엔 제재를 회피하기 위하여 공해상에서 '선박 대 선박' 방식의 불법 선박 환적을 크게 늘렸다고 보고했다.

2-3 레그테크 활용 기법

이러한 형태의 선박을 통한 불법 환적에 대해서는 인공위성과 빅데이터 분석 등 첨단 추적기법이 사용된다. 대표적인 기업으로는 이스라엘 텔아비브에 기반을 둔 해상교통 분석업체 윈드워드(Windward)나 미국의 유조선 추적업체 탱커트래커스(TankerTrackers), 프랑스 파리의 에너지 연구기관 케이로스(Kayrros) 등이 있다.

〈그림 XII-12〉 불법 환적 선박이 기항한 항구들



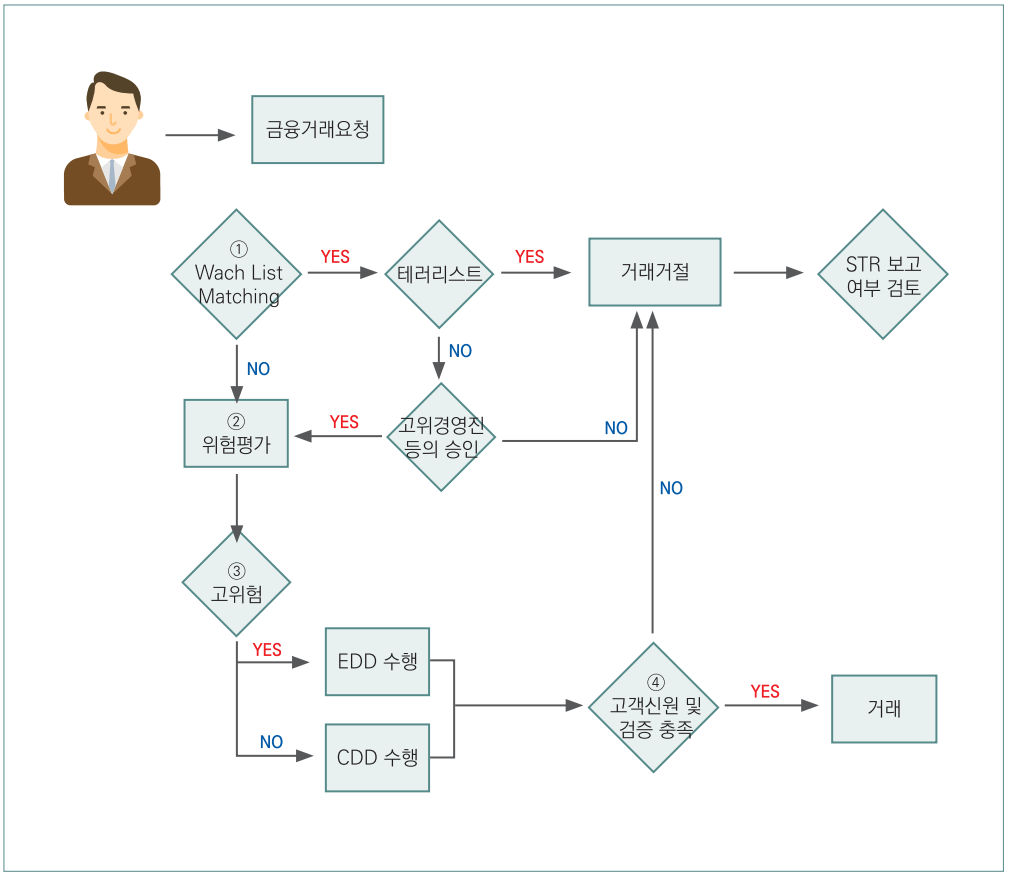
출처: 미재무부(2019.3.21), https://www.treasury.gov/

3 요주의 인물 검색(WLF)

3-1 요주의 인물 검색(WLF) 업무의 정의

요주의 인물 검색(WLF; Watch-list Filtering)이란 고객확인의무를 수행하면서 해당 고객이 자금세탁위험도가 높은 외국의 정치적 주요인물인지, 기획재정부가 고시하는 금융거래제한대상자가 아닌지, 테러리스트 및 경제사범 등의 인물인지 아닌지를 확인하여 금융회사가 그 대상자를 금융회사의 고객으로 수용할 것인지를 결정하는 절차를 말한다.

〈그림 XII-13〉 고객확인제도 수행 절차



출처: 고철수 · 김춘규(2017), 업무에 활용하는 자금세탁방지 가이드, 한국금융연수원

3-2 구축 필요성

해외송금업은 국경 간 자금이동을 비대면 거래방식으로 취급함에 따라 자금세탁 및 테러자금의 통로로 이용될 가능성이 매우 크기 때문에 자금세탁방지 체계구축을 등록요건으로 규정하여 업무의 건전성을 유지해야 할 공익적 필요성이 매우 크다 하겠다. 이러한 공익적 필요성에 의해 해외 송금업자는 필수적으로 고객확인 시스템과 Watch-list Filtering 시스템을 반드시 구축하여야 한다.

4 보이스 피싱(Voice Phishing)

4-1 보이스 피싱(Voice Phishing)의 정의

보이스 피싱은 보이스(Voice)와 피싱[(Phishing; '개인정보(Private Data)'+'낚시(Fishing)']의 합성어로 불법적으로 취득한 개인정보를 이용하여 전화 등을 통하여 선량한 금융소비자를 위계와 사기로 금전적 이익을 취하는 전화금융 사기이다.

4-2 레그테크를 활용한 금융당국의 대응

금융감독원은 선량한 금융소비자의 피해를 막기 위하여 '보이스 피싱 방지 AI 앱'과 '대출사기문자 방지 AI 알고리즘' 개발을 지속적으로 추진하였다. 따라서 금융회사와 IT 기업 등과 함께 음성 및 문자로 이루어지는 금융사기를 파악할 수 있는 AI 앱과 AI 알고리즘 개발을 진행해 왔다. 「보이스피싱 방지 AI 앱」은 2018년 11월 금감원과 기업은행 · 한국정보화진흥원 간 업무협약을 체결하여 개발을 진행하였고 2019년 2월에 보이스피싱 실시간 차단 시스템을 개발 완료하였다. 또한, 「대출사기문자 방지 AI 알고리즘 개발」은 금감원과 국민은행 및 아마존이 협력하여 2018년 11월에 개발을 완료하였다.

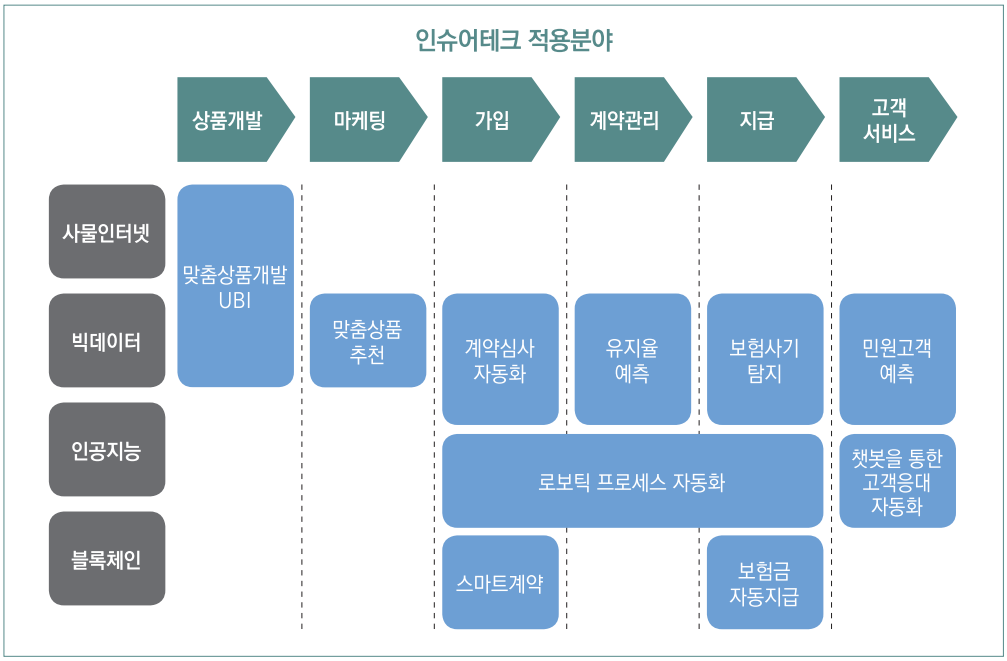
제4절

레그테크의 미래 전망

1 금융분야

레그테크와 관련하여 다양한 시도가 이루어지는 곳은 금융분야이다. 규제 관리와 약관심사 등의 자동화뿐만 아니라 자산관리와 소비자 보호 분야에도 IT를 활용하여 많은 호평을 받고 있으며 특히, 보험업계의 노력은 단순한 규제 준수의 효율성을 넘어서 금융소비자에게 편리함을 제공하는 동시에 법령을 준수하는 단계에 이르렀으며 그러한 측면에서 최근에는 인슈테크(InsurTech = Insurance + Technology)라는 용어를 사용하기도 한다.

〈그림 XII-14〉 보험업계의 레그테크 활용 사례



출처: 금융감독원, 보험회사 인슈어테크(InsurTech) 활용현황(2018.5.21), http://www.fss.or.kr

2 법률 분야

2-1 레그테크와 법률 분야

레그테크의 법률 활용 분야는 크게 '법률 자문'과 '송무 업무' 2가지 부문으로 나눈다. 법률 자문 분야는 최근 몇 년 사이 괄목한 성장을 보이고 있으며, 송무 분야에서는 인공지능을 활용한 다양한 시도들이 이루어지고 있다.

가. 법률 자문 분야

〈그림 XII-15〉에서처럼, 법률 자문 분야에는 단순한 판례 및 사례를 검색해주어 법률의견서 작성에 도움을 주는 '법령 관리' · '리스트 관리' · '리포팅' 기능이 있고, 계약서 검토 및 기업 내의 자문을 수행해 주는 '컴플라이언스 관리'와 '보안'도 있으며, 또한 최신 '블록체인' 기술을 활용한 스마트 계약(Smart Contract) 부문도 새롭게 연구되고 있다.

〈그림 XII-15〉 비대면 이혼 소송 대행업체

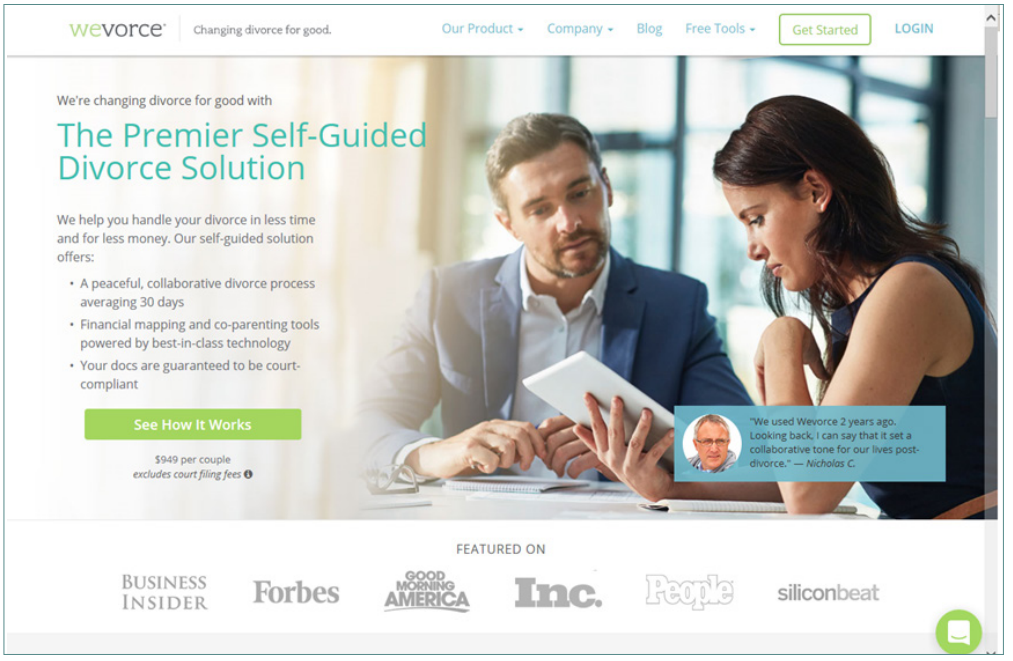
출처: 금융보안원(2017), 금융보안 분야 레그테크 도입 방향, p. 5

나. 송무 분야

그동안 법률 소송을 진행하는 송무 분야는 인간 변호사가 수행하는 고유한 영역으로 간주하였다. 그러나 인공지능의 발달로 송무 분야도 AI의 도전이 강해지고 있다.

〈그림 XII-16〉 예시로 든 위보스(WEVORCE)라는 회사는 이혼 소송을 대신 처리해주는 회사이다. 물론 인터넷으로 이혼 소송을 접수하여 내부적인 처리는 변호사가 진행을 모니터링을 하지만, 이혼 당사자는 이혼 소송이 완료될 때까지 불편한 당사자를 만날 필요도 없으며 재산 분할 합의까지도 온라인으로 이루어진다. 또한, 이혼 비용에서도 오프라인(Off-line) 가격의 1/3인 $949로 변호사 사무실 방문 없이 합의이혼이 가능하다고 광고하고 있다.

〈그림 XII-16〉 비대면 이혼 소송 대행업체



출처: WEVORCE, http://www.wevorce.com

3 인사 분야

3-1 인공지능의 채용 필요성

최근 채용 분야에 인공지능을 도입하는 기업들이 늘고 있다. 물론 채용 응시자 증가로 인한 채용 비용 증가도 하나의 원인이지만, 가장 큰 이유는 2012년 OO통신사 채용 비리, 2016년 OO은행 채용 비리, 2020년 OO전자 채용 비리 수사 등과 같이 채용에 있어서 객관성과 투명성을 담보하는 것이 기업과 조직 경영에 매우 중요한 사안이기 때문이다.

〈그림 XII-17〉 인공지능 채용

출처: 픽사베이(Pixabay)

3-2 인공지능의 측정 방법

인공지능의 측정 방법은 흥미롭게도 동양의 인재 선발 방법론인 신언서판(身言書判)과 매우 유사한 점을 가지고 있다.

가. 신(身)

인공지능은 얼굴의 68개의 지점을 모니터하여 질문에 따른 표정 변화 및 얼굴색 변화 등을 분석한다.

나. 언(言)

준비된 시나리오를 바탕으로 질문을 던지고 응시자의 목소리 변화와 속도 등을 측정하여 언어사용 능력과 감정 상태 등을 분석한다.

다. 서(書)

여러 가지 상황을 제시하고 상황에 대해 어떻게 서술하는지를 사용한 단어와 표현 등을 분석한다.

라. 판(判)

간단한 게임(game)을 실시하여 응시자가 어떻게 대응하는지를 분석한다.

〈그림 XII-18〉 행동경제학적 분석

동양적 관점 신언서판 : 주가+ 경영에 영향을 미치나?

인재의 요건		뜻	신고전파 재무	행동재무
신	身	풍채와 용모	No	키, 얼굴의 남성성, 표정 등이 영향을 미친다.
언	言	언행	No	중저음은 위험선호, 자기과신, 자기 중심적 언행 모두 영향을 미친다.
서	書	글솜씨	No	간단명료, 일목요연하게 보고하는 것이 중요하다.
판	判	판단력 (IQ)	No	당연히 중요하다.
			한마디로, 경영자는 언제나 대체 가능한 생산함수의 투입 요소일 뿐이다	개개인은 특별하고, 경영자의 특질이 회사전반에 미치는 영향은 지대하다.

출처: 김영한(2018), 핀테크와 행동재무 – 기업재무6, 배포자료 p. 11

인공지능은 다양한 방법으로 응시자의 행동을 분석하고 또한 현재 재직 중인 직원들의 채용 데이터와 연관성 및 업무적합도를 분석하여 합격 여부와 적합한 직무 분야도 추천한다.

3-3 인공지능 면접 대응 사례

현재는 채용 부분에 인공지능을 활용하는 기업이 많이 늘어났다. 이에 따라 인공지능 면접 요령을 지도하는 업체도 등장했다.

〈그림 XII-19〉 인공지능 면접 솔루션

출처: 서대문구청 블로그, https://blog.naver.com/sdmstory/222358734429

〈그림 XII-19〉의 예와 같이 이제는 일선 구청에서도 주민들을 위한 인공지능 면접 솔루션을 제공하고 있다. 예비 면접자에게 인공지능 면접 방식을 사전에 연습할 수 있도록 모의 면접 서비스를 제공하고 있다. 이러한 서비스는 사전 모의 면접을 통하여 예비 면접자가 인공지능 면접의 특성을 이해하고 대응 능력을 향상하는 것을 목적으로 하고 있다.

4 범죄 예방 분야

4-1 경찰 범죄 예측 시스템(Pre-crime System)

범죄가 발생하기 전에 미리 인공지능을 통해 빅데이터를 분석하여 경찰 인력의 순찰을 강화하거나 치안 환경을 개선하여 범죄 발생률을 낮추는 시스템이다. 2013년과 2014년에 미국 캘리포니아 알램브라 경찰은 실시간 범죄 예측 프로그램(PREDPOL; Predict Crime in Real Time)을 활용하여 범죄율을 32% 감소시키는 성과를 보았다.

4-2 범죄 예방 환경설계(CPTED)

셉테드(CPTED; Crime Prevention through Environmental Design, 범죄 예방 환경설계)는 범죄예방을 위한 다양한 방법 환경을 설계하고 운영하는 시스템을 말한다. 단순한 디자인에서부터 인공지능 방범 카메라 운영 등 다양한 방법으로 범죄 예방이 가능하다.

2019년 경찰청과 건축공간연구원이 협업해 실시한 연구에 따르면 셉테드 사업이 시행된 서울시 5개 지역의 5대 범죄(살인·강도·강간·절도·폭력) 발생이 최대 54% 가까이 줄어든 것으로 나타났다.[154)]

154) 건축공간연구원, www.auri.re.kr

핵심정리

- **섭테크(SupTech)의 정의**

  섭테크(SupTech)란, 감독(Supervision)과 기술(Technology)의 합성어를 말한다. 금융감독기구의 주 업무인 감독(Supervision)에 기술(Technology)을 접목해 감독과 검사를 효율적으로 수행하는 것을 말한다. 레그테크가 금융회사의 업무 효율화에 필요한 것이라면, 섭테크(SupTech)는 금융회사들의 감독자인 금융감독기구의 감독업무를 효율화하는 데 사용된다.

MEMO

헬로, 핀테크!(보안인증 · 블록체인) HELLO, FINTECH!

헬로, 핀테크!(보안인증 · 블록체인)

HELLO, FINTECH!

13장

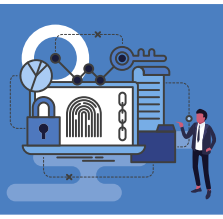
레그테크 관련 법규 및 정책 동향

제1절 레그테크 관련 법규 및 제도

제2절 레그테크 관련 사례 분석

제3절 레그테크 관련 정부 정책 동향

13장 레그테크 관련 법규 및 정책 동향



학습목표

1. 레그테크(RegTech)와 밀접한 법규제들을 이해하고, 레그테크가 해당 법규제와 관련된 업무를 어떻게 도울 수 있는지 설명할 수 있다.
2. 최근 컴플라이언스 이슈에 대하여 알아보고, 해결책으로 레그테크의 도입 방안을 연구하여 설명할 수 있다.
3. 레그테크와 관련된 최근 금융당국의 정책 동향에 대하여 알아보고 설명할 수 있다.

학습개요

이 장에서는 2020년 개정된 데이터 3법(개인정보 보호법, 신용정보법, 정보통신망법)과 「특정금융거래정보의 보고 및 이용 등에 관한 법률」(약칭: 특정금융정보법)에 따른 마이데이터 산업과 가상자산 산업의 발전 방안에 대하여 논의해본다. 데이터 3법과 특정금융정보법은 금융소비자의 개인정보 관리를 규제할 뿐만 아니라, 최근 핀테크의 발전에 따른 비대면 실명확인 및 본인인증 등을 관리하는 법률이므로 레그테크의 활용이 필수 불가결하다.

아울러, 최근 발생한 불완전판매 이슈와 A 은행의 자금세탁 관련 거액의 과태료 처분 건과 초단타(High Frequency) 매매와 관련하여 레그테크의 활용에 대하여 알아본다.

또한, 최근 금융당국(금융위원회, 금융감독원)이 추진하고 있는 레그테크 사업의 주요 사업인 '인공지능 기반의 차세대 심사분석시스템'과 '섭테크(SupTech)'의 주요 사업에 대하여 알아본다.

용어해설

❶ 데이터 3법

데이터 3법이란 4차 산업의 근간이 되는 데이터와 정보의 이용과 보호와 관련된 「개인정보 보호법」(소관: 행정안전부), (「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(약칭: 정보통신망법/소관: 개인정보보호위원회), 「신용정보의 이용 및 보호에 관한 법률」(약칭: 신용정보법/소관: 금융위원회) 개정안을 말한다.

❷ 가상자산

특정금융정보법 제2조의 정의에 따르면 "가상자산"이란 경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표(그에 관한 일체의 권리를 포함한다)를 말한다.

❸ 팻 핑거

'팻 핑거'란 직역을 하면 '굵은 손가락'이다. 일반적으로 주식시장에서 트레이더의 주문 실수를 말하는데 손가락이 두꺼워서 실수로 주문을 잘못 넣었다는 의미다.

제1절

레그테크 관련 법규 및 제도

1 데이터 3법 및 마이데이터

1-1 데이터 3법

가. 정의

데이터 3법이란 4차 산업의 근간이 되는 데이터와 정보의 이용과 보호와 관련된 「개인정보 보호법」(소관: 행정안전부), (「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(소관: 개인정보보호위원회), 「신용정보의 이용 및 보호에 관한 법률」 (소관: 금융위원회)을 말한다.

나. 주요 개정 내용

- **개인정보 보호법**

  가명정보 개념을 도입하고 동의 없이 사용 가능한 목적 범위를 구체화하였다. 또한, 가명정보 이용 시 안전장치 및 통제 수단을 강구하였으며, 개인정보의 관리 감독을 '개인정보보호위원회'로 일원화하였다.

- **신용정보법**

  금융분야의 빅데이터 분석을 이용할 법적인 근거를 명확히 하였다. 또한, 신용정보 통합조회(일명: 마이데이터)를 도입하고 금융분야의 관련 규제를 정비하였으며, 신용 주체자의 본인정보에 대한 통제 기능을 강화하였다.

- **정보통신망법**

  기존의 개인정보 보호 조항은 「개인정보 보호법」으로 이관하고, 온라인 이용자들의 개인정보에 대한 규제와 감독 권한을 '방송통신위원회'에서 '개인정보 보호 위원회'로 이관하였다.

1-2 마이데이터(MyData)

가. '본인신용정보관리업' 신설

2020년 8월 5일부터 신용정보법의 개정 시행에 따라, 개정된 법률에 근거하여 본인신용정보관리법(속칭, '마이데이터')이 시행되었다. 마이데이터(MyData)는 신용정보의 주체가 자신의 권리행사에 따라 개인신용정보를 수집하고, 수집된 정보를 신용정보 주체가 조회와 열람 등을 제공하는 행위를 영업으로 하는 새로운 산업이다. 이와 같은 마이데이터 산업을 영위하려는 자는 금융위원회로부터 관련 허가를 득하여야 한다.

나. '본인신용정보관리업'의 기대 효과

- **금융소비자 측면**

  금융소비자의 주권이 강화되어서 금융회사가 보관하고 있는 소비자의 정보에 대한 통제권과 활용성이 강화되어 소비자 권익이 향상된다.

- **금융 산업 측면**

  금융 산업 내 존재하였던 많은 데이터를 빅데이터로 활용 가능하다.

〈그림 Ⅷ-1〉 신용정보법 개정에 따른 소비자의 기대효과

출처: 금융위원회, 신용정보법 개정에 대비하여 금융분야 마이데이터(MyData) 산업 도입 준비(2019.10.16), http://www.fsc.go.kr

다. '본인신용정보관리업'의 정보보호 강화

총자산이 2조원이 넘는 마이데이터 서비스 사업자는 '신용정보관리 · 보호인'을 둬야 한다. '신용정보관리 · 보호인'은 데이터의 체계적 보안 관리와 사고 예방을 위해 모든 정보 제공 및 활용, 보호와 관리 업무를 총괄한다.

2 특정금융정보법과 레그테크

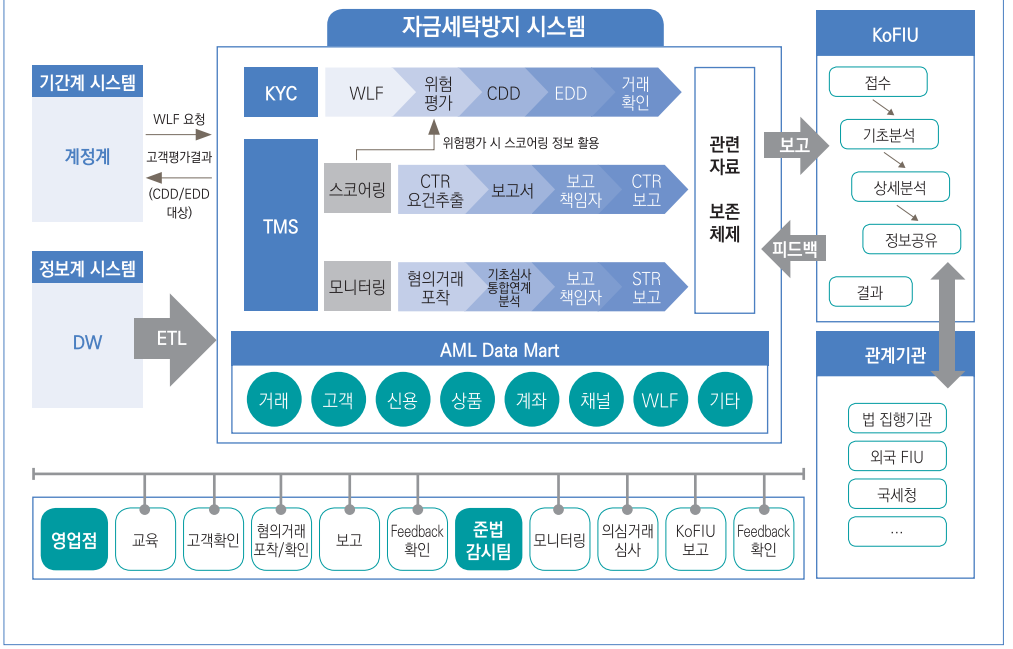
2-1 국내 자금세탁방지 관련 법

국내의 자금세탁방지와 관련된 법은 국제자금세탁방지기구(FATF)의 권고안(Recommendation)을 참고하여, 「공중 등 협박목적 및 대량살상무기 확산을 위한 자금조달행위의 금지에 관한 법률」(약칭: 테러자금금지법), 「범죄수익 은닉의 규제 및 처벌 등에 관한 법률」(약칭: 범죄수익은닉규제법), 「국민보호와 공공안전을 위한 테러방지법」(약칭: 테러방지법) 및 「특정금융거래정보의 보고 및 이용 등에 관한 법률」(약칭: 특정금융정보법) 등으로 구성되어 있다.

일반적인 시중 은행의 자금세탁방지 시스템[155]은 〈그림 Ⅷ-2〉와 같은 구성을 갖추고 있다.

155) [솔루션리뷰] "지티원 자금세탁방지 솔루션, 'AMLExpress 4.0'", 컴퓨터월드(2015. 5. 31.), http://www.comworld.co.kr/news/articleView.html?idxno=48785

〈그림 XIII-2〉 자금세탁방지 시스템 구성도



2-2 가상자산 관련 특정금융정보법 개정

2019년 6월 21일 발표된 국제자금세탁방지기구(FATF)의 권고안 개정에 따라 주관부서인 금융위원회 산하 금융정보분석원(KoFIU)은 국회와 협력하여 지속적으로 입법화를 추진하였다. 제20대 국회에서는 제운경 · 전재수 · 김병욱 · 김수민 국회의원 등이 가상자산 관련 자금세탁방지 입법 활동을 시도하였다. 입법안들은 2019년 11월 25일자 국회 정무위원회 전체회의를 통해 정무위원장 안으로 통합 개정되었으며, 이 수정안이 법제사법위원회 심사와 국회 본회의를 통과하여 2020년 3월 24일 자로 특정금융정보법이 개정되었다. 개정된 특정금융정보법은 2021년 3월 25일 자로 시행되었다.

2-3 가상자산의 정의와 특징

가. 가상자산

특정금융정보법 제2조의 정의에 따르면 "가상자산"이란 경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표(그에 관한 일체의 권리를 포함한다)를 말한다.

〈그림 Ⅷ-3〉 가상자산(Virtual Asset)의 정의와 범위

나. 가상자산의 특징

가상자산은 비대면성과 익명성 및 편의성과 활용성이 높아 마약 거래 등 불법 거래에 이용되고 가상자산 사업자를 통해 현금화되는 등 가상자산이 자금세탁에 이용될 가능성이 매우 크다.

2-4 가상자산 관련 특정금융정보법의 주요 개정 내용

가. 금융회사의 높은 수준의 주의 의무

금융회사에게 가상자산 사업자에 대하여 특별한 주의 의무를 부여하고, 가상자산 사업자가 '정보보호 관리체계 인증'을 획득하지 못하거나 '실명확인 입출금계정 서비스'를 이용하지 않거나, 가상자산 사업자가 '신고 불수리 및 직권 말소' 상태일 때 의무적으로 거래를 거절하도록 하였다.

〈그림 Ⅷ-4〉 정보보호 관리체계 인증 및 법적 근거

법	정보통신망법 제47조	정보통신망법 제47조	개인정보보호법 제32조의2
하위법령	시행령 제47조 ~ 54조 시행규칙 제3조	시행령 제54조의2	시행령 제34조의2 ~ 제34조의 7
고시	정보보호 및 개인정보 보호 관리체계 인증 등에 관한 고시		

나. 가상자산 사업자 관련 신고제

FATF의 가상자산 사업자에 대한 신고제 등을 통한 실효적 감독과 제도 운용 요청을 반영하여, 미신고(또는 등록 등) 영업 시 처벌하는 조항과 범죄 경력자의 가상자산 관련 사업의 진입을 금지하였으며, 당국의 신고 말소 및 제한 권한 규정을 신설하였다.

2-5 금융회사의 가상자산 사업자 위험 평가 방법 및 절차

가. 금융회사의 가상자산 사업자 위험 평가 방법

특정금융정보법 제7조(신고)에서 정한 '대통령령으로 정하는 금융회사 등'은 동법 제5조(금융회사 등의 조치 등)에 따라 가상자산 사업자에 내재된 자금세탁행위와 공중협박자금조달행위의 '위험을 식별, 분석, 평가하여 위험도에 따라 관리 수준을 차등화' 하여야 한다.

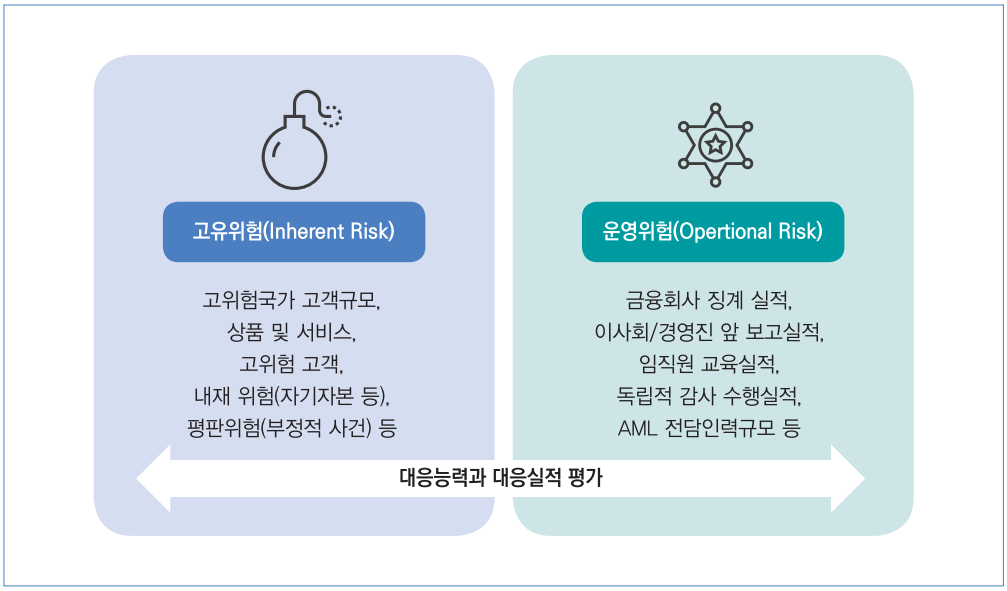
이러한 위험평가 방법론(RBA: Risk Based Approach, 위험기반 접근법) 중 대표적인 방식으로는 '금융정보분석원의 RBA 평가 방식', '환거래 은행 평가방식'과 '은행연합회점검 방식' 등이 있다.

나. 금융회사의 가상자산 사업자 위험 평가 절차

금융회사는 여러 가지 위험평가 방법론 중에서 적절한 방법론을 선택하여 '실명확인 입출금계정'의 사용을 신청한 '가상자산 사업자'에 대하여 '자금세탁 및 공중협박자금조달 행위'의 위험을 식별, 분석 및 평가하여야 한다. 금융회사의 실사절차 및 필수 검토 사항은 특정금융정보법 시행령에서 정한 검토 항목과 금융회사가 자체적으로 내규로 정한 검토 항목 및 절차를 따른다.

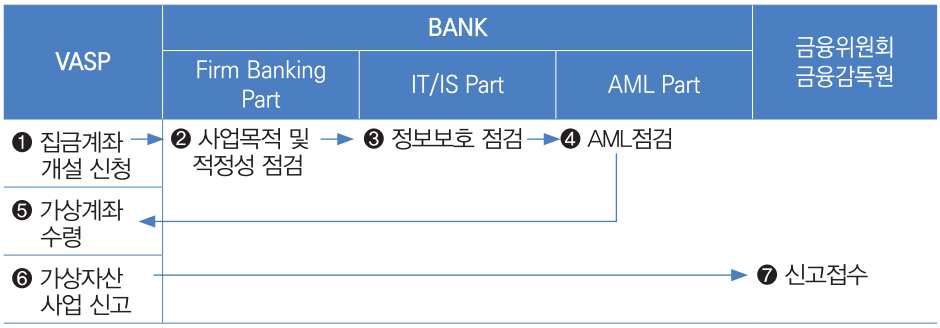
금융회사는 평가 결과 적정하다고 판단되면 가상자산 사업자에게 '실명확인 입출금계정 발급 획인서'를 발급하고, 가상자산 사업자는 금융위원회 앞 신고서 접수 시 해당 서류를 제출한다.

〈그림 Ⅷ-5〉 금융정보분석원의 RBA 평가 방식 사례



〈그림 Ⅷ-6〉 금융회사의 가상자산 사업자 실사 절차 및 검토 내용

은행 심사 절차



필수 검토 내용

구분	Firm Banking Part	IT/IS Part	AML Part
시형령	예치금 구분 관리	정보보호 관리 체계	AML 위험·식별 분석평가
	신고 불수리 요건	고객별 거래내역 분리	KOFIU 업무규정
내규	가장계좌 이용 계약(서)	정보보안 업무규정	신규상품 및 서비스에 대한 사전 위험평가 체크리스트

제2절

레그테크 관련 사례 분석

1 불완전 판매

1-1 최근 사례

2020년은 해외금리 연계 파생결합상품(DLF; Derivative Linked Fund, DLS; Derivative Linked Securities)에 연이은 L자산운용 사모펀드의 환매중단 사태로 금융권이 흔들렸다. 이러한 불완전 판매 또는 불법행위는 금융소비자에게 미치는 피해가 엄청나지만 조기에 발견하거나 대처하기에는 현재 감독체계로는 매우 어렵다. 이러한 불완전 판매 문제 대응하고자 인공지능 기법 등을 활용한 방안 등 다양한 방법들이 시도되고 있다.

〈그림 Ⅷ-7〉 환매연기 母펀드 및 子펀드 현황('19.12말 기준)

(단위: 개, 억원)

子펀드		
펀드명	펀드수	금액
TOP2 밸런스 6M 35호 등	110	10,091
새턴 10호 등	21	3,207
무역금융 밸런스 6M 5호 등	38	2,438
Credit Insured 1Y 1호 등	16	2,949
합계*	173	16,679

母펀드		
펀드명	금액	주요 투자자산
① 플루토 FI D-1호	9,391	국내 사모사채
② 테티스 2호	2,963	국내 메자닌
③ 플루토 TF-1호	2,408	P-note (약속어음)
④ Credit Insured 1호	2,464	해외 무역채권
합계	17,226	

* 1개의 子펀드가 복수의 母펀드에 중복 투자한 경우 중복을 제거하고 합계를 산출

출처: 금감원, 라임자산운용에 대한 중간 검사결과 및 향후 대응방안(2020.2.14), http://www.fss.or.kr

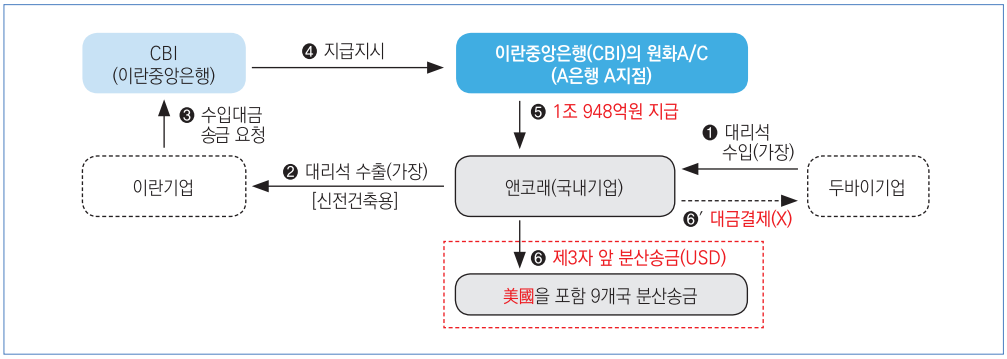
1-2 대응 방안

2019년 11월에 IT기업인 S사는 금융사의 금융상품 불완전 판매에 '딥러닝 기반의 모니터링 기법' 도입을 제안했다. 발표에 따르면, 보험사의 비대면 영업상의 불완전 판매에 대한 점검은 현재 직원의 수행률 20%에서 인공지능 도입 시 100% 수행률을 달성하였음을 보였고, 보험심사에 자연어 처리와 정형 데이터 분석을 통한 예측모형 도입으로 인수심사 시간을 건당 평균 2분에서 1초로 단축하였다고 발표했는데 이러한 방법 등이 대안으로 모색되고 있다.

2 국제 제재(Sanction)

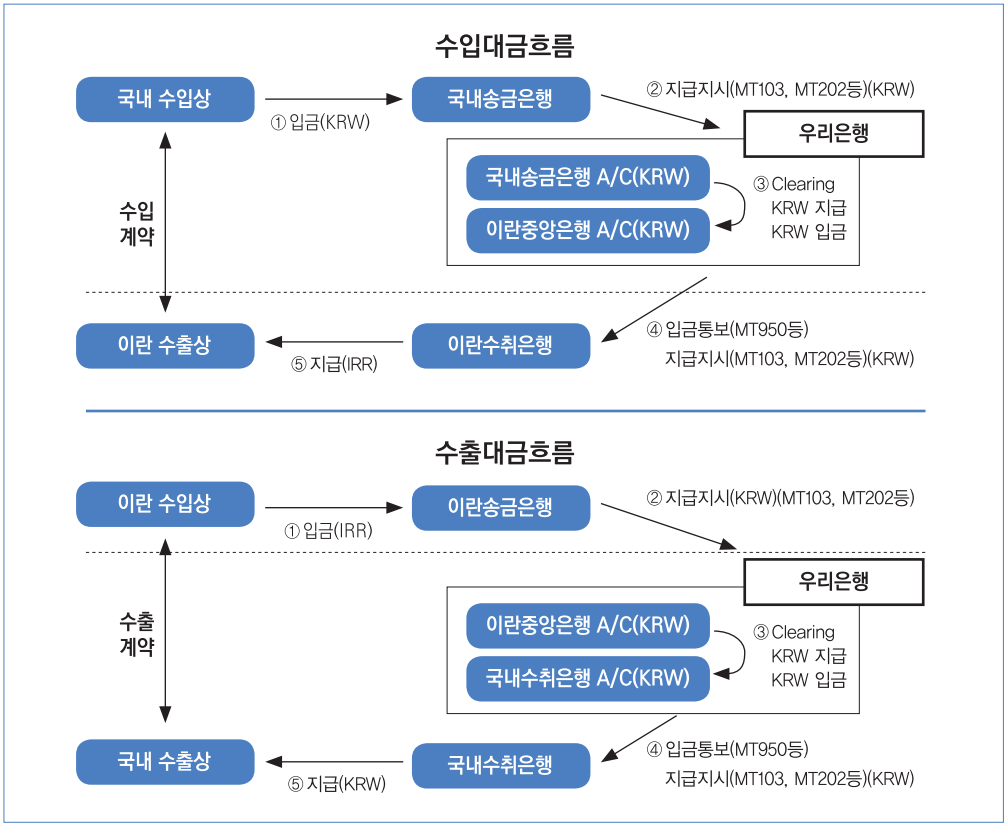
2-1 국내 은행 자금세탁방지 위반 사례

〈그림 XIII-8〉 A 은행의 과태료 처분 사례



2020년 4월 국내의 A 은행이 자금세탁방지 위반으로 미국 사법당국과 금융당국으로부터 1,049억원이라는 거액의 과태료 처분을 받았다. 이란은 2007년 10월 25일부터 미국으로부터 강력한 경제제재를 받고 있었다. 2010년 8월 17일에는 미국의 포괄적 이란제재법 시행세칙 연방관보 게재에 따라 한국에 있는 멜라트은행 서울지점이 폐쇄되었다. 멜라트은행 서울지점의 폐쇄는 한국이 더 이상 이란으로부터 수출입 거래를 할 수 없게 되었다는 것이다. 그래서 한국은 2010년 1월 1일 미국의 허가와 이란과의 협의에 따라 〈그림 XIII-7〉와 같은 방식으로 대이란 원화결제 방식을 도입하여 결제대금을 정산하였다.

〈그림 Ⅷ-9〉 대이란 원화결제 방식



출처: 전략물자관리원(2010). 對이란 확인서발급 및 대금결제 관련 설명회 자료, 산업통상자원부, p. 65

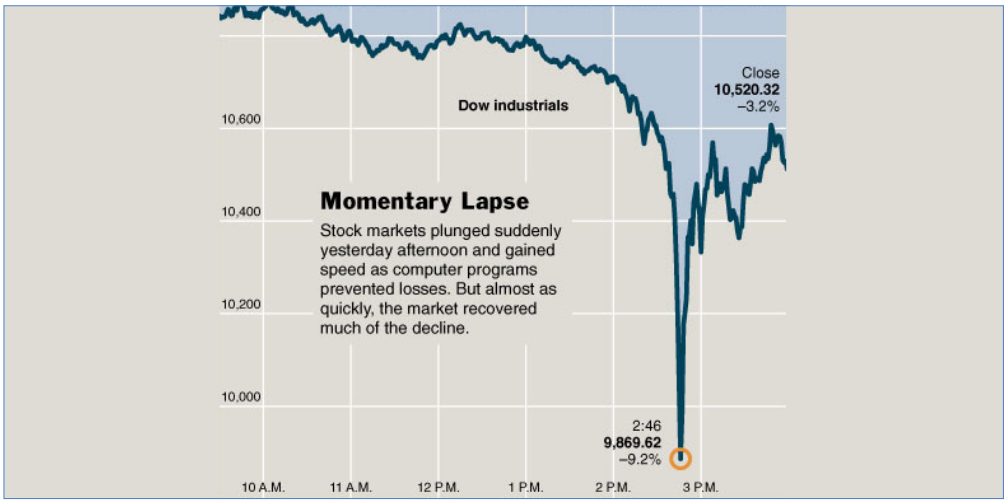
이러한 대이란 원화결제 방식으로 수출입대금을 결제하던 중, 국내 무역업체 앤코래가 이란기업에 대리석을 수출하는 것(중계무역)을 가장하여 A 은행의 이란중앙은행 명의의 원화계좌에서 1조 948억원(2011년 2월 ~ 7월, 총 87건)을 인출하여 9개국에 미국 달러로 불법 송금하였다. 이와 관련하여 2013년 1월에 서울중앙지검이 앤코래 대표 정OO씨를 「외국환거래법」 위반으로 구속하고 A 은행은 무혐의 처분하였다. 이후 2014년 5월에 금융감독원은 A 은행 직원을 제3자 앞 송금에 대한 한국은행 신고 및 확인 누락으로 징계처분하였다. 또한, 2014년 11월에는 미국의 연방 및 뉴욕 검찰이 비록 제3국에서 발생한 거래이지만 미국 금융 시스템을 이용했다는 이유로 수사를 진행해왔다. 최종적으로 2020년 4월 A 은행은 미국 뉴욕지점의 이란 제재 위반 혐의와 관련하여 8,600만달러(한화 약 1,049억원)의 과태료를 납부하기로 최종 합의하였다.

3 휴먼에러와 불공정 거래

3-1 팻 핑거(Fat Finger)와 금융범죄

팻 핑거는 직역을 하면 굵은 손가락이다. 일반적으로 주식시장에서 트레이더의 주문 실수를 말하는데 손가락이 두꺼워서 실수로 주문을 잘못 넣었다는 의미다. 한동안, 팻 핑거의 대표적인 사례로 2010년 5월 6일 뉴욕 주식시장에서 한 트레이더가 백만(1M) 단위 거래를 십억(1B) 단위로 잘못 주문을 넣은 것이 매매 프로그램의 연쇄 반응을 일으켜 다우지수를 폭락시킨 '플래시 크래시(Flash Crash)'가 대표적 사례로 회자하였다(〈그림 XIII-8〉).

〈그림 XIII-10〉 플래시 크래시(Flash Crash)



출처: THE NEW YORK TIMES

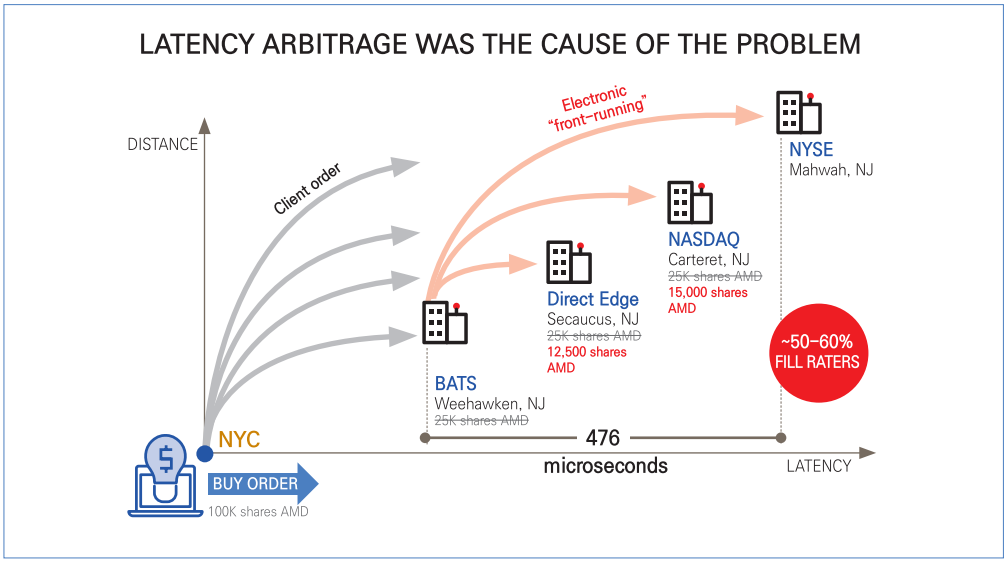
그러나 5년 뒤인 2015년 4월 21일 영국 런던에서 주범인 나빈더 싱 사라오가 체포되었다. 나빈더 싱 사라오는 2010년 5월 6일에 약 88만달러의 불법 이익을 챙겼고 그 이후 2014년까지 총 4천만달러의 금융범죄를 저질렀다. 그는 범죄기법으로 초단타 매매 기법을 사용하였다.

3-2 초단타(High Frequency) 매매

가. 초단타 매매의 원리

〈그림 Ⅻ-9〉에서 보듯이, 뉴욕시(NYC)에 거주하는 고객이 대량의 매수 주문을 넣으면, 실제로는 뉴저지에 존재하는 4개의 거래소 중에 제일 먼저 'BATS 글로벌 마켓 증권거래소'에 도착하고 제일 마지막에 제일 거리가 먼 '뉴욕증권거래소(NYSE)'에 도달하게 된다. 이 백만분의 1초(마이크로세컨드)라는 찰나(刹那)의 시간에 기존의 매도 거래를 취소하고 매도 가격을 높여 버리는 수법으로 부당이익을 얻는다.

〈그림 Ⅻ-11〉 초단타 매매의 원리



출처: Investors Exchange(IEX) Building A Market that Works for Investors

이처럼 초단타 매매는 주식거래소 전용 초고속 통신망과 고성능 컴퓨터를 기반으로 자동화된 복잡한 알고리즘을 사용해 믿기 어려울 정도로 짧은 시간 동안 수백 번에서 수천 번의 거래를 하며 매매차익을 내는 투자방식이다.

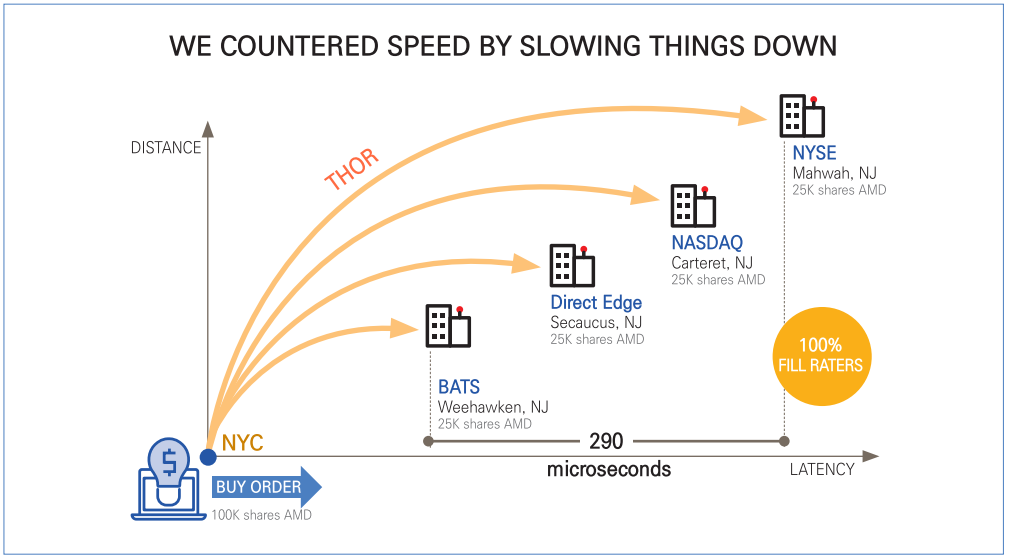
예를 들어, 어떤 투자자가 A 주식 300만 주를 일괄매각하고자 하는데 시장에는 100만 주의 매수세가 있는 경우, 주식중개인은 전체 주식을 일괄 매수해 일단 100만 주만 판 다음 나머지

200만 주는 시장상황을 봐가며 분할 매도한다. 이렇게 하려면 시장의 매수 물량을 정확하게 파악해야 한다. 그런데 엔터키를 누르는 1초도 되지 않는 짧은 순간에 매수 물량이 모두 제로가 되어버린다면 정상적인 거래를 할 수 없다. 하지만 초단타 매매 트레이더들이 백만분의 1초도 안 되는 시간을 악용해 엄청난 부당이익을 얻었다.

나. 초단타 매매의 방지책

증권거래소 간의 거리의 차이와 거래소 간의 매매 체결 시간의 차이를 이용하는 초단타 매매의 방지책은 멀리 있는 거래소에서 먼저 거래를 체결하고 거리의 역순으로 가장 가까운 거래소는 가장 마지막에 주문 거래를 체결하는 방법으로 해결하게 되었다.

〈그림 XIII-12〉 초단타 매매의 방지책



출처: Investors Exchange(IEX) Building A Market that Works for Investors

이처럼 금융 범죄도 최첨단화하고 있어 과거에 대응하던 방식으로는 금융 범죄를 막을 수 없다. 이와 같은 범죄를 막기 위해 인공지능과 고성능 컴퓨팅 능력이 바탕이 되는 레그테크의 필요성이 점점 커지는 상황이다.

제3절

레그테크 관련 정부 정책 동향

1 금융위원회

1-1 금융정보분석원의 인공지능 분석 시스템

가. 목적

금융위원회 산하 금융정보분석원(KoFIU: Korea Financial Intelligence Unit)은 금융회사 등으로부터 자금세탁과 관련된 의심거래 자료를 수집하고 분석하여 합리적 의심이 있는 건을 법집행기관에 제공하여 자금세탁행위에 대한 실질적인 방지를 목적으로 하는 기관이다.

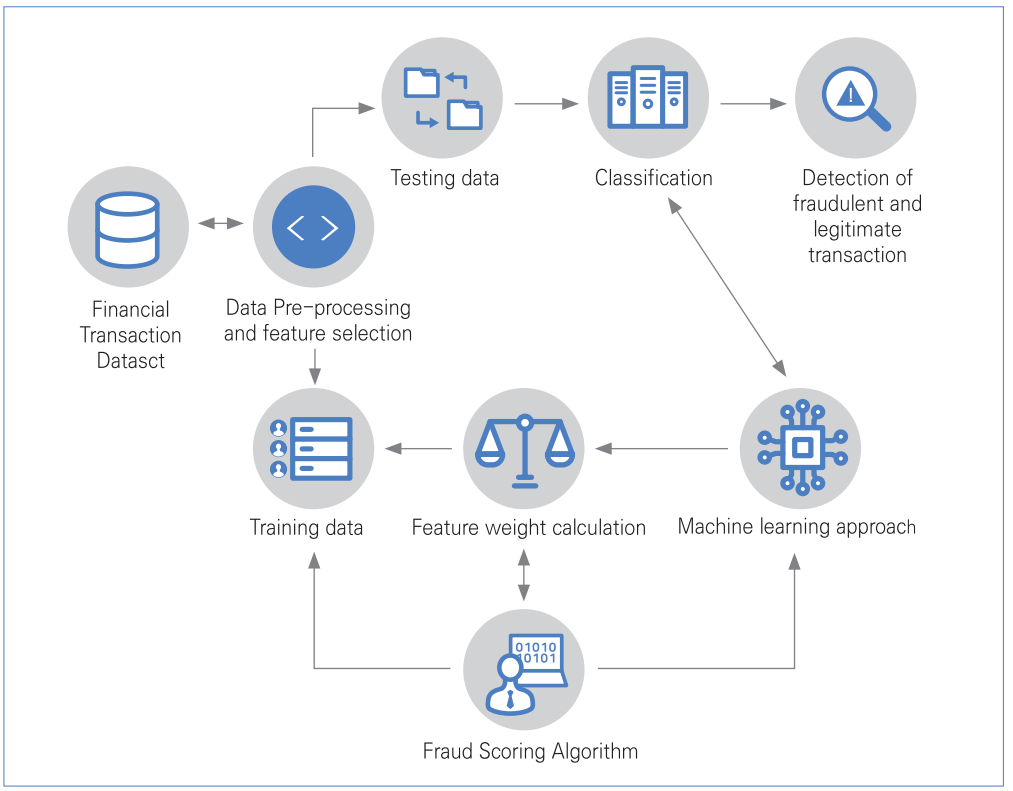
나. 기능

과거에 사용했던 시스템은 2002년 구축한 시스템으로 이번 개편을 통하여 2021년 상반기에 인공지능과 빅데이터 등의 기술을 반영한 차세대 심사분석 시스템[156]을 도입하였다.

156) FIU, 차세대 자금세탁방지시스템(2021.01.08.)

1-2 레그테크 고도화

〈그림 XIII-13〉 Architectural design of the model



출처: Aderonke Thompson 외 3명(2019),
A Fraud Detection Framework using Machine Learning Approach, IARIA, p. 15

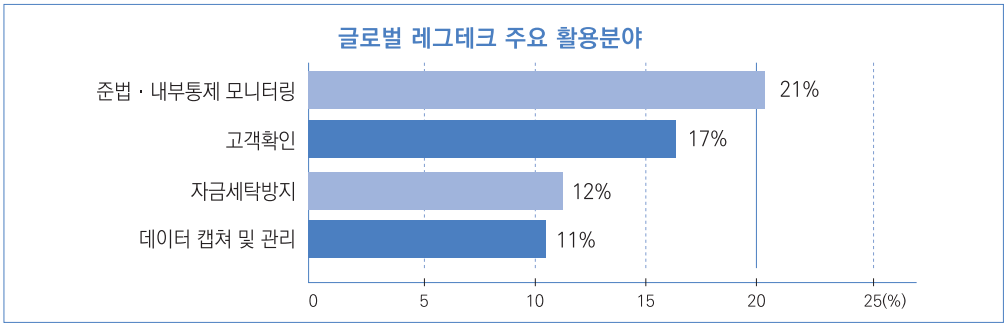
가. 금융혁신 가속화를 위한 핀테크 스케일업 추진전략

금융위원회는 2019년 12월 4일 그간의 4차 산업혁명을 위한 혁신성장 노력의 성과를 바탕으로 핀테크 기업과 금융회사의 금융혁신을 선도하기 위하여 핀테크 시장과 산업의 Scale-up 전략을 도입 · 발표하였다. 이 발표를 통해 금융규제 샌드박스, 오픈뱅킹 도입 및 규제개선의 디지털 금융혁신을 강조하였다. 344개의 금융회사 등이 레그테크를 통해 보안규제 준수 여부의 자체점검 등에 활용 중이며, 금융위원회는 금융회사의 보안수준과 규제현황을 자동으로 점검하고 분석하는 금융보안 레그테크 고도화를 통해 자율보안역량을 강화토록 독려하고 있다.

나. 국내외 금융권 레그테크 적용분야, 활용 동향 등 연구

금융위원회는 레그테크 기술을 활용한 AI기반의 자금세탁방지(AML) 및 고객확인(KYC) 등의 활용범위 확대를 추진하고 있다.

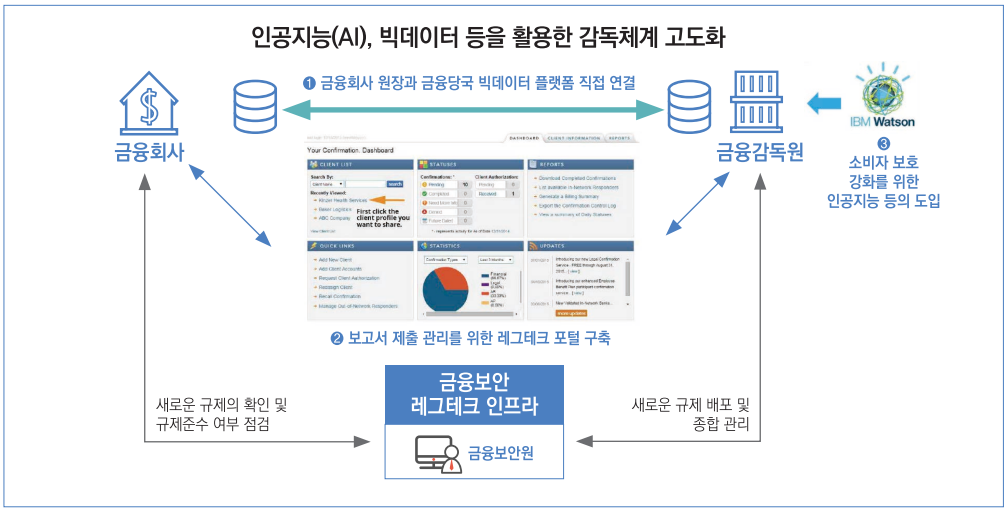
〈그림 XIII-14〉 레그테크 주요 활용분야



출처: Thomson Reuters

2 금융감독원 동향

〈그림 XIII-15〉 인공지능과 빅데이터를 활용한 감독체계



출처: 김용태, 레그테크 활성화를 위한 금융당국의 역할, 금융감독원(2017.10.19)

2-1 섭테크 활성화 방안

가. 인공지능 약관 심사 시스템 시범 구축

금융회사 등이 금융감독원에 제출한 각종 약관을 데이터로 자동 변환한 후 인공지능 컴퓨터가 규정 위반 여부 및 소비자 권익 침해 여부 등을 심사 분석하는 시스템을 구축하고자 한다.

나. 금융 감독 챗봇(Chatbot) 시범 구축

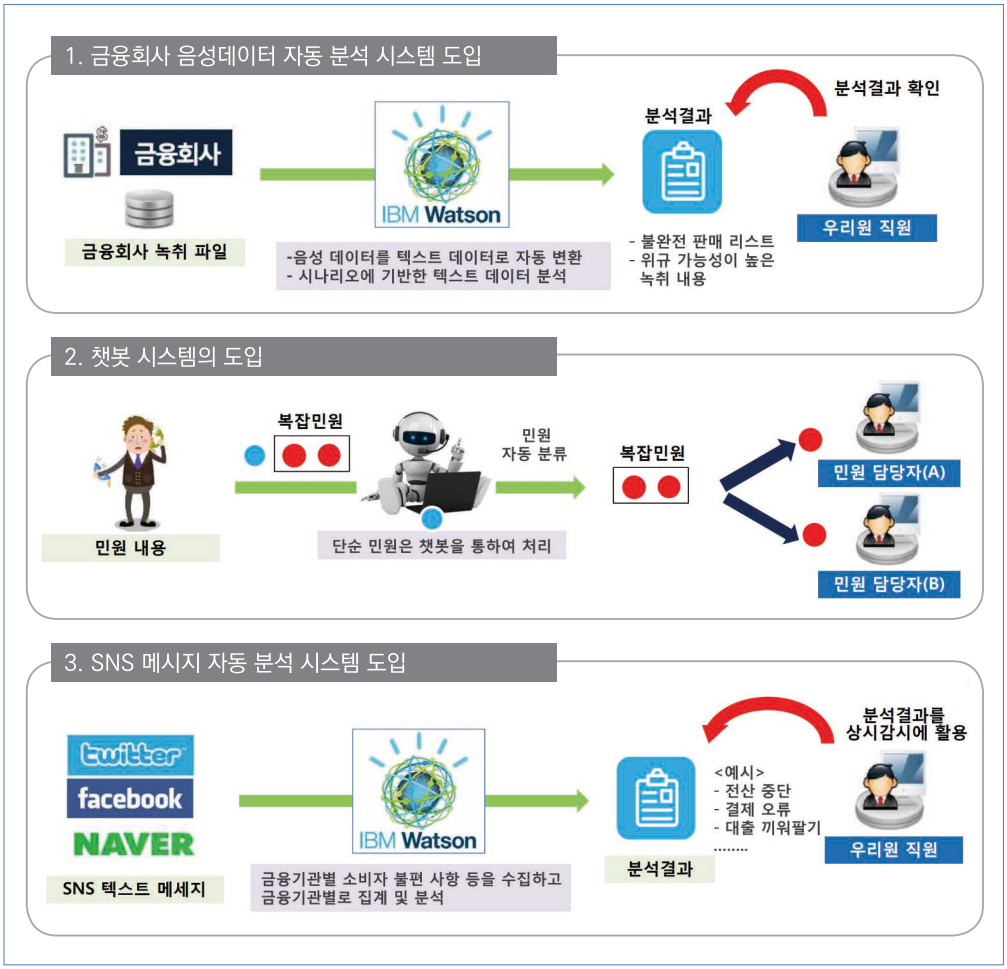
금융 감독 임직원뿐만 아니라 금융소비자와 금융 회사 등의 질의에 대하여 인공지능이 해답과 자료를 자동으로 제공하는 챗봇 시스템을 개발 중이다. 특히, 금융소비자들이 자주 질문하는 내용은 자연스러운 대화형으로 구현하고자 한다.

다. 전자금융 금융사기 방지 알고리즘 개발

휴대폰 문자이용 사기 및 개인금융정보 탈취와 같은 스미싱 등 다양한 형태의 금융사기를 사전에 자동으로 차단하는 알고리즘을 개발하여 스타트업 회사 등에게 무료로 제공하고자 한다.

2-2 인공지능(AI), 빅데이터 분석을 활용한 소비자 보호 강화

〈그림 Ⅷ-16〉 인공지능과 빅데이터를 활용한 소비자보호



출처: 김용태, 레그테크 활성화를 위한 금융당국의 역할, 금융감독원(2017.10.19)

소비자 분쟁 발생 시 혹은 분쟁 발생 전에 금융회사의 음성데이터를 인공지능 컴퓨터가 자동으로 분석하거나 소셜 네트워크 서비스상에서 불완전판매 및 위규 가능성이 높은 건에 대하여 인공지능을 활용하여 사전적 소비자 보호를 강화하는 방안을 추진 중이다.

핵심정리

1. 마이데이터(MyData) 산업

- **본인신용정보관리업**

2020년 8월 5일부터 신용정보법의 개정 시행에 따라, 개정된 법률에 근거하여 '본인신용정보관리법(속칭, '마이데이터')이 시행된다. 마이데이터(MyData)는 신용정보의 주체가 자신의 권리행사에 따라 개인신용정보를 수집하고, 수집된 정보를 신용정보 주체가 조회와 열람 등을 제공하는 행위를 영업으로 하는 새로운 산업이다. 이러한 마이데이터 산업을 통하여 금융소비자는 본인의 정보에 대한 통제권과 활용성이 강화되어 소비자 권익이 향상된다.

2. 자금세탁방지 관련 국제 제재(Sanction) 준수의 중요성

- **국내 A 은행의 거액 과태료 사례**

2014년 11월에는 미국의 연방 및 뉴욕 검찰이 비록 제3국인 한국에서 발생한 거래이지만 미국 금융시스템을 이용했다는 이유로 수사를 진행해왔다. 최종적으로 2020년 4월 A 은행은 미국 뉴욕지점의 이란 제재 위반 혐의와 관련하여 8,600만달러(한화 약 1,049억원)의 과태료를 납부하기로 최종 합의하였다. 미국 금융시스템을 이용하는 모든 금융회사는 자신들의 금융거래가 국제기구와 미국이 정한 제재(Sanction) 위반 여부를 반드시 점검하여야 한다.

헬로, 핀테크!(보안인증 · 블록체인)

HELLO, FINTECH!

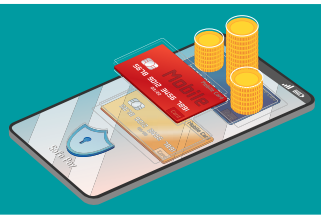
14장

레그테크 시장 및 산업 동향

제1절 레그테크 시장 현황

제2절 레그테크 산업 동향

14장 레그테크 시장 및 산업 동향



학습목표

1. 레그테크(RegTech)의 시장 현황을 설명할 수 있다.
2. 레그테크와 국제자금세탁방지기구(FATF)의 관계를 설명할 수 있다.
3. 레그테크와 관련된 금융산업과 법률 분야의 산업 동향을 설명할 수 있다.

학습개요

레그테크는 매우 다양한 산업에 적용되고 있다. 특히, 국제자금세탁방지기구는 급변하는 금융환경 대응과 가상자산 등이 자금세탁의 수단으로 사용될 위험에 대한 대응으로서 레그테크를 중요한 방법론으로 소개하고 있다. 아울러, 금융산업 분야에서 시도되고 있는 '위규 외국환거래 방지시스템'과 '인공지능 사모펀드 약관심사' 등에 대하여 알아본다. 또한, 리걸테크(LegalTech)로 불리는 법률 시장에서의 레그테크의 영향력, 관련 스타트업 현황 및 기술적 구조에 대하여 알아본다.

용어해설

❶ 트래블 룰(Travel Rule)

국제자금세탁방지기구의 권고 사항 제16번 전신송금(Wire Transfers)에 따르면, 각국은 금융기관이 전신송금 및 관련 메시지에 '요구된 그리고 정확한 송금인(Originator) 정보'와 '수취인(Beneficiary) 정보'를 포함하고 있어야 한다는 규칙(Rule)이다.

권고사항에는 트래블 룰(Travel Rule)을 준수하여야 한다고 명기하고 있으며 아울러 송금정보는 일련의 지급 · 결제 과정 내내 전신송금 혹은 관련 메시지와 함께 기록(Remain)되도록 하여야 한다. 이는 가상자산이 소위 '여행하는 과정'을 추적해야 한다는 의미로 트레블 룰이라 한다.

❷ 기계독해(MRC; Machine Reading Comprehension)

인공지능 기술 중의 하나로 컴퓨터가 인간처럼 문자를 읽고 분석하여 특정 질문에 대하여 해답을 제시하는 기술이다. 컴퓨터가 전산화된 문서 또는 전문의 내용을 읽고 자체 심사 또는 심사 보조업무를 수행한다.

❸ 리걸테크(LegalTech)

리걸테크(LegalTech)의 사전적 의미는 법을 의미하는 'Legal'과 기술의 'Technology'의 합성어이다. 레그테크의 하부 개념 또는 별도의 개념으로 분류하기도 하나 인공지능 등과 같은 혁신적 기술을 사용하는 방법론은 같다.

제1절

레그테크 시장 현황

1 레그테크 시장 현황

1-1 폭발적인 시장 성장률

레그테크 시장은 규제의 강화와 IT 기술의 혁신적인 발전으로 매년 폭발적인 시장 성장률을 보여 왔다. 글로벌 리서치 회사인 테크나비오에 따르면, 연평균 성장률(CAGR; Compound Annual Growth Rate)은 21%로 가속화되며, 2023년에 증가할 시장규모는 미화 약 60억불에 달하며, 2019년 연간 성장률은 18.45%로 추산된다고 발표하였다. 아울러, 레그테크 시장 점유율은 예닐곱 개의 회사들로 과점될 것이며, 성장률의 34%는 북미에서 이루어지며, 레그테크 시장의 핵심적인 동력 중 하나는 금융 범죄 식별 분야가 될 것이라고 말하고 있다.

〈그림 XIV-1〉 2019~2023 세계 레그테크 시장

출처: technavio

2 레그테크와 국제자금세탁방지기구

2-1 가상자산 사업자의 자금세탁 방지의무 부가의 의미

가. 국제자금세탁방지기구는 가상자산과 관련하여 각국의 자금세탁방지 관련 국제기준 이행을 촉구하였고, 이에 따라 2021년 3월 25일부터 가상자산 사업자에 대해 자금세탁행위 방지를 위한 의무를 부과하고, 금융회사가 가상자산 사업자와 금융거래를 수행할 때 준수해야 하는 사항을 규정하는 「특정 금융거래정보의 보고 및 이용 등에 관한 법률(약칭: 특정금융정보법) 개정안이 통과되었다. 가상자산 사업자에게는 금융정보분석원(KoFIU)에 대한 신고의무, 고객확인(KYC) 및 의심거래보고(STR)의 기본적 자금세탁방지 의무, 이용자별 거래내역 분리 등의 의무가 부가되었다.

가상자산 사업자(VASPs; Virtual Assets and Virtual Asset Service Providers)가 법제화되면 '가상자산 입출금계정 서비스'로 대표되는 '가상자산 관련 자금세탁방지 가이드라인'이 자동 종료될 것이다. 2019년 5월 7일 금융위원회는 '금융규제혁신 통합추진 회의'에서 가이드라인은 법제화 후 폐지 조건으로 행정지침에 포함하였다.

나. 가상통화 입출금계정 서비스의 문제점: 코인OO는 2019년 9월 주거래은행인 NOOO은행이 금융위원회의 '가상통화자금세탁방지 가이드라인'을 근거로 거래를 종료하겠다고 하자, 서울중앙지법에 입금정지조치금지 임시처분을 신청했다. 서울중앙지방법원 제50 민사부(재판장 구OO)는 29일 가상자산 거래소 코인OO를 운영하는 (주)웨이브OO링이 NOOO은행을 상대로 낸 입금정지조치금지 임시처분에 대해 인용을 결정했다. 현재 '실명확인 입출금계정 서비스'에서 사용되고 있는 가상계좌는 법률적으로 계좌가 아닌 단순한 자금관리시스템(CMS; Cash Management System) 코드(Code)이며, 가상계좌(Virtual Account)라는 용어 자체가 FATF에서 금지하고 있는 '대리 지급계좌(Payable Through Account)' 및 미국 FinCEN(Financial Crimes Enforcement Network)이 BSA(Bank Secrecy Act) 법으로 금지하고 있는 '중첩계좌(Nested Account)'로 오인될 수 있다. FATF의 권고안 개정은 VASP를 금융회사 등의 위치로 상향시켜 고객확인(KYC)의무를 부여한 만큼 앞으로 가상자산 사업자(VASP)의 고객확인의무 준수가 기대된다.

〈표 XIV-1〉 가상계좌 서비스의 문제점

문제점	내용
자금의 소유권 문제	법률적으로도 가상계좌로 입금된 자금은 이용자의 자금이 아닌 모계좌의 예금주인 거래소의 자금임
해외 사례 없음	가상계좌를 사용해 자금세탁방지업무를 수행하는 국가가 없음. 그 이유는 가상계좌 자체가 자금세탁방지업무에서 고위험으로 평가되는 서비스임
가상계좌 자체가 고위험	금융위원회 금융정보분석원의 '자금세탁방지 및 공중협박자금조달금지에 관한 업무규정' 제5절 '신상품 등 자금세탁방지 절차 수립에 따른 신규 금융상품 및 서비스 위험 검토' 시에 가상계좌를 사용하는 상품 및 서비스는 고위험으로 평가함
단기 실행 방안	2017.9.4. 금융위원회의 '가상통화 현황 및 대응 방향' 보도자료 별첨1을 보면 '단기 실행방안'에 따르면 "현재 가상통화 취급업자는 은행 등 기존 금융회사에 요구되는 수준의 이용자 본인확인 절차를 갖추고 있지 못한 상황으로 은행이 가상통화 취급업자의 이용자 정보를 확인하고, 이용자 본인 계좌에서만 입출금되도록 관리하는 방안을 추진한다"고 하였음
거래소의 법적 지위	FATF 권고안과 주석서에 따라 가상자산 사업자를 특금법 시행령 제2조(금융회사등)에 추가됨에 따라 은행을 통해 가상자산 사업자를 간접 규제 및 감독 방식은 이제는 그만두어야 함
원시적 불능 문제	현재의 가상통화 가이드라인 제5절 제2항 제1호의 '금융회사 등의 고객이 취급업소인 경우로서 실명확인 입출금계정 서비스를 이용하지 않는 등 자금세탁 등의 위험이 특별히 크다고 판단하는 경우 '지체 없이' 거절하거나 종료할 수 있다고 하였으나, 은행이 실명계좌를 주지도 않으면서 실명계좌를 이용하지 않는다고 거래를 거절하거나 종료하는 행위는 '원시적 불능' 행위임

2-2 가상자산 사업자의 자금세탁방지 시스템 구축 필요성

가. 2019년 7월 1일 자 「특정 금융거래정보의 보고 및 이용 등에 관한 법률 시행령」 개정 시행에 따라 「전자금융거래법」에 따른 '전자금융업자'와 자산규모 500억원 이상의 '대부업자'도 자금세탁방지 의무가 부과되었다. 이미 '가상자산 거래소'보다 회사 규모가 작은 '환전영업자'도 2016년 3월 22일부터 모든 환전영업자가, '소액해외송금업자'는 2017년 7월 18일에 이미 자금세탁방지 의무를 준수하고 있다.

나. 가상자산 사업자(VASPs; Virtual Assets and Virtual Asset Service Providers)는 영업의 형태와 파급력을 고려할 때 '환전영업자'보다는 회사의 규모와 사회적 책임이 커야 한다고 보며, 아울러 비슷한 영업 형태를 보여주고 있는 소액해외송금업자와 같은 사회적 책임과 임무를 수행해야 할 것이다.

다. 현재 시장에는 '암달러상' 및 '환치기상'이 어둠 속에 존재하고 양지에는 '환전영업자'와 '소액해외송금업자'가 존재한다. 이제 가상자산 거래소는 인가된 '가상자산 사업자'가 될 것인지 아니면 계속 어둠 속에 남아 있을 것인가를 선택해야 한다.

2-3 트래블 룰(Travel Rule) 구축 방안

FATF의 권고사항 16번 전신송금(Wire Transfers)에 따르면, 각국은 금융기관이 전신송금 및 관련 메시지에, '요구된 그리고 정확한 송금인(Originator) 정보'와 '요구된 수취인(Beneficiary) 정보'를 포함하는 트래블 룰(Travel Rule)을 준수하여야 한다. 그 정보는 일련의 지급 · 결제 과정 내내 전신송금 혹은 관련 메시지와 함께 기록(Remain)되도록 하여야 한다. 각국은 가상자산 사업자에게 요구된 송금인 그리고/혹은 수취인 정보가 관리될 수 있도록 적절한 조치를 취하여야 한다.[157)]

요약하면, FATF의 트래블 룰(Travel Rule)은 미화 1,000달러 이상의 송금거래를 실시할 때 가상자산 사업자(VASP)는 다음과 같은 정보를 관리해야 한다.

〈표 XIV-2〉 FATF: 트래블 룰(Travel Rule) 규칙에서 제공하여야 할 정보

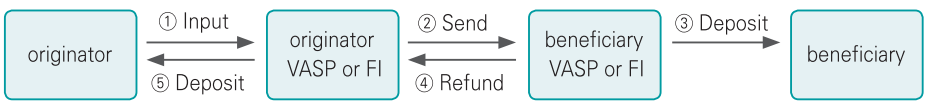
일련번호	제공 정보
1	송금인명
2	송금인 계좌번호(지갑 주소 등)
3	송금인 주소 · 국적 · 식별번호 · 생년월일 · 출생지
4	수취인 성명
5	수취인 계좌번호(지갑 주소 등)

157) 정지열 · 강형구 (2020), 가상자산 사업자(VASPs)의 가상자산 거래 시 송금 규정(Travel Rule) 준수를 위한 방법론 연구, 「법경제학연구」 제17권 제1호, pp. 331-352

하지만 이러한 정보 제공은 가상자산 사업자(VASP)의 기술적인 면을 포함해 개인의 금융 프라이버시와 자율성을 중시하는 가상자산의 기본 이념에까지 영향을 미칠 수도 있다. 기술적인 측면으로는 송금처의 주소가 가상자산 사업자(VASP)인지 프라이빗 지갑인지 판별하는 것의 어려움, 신뢰할 수 있는 고객 정보 이전의 방법 등이 지적되었다. 또 트래블 룰에 대응하는 인프라의 개발 운용에는 막대한 비용이 드는 것이 예상되기 때문에 자금력이 한정된 스타트업의 존속을 힘들게 할 수 있다는 우려의 목소리도 나오고 있다.

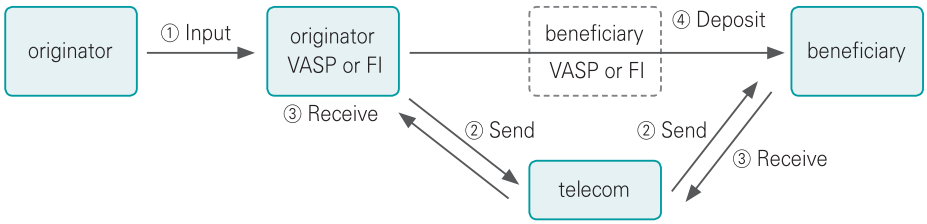
이에 대해 금융업계 전문가들은 레그테크(RegTech)를 활용하면 효과적인 송금 규정 준수가 가능하다고 말한다.

〈그림 XIV-2〉 일방향 전신송금 방식



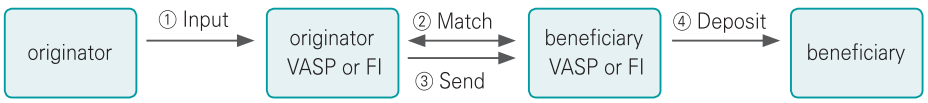
일방향 전신송금 방식은 〈그림 XIV-2〉처럼 가상자산의 전신송금을 원하는 송금인이 직접 수취인 지갑 주소와 수취인명 등 송금 정보를 투입하는 방식이다(①). 송금 가상자산 사업자(VASPs or Financial Institution)는 이용자가 해당 사업자의 정당한 이용자임을 확인하고 송금인 정보는 이용자 정보를 기반으로 하여 작성하고 수취인과 관련된 정보는 송금인으로부터 직접 입력받는 방식이다. 이때 송금 가상자산 사업자는 수취인의 전자지갑이 공인거래소의 전자지갑 주소인지를 확인하고 해당 수취인명은 요주의 인물 확인을 통해 요주의 인물 앞 송금 여부를 확인한 후, 중계은행 또는 공인된 지급 가상자산 사업자 앞 송금 요청을 하는 방식이다(②). 이때 수취 가상자산 사업자는 최종 수취인(Beneficiary)이 해당 사업자의 고객확인이 완료된 적법한 수취인일 경우에만 해당 전자지갑에 입금한다(③). 만약 정당한 수취인이 아니면 송금 가상자산 사업자에게 정정(Amend) 요청을 하거나 일정한 수수료를 차감한 가상자산을 송금 가상자산 사업자로 반송하는 퇴결 조치를 수행한다(④). 나머지 차액은 송금인 지갑에 입금된다(⑤).

〈그림 XIV-3〉 비인가 거래소와의 전신송금 방식



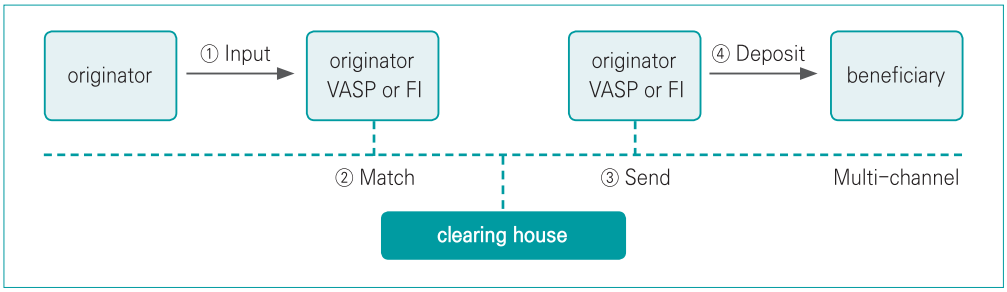
비인가 거래소와의 전신송금 방식은 〈그림 XIV-3〉처럼 먼저 송금인은 전신송금 정보와 수취인 핸드폰 번호를 입력한다(①). 인가된 가상자산 사업자는 해당 통신사에게 수취인의 성명을 요구한다(②). 수취인이 통신사에게 자신의 성명을 송신 가상자산 사업자에게 제공해도 된다는 정보제공 동의를 휴대폰으로 승인해 주면, 통신사는 송신 가상자산 사업자 앞으로 등록된 성명을 전달한다(③). 가상자산 사업자는 송금인이 투입한 수취인 성명과 통신사가 보내온 수취인 정보가 일치할 경우 해당 전신송금을 수행한다(④).

〈그림 14-4〉 인가된 거래소 간의 전신송금 방식



인가된 거래소 간의 전신송금 방식은 〈그림 XIV-4〉처럼 송금인이 입력한 전신송금 정보(①)를 상대 가상자산 사업자에게 예비거래 전문을 통해 송금 정보(양측 전자지갑 주소 포함) 및 관련인 들의 정상 여부를 서로 점검하는 방식(②)이다. 현재 전자금융 공동망 등에서 사용하는 방식으로 허가된 가상자산 사업자 사이에는 상호 점검을 완료한 후, 안전한 전신송금이 이루어진다(③).

〈그림 XIV-5〉 제3의 플랫폼 방식의 전신송금 방식



제3의 플랫폼 방식의 전신송금 방식은 〈그림 XIV-5〉처럼 송금인이 송금 정보를 입력(①)하면 가상자산 사업자는 해당 전문을 조립하여 현재의 금융결제원 같은 제3의 플랫폼을 주관하는 기관에 정상 여부를 확인한다(②). 이때 플랫폼을 주관하는 청산기관(Clearing House)은 해당 거래의 적정성을 확인한 후 거래를 승인할 것인가를 결정한 후 적정하면 해당 전신송금을 수취 가상자산 사업자로 전송한다(③). 이 플랫폼은 비공개(Private) 플랫폼으로 인가된 가상자산 사업자에게만 다중채널 방식으로 제공되기 때문에 블록체인 거래내역 보관영역에 다양한 프로그램 기능(Smart Contract)을 추가하면 「개인정보 보호법」이 요구하는 5년 이상 경과된 전신송금의 거래내역의 별도 보관 및 자동 삭제 기능 등을 프로그래밍할 수 있는 장점이 있다.

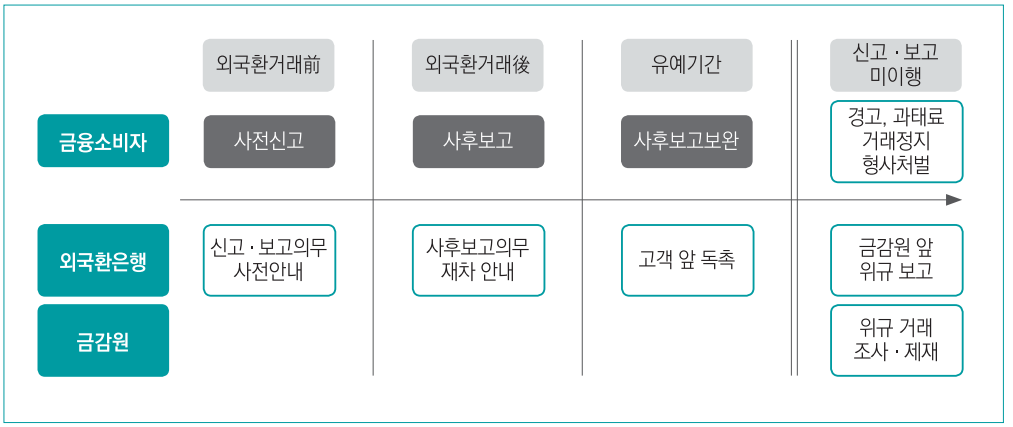
3 제재법규 심사시스템

3-1 위규 외국환거래 방지 및 레그테크

가. 목적

2019년 6월 금융감독원과 국내 12개 은행이 외국환거래 시 금융소비자의 반복되는 「외국환거래법」 위반을 방지하기 위하여 레그테크를 활용하여 「위규 외국환거래 방지시스템」을 만들었다. 이를 통해 금융소비자를 보호하고 외국환은행의 위규 방지 및 감독 당국의 업무역량을 강화할 수 있게 되었다.

〈그림 XIV-6〉 외국환거래 시 업무흐름도



출처: 금융감독원, 레그테크를 활용한 「위규 외국환거래 방지시스템」 구축 추진(2019.6.18), http://www.fss.or.kr

나. 기대효과

- **금융소비자**

  외국환 관련 거래 시 관련 법규에 따라 신고할 사항을 조기에 통지받아 과태료 처분 등을 받지 않게 된다.

- **금융회사**

  금융소비자에게 관련 법규를 정확하게 안내하여 회사는 제재 부담이 경감되고 업무 표준화에 따른 비용 절감효과도 있다.

- **금융당국**

  단순한 외국환 법규 위반에 사용되는 검사 자원을 금융회사 검사에 투입하여 감독 자원을 효과적으로 운영하게 된다.

3-2 인공지능 사모펀드 약관심사

가. 목적

2015년 10월 사모펀드 제도 개편에 따라 사모펀드의 설립과 설정 관련 보고 건수가 폭증하여 섭테크(SupTech)의 일환으로 업무혁신과 효율화 필요성이 대두되었다. 인공지능이 자동으로 약관심사를 수행하여 심사업무의 신속성과 효율성 제고하게 되었다.

나. 구축내용

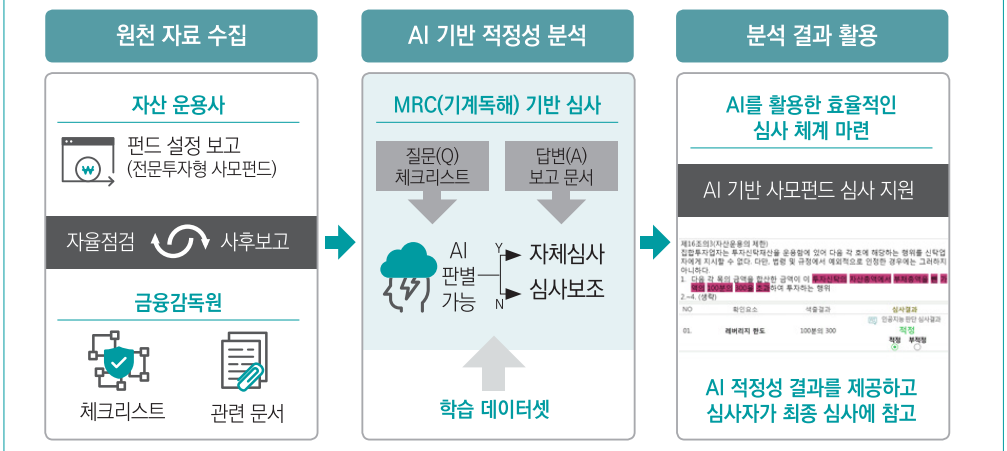
- 기계독해(MRC; Machine Reading Comprehension)기술 사용

  인공지능기술 중의 하나로 컴퓨터가 인간처럼 문자를 읽고 분석하여 특정 질문에 대하여 해답을 제시하는 기술이다. 컴퓨터가 약관의 내용을 읽고 자체 심사 또는 심사 보조 업무를 수행한다.

- 지도학습(Supervised Learning) 방식 사용

  인공지능 기술 중 기계학습(Machine Learning) 방법 중 한 가지 방법으로 사전에 프로그램된 입력(Input)과 출력(Output) 방식의 훈련 자료(Training Data)를 반복적으로 학습하여 업무에 활용한다.

〈그림 XIV-7〉 인공지능 약관심사 지원 시스템



출처: 금융감독원, 금융감독원의 레그테크 · 섭테크 혁신 – ② AI(인공지능)가 사모펀드 약관 심사를 지원한다(2019.6.18), http://www.fss.or.kr

제2절

레그테크 산업 동향

1 금융 산업과 레그테크

1-1 금융과 레그테크 생태계

가. 규제 당국(Regulators): 규제 당국은 규제를 만드는 주체이자 규제의 준수 여부를 검사하는 구성원이다. 레그테크의 필요성이 매우 크다.

나. 스타트업(Startups): 규제 환경에 새로운 해법을 제시하는 주체다.

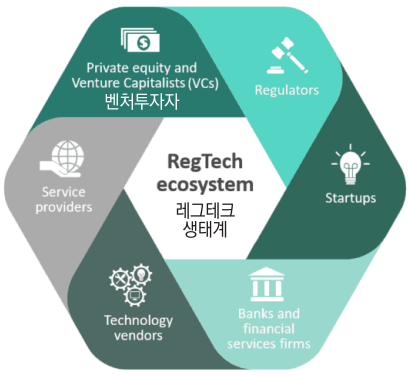
다. 금융회사 등(Banks and financial services firms): 레그테크의 주요 소비자이며 레그테크 생태계에의 주요 자금 공급원이다.

라. IT업체(Technology vendors): 기술 및 클라우드 서비스의 공급자이다.

마. 서비스제공업자(Service providers): 레그테크 패키지를 포함한 전산 서비스 제공뿐만 아니라 법률 및 요주의인물 정보제공도 포함한다.

바. 벤처투자자(Private equity and Venture Capitalists): 투자를 담당한다.

〈그림 XIV-8〉 금융과 레그테크 생태계



출처: Everest Group

1-2 2020년 코리아 핀테크 위크 - 레그테크 참여 금융회사

금융위원회는 2020년 5월 28일부터 제2회 코리아 핀테크 위크 2020을 개최하였다. 이 박람회에는 핀테크를 포함한 레그테크와 관련된 많은 행사가 있었는데 그중에 레그테크 쇼케이스에 대하여 알아보자.

먼저, 금융감독원과 코스콤에서 섭테크(SupTech)의 일환으로 머신 리더블 레귤레이션(MRR) 시범사업을 선보이고, 금융보안원에서는 금융보안과 관련된 레그테크 포탈을 공개하며, 에임스는 인슈어테크(InsurTech)의 사례로 보험금 착오 지급 방지 서비스를, 옥타솔루션은 전자금융업자 등을 위한 자금세탁방지(AML) 시스템을 선보였다. 은행권에서는 신한은행이 글로벌 정보보호 분야와 관련하여 '글로벌 정보보호 레그테크 시스템'을 소개하며, 우리은행의 무역기반 자금세탁(TBML; Trade-Based Money Laundering) 방지를 위한 인공지능 기반의 수출입 선적서류 심사업무를 선보였다. 최근 북한의 불법 환적(Transshipment) 문제가 국제적 문제로 대두되는 시점에 우리은행의 인공지능을 활용한 수출입 서류 심사업무 도입은 매우 시기적절하다.

〈그림 XIV-9〉 코리아 핀테크 위크 2020 참여 회사

레그테크 쇼케이스 참여기관 구성(안)

기관명	분야	주요내용
금융감독원 · 코스콤	MRR	전자금융거래법 관련 MRR 시범사업 결과
금융보안원	금융보안 레그테크 포탈	정보보호 수준 자율진단, 금융보안 보고서 자동 생성 등
에임스	보험금 착오지급 방지	보험약관의 자동 알고리즘화 및 보험금 착오지급 검출
옥타솔루션	자금세탁방지	전자금융업자 등 업종 맞춤형 자금세탁방지 솔루션 제공
신한은행	글로벌 정보보호	뉴욕주 사이버보안법 등 글로벌 정보보호 법규 준수 여부 점검
우리은행	수출입 선적서류 심사	서류분류 → 텍스트 추출→ 데이터 축적→ 심사 등 일련의 과정을 자동화

출처: 금융감독원, 금융 규제준수 자동화 기술 및 사례를 한눈에 만나보세요(2020.5.26), http://www.fss.or.kr

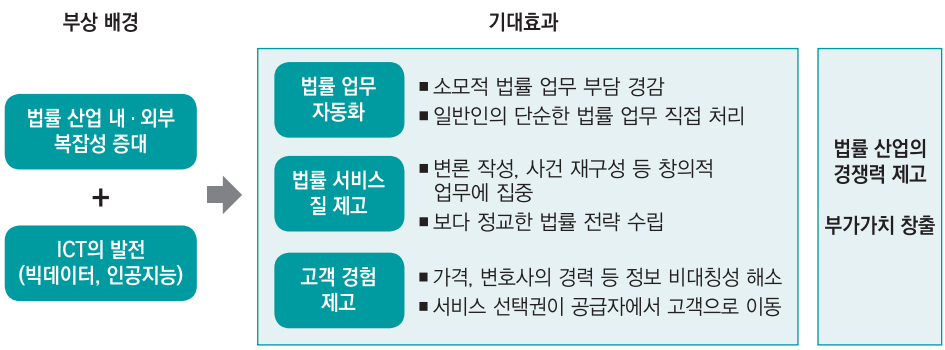
2 법률 분야와 레그테크

2-1 리걸테크(LegalTech) 등장

가. 리걸테크의 정의

리걸테크(LegalTech)의 사전적 의미는 법을 의미하는 'Legal'과 기술의 'Technology'의 합성어이다. 레그테크의 하부 개념 또는 별도의 개념으로 분류하기도 하나 인공지능 등과 같은 혁신적 기술을 사용하는 방법론은 같다.

〈그림 XIV-10〉 리걸테크의 부상과 기대효과



출처: 현대경제연구원, 리걸테크(Legaltech) 산업 현황과 시사점(2016.10.12), http://hri.co.kr

나. 국내 리걸테크 스타트업

〈그림 XIV-11〉 국내 리걸테크 스타트업과 서비스

서비스명	개발사	특징
모두싸인	로아팩토리	온라인 계약서 체결 서비스
헬프미	헬프미 법률사무소	변호사 찾기, 지급명령, 등기, 상속 온라인 법률 서비스
로톡	로앤컴퍼니	변호사 · 사례 검색 및 온라인 법률 상담 플랫폼
아이리스	인텔리콘 메타연구소	지능형 법률 정보 시스템 (자연이로 법률, 판례 등 자료 검색 기능)

출처: 모두싸인 외 각사

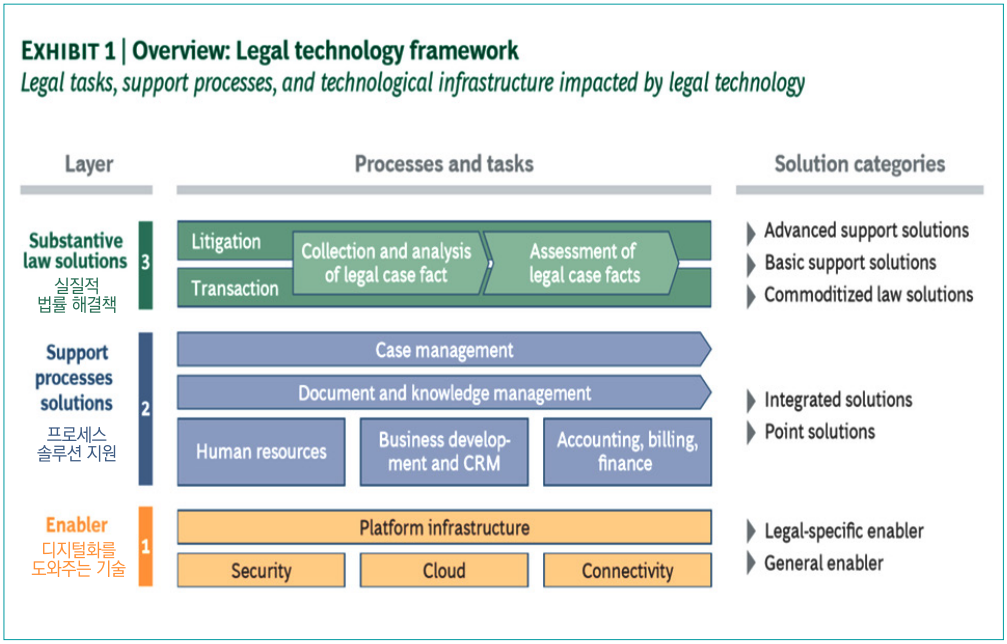
다. 리걸테크의 구조(3 Layers)

1) 1단계(Layer 1) – 디지털화를 도와주는 기술(Enabler): 법률 상담과 관련된 포탈이나 플랫폼을 구축하여 간단한 법률 서비스를 제공하는 단계이다.

2) 2단계(Layer 2) – 기술지원과 판례관리 시스템(Support processes solutions): 판례 분석, 자문과 송무 관련 문서와 노하우 관리, 내부 자원관리, 비용 청구 및 재무관리를 제공하는 단계이다.

3) 3단계(Layer 3) – 실제 송무 업무 수행 기술(Substantive law solutions): 소송 판례를 취합하여 분석 및 평가한 후, 실질적인 법률 해결책을 제시하는 단계이다. 단순 반복적인 계약서 검토뿐만 아니라 실제 소송에서 인간 변호사에게 조언이 가능한 단계이다.

〈그림 XIV-12〉 리걸테크 구조



출처: BCG analysis

핵심정리

1. 레그테크 시장 현황

- **레그테크 시장의 높은 성장률**

  레그테크 시장은 규제의 강화와 IT 기술의 혁신적인 발전으로 매년 폭발적인 시장 성장률을 보였다. 글로벌 리서치 회사인 테크나비오에 따르면 연평균 성장률(CAGR; Compound Annual Growth Rate)은 21%로 가속화되며, 2023년에 증가할 시장규모는 미화 약 60억불에 달하며, 2019년 연간 성장률은 18.45%로 추산된다고 발표하였다.

- **실명확인 입출금계정 서비스**

  현재 '실명확인 입출금계정 서비스'에서 사용되고 있는 가상계좌는 법률적으로 계좌가 아닌 단순한 자금관리시스템(CMS; Cash Management System) 코드(Code)이며, 가상계좌(Virtual Account)라는 용어 자체가 FATF에서 금지하고 있는 '대리지급계좌(Payable Through Account)' 및 미국 FinCEN(Financial Crimes Enforcement Network)이 BSA(Bank Secrecy Act) 법으로 금지하고 있는 '중첩계좌(Nested Account)'로 오인될 수 있다. FATF의 권고안 개정은 VASP를 금융회사 등의 위치로 상향시켜 고객확인(KYC) 의무를 부여한 만큼, 금융회사와 가상자산사업자(VASP) 모두를 힘들게 하는 실명확인 입출금계정 서비스의 사용을 강제화할 필요는 없다.

2. 레그테크 산업 동향

- 금융 분야의 레그테크 생태계 6요소

첫째, 규제 당국(Regulators)으로 규제 당국은 규제를 만드는 주체이자 규제의 준수 여부를 검사하는 구성원이다.

둘째, 스타트업(Startups)으로 규제 환경에 새로운 해법을 제시하는 주체다.

셋째, 금융회사 등(Banks and Financial Services Firms)으로 레그테크의 주요 소비자이며 레그테크 생태계의 주요 자금 공급원이다.

넷째, IT업체(Technology Vendors)로 기술 및 클라우드 서비스의 공급자이다.

다섯째, 서비스제공업자(Service Providers)로 레그테크 패키지를 포함한 전산 서비스 제공뿐만 아니라 법률 및 요주의인물 정보제공도 포함한다.

마지막으로 벤처투자자(Private Equity and Venture Capitalists)를 들 수 있다.

- 리걸테크의 구조(3 Layers)

리걸테크의 3 레이어는 1단계(Layer 1)는 법률 서비스의 디지털화를 도와주는 기술(Enabler)로 포탈이나 플랫폼을 구축하는 단계를 말한다. 2단계(Layer 2)는 기술지원과 판례관리 시스템(Support Processes Solutions)으로 판례 분석, 자문과 송무 관련 문서와 노하우 관리 등을 제공하는 단계이다. 3단계(Layer 3)는 실제 송무 업무 수행 기술(Substantive Law Solutions)로 소송 판례를 취합하여 분석 및 평가한 후, 실질적인 법률 해결책을 제시하는 단계이다.

MEMO

헬로, 핀테크!(보안인증 · 블록체인) HELLO, FINTECH!

참고문헌

웹사이트

- 국립국어원 www.korean.go.kr
- 국세청홈택스 www.hometax.go.kr
- 금융소비자 정보포털 파인 https://fine.fss.or.kr/main/
- 금융감독원 www.fss.or.kr
- 금융결제원 www.kftc.or.kr
- 금융보안원 www.fsec.or.kr
- 금융위원회 www.fsc.go.kr
- 건축공간연구원 www.auri.re.kr
- 경찰청 www.police.go.kr
- 네이버 www.naver.com
- 롯데케미칼 www.lottechem.com
- 문화체육관광부 www.mcst.go.kr
- 법제처, 국가법령정보센터 law.go.kr
- 뱅크사인 www.banksign.or.kr
- 서대문구청 공식 블로그 https://blog.naver.com/sdmstory
- 시비인사이트 www.cbinsights.com
- 아이콘루프 www.iconloop.com
- 위키피디아 www.wikipedia.org
- 전략물자관리원 www.kosti.or.kr
- 카카오페이 www.kakaocorp.com
- 컴퓨터월드 www.comworld.co.kr
- 한국금융연수원 www.kbi.or.kr
- 한국인터넷진흥원 www.kisa.or.kr
- 한국지능정보사회진흥원 www.nia.or.kr
- 한국정보통신기술협회 정보통신용어사전 https://terms.tta.or.kr/main.do

- BISINESSINSIDER www.businessinsider.com
- Bloomberg www.bloomberg.com
- CoinMarketCap www.coinmarketcap.com
- Cointelegraph Facebook www.facebook.com/cointelegraph
- Everest Group www.everestgrp.com
- FCA www.fca.org.uk
- FINTRAC www.fintrac-canafe.gc.ca
- Investopedia www.investopedia.com
- KISA(전자서명인증관리센터) www.rootca.or.kr
- Newsweek www.newsweek.com
- NSHC www.nshc.net
- PASS www.passauth.co.kr
- Technavio www.technavio.com
- Thomson Reuters www.thomsonreuters.com
- U.S. Department of the Treasury home.treasury.gov
- Wevorce www.wevorce.com

도서 및 문헌

- 금융감독원(2006), 은행 준법감시인 제도운영 모범규준
- 금융감독원(2009), 전자금융 감독규정 해설
- 금융감독원(2017), 전자금융 감독규정 해설
- 금융감독원(2018), 보험회사 인슈어테크(InsurTech) 활용현황
- 금융감독원(2019), 레그테크를 활용한 「위규 외국환거래 방지시스템」 구축 추진
- 금융보안원(2017), 「금융보안 분야 레그테크 도입 방향, 금감원 레그테크 포럼」
- 금융위원회(2016), 비대면 실명확인 운영 현황 및 향후 계획
- 금융위원회(2019), 제1회 「코리아 핀테크 위크 2019」 개최 결과
- 금융위원회(2019), 정맥인증 서비스로 은행거래가 편리
- 금융위원회(2021), 보험업법 시행령 및 감독규정 등 입법예고
- 금융위원회 및 한국신용정보원 (2021.2.), 금융분야 마이데이터 서비스 가이드라인

- 금융위원회 및 금융보안원 (2021.2.), 금융분야 마이데이터 기술 가이드라인
- 방송통신위원회 보도자료, 2020년 제51차 위원회 결과(2020.9.23.)
- 한국은행(2016), 바이오인증기술 최신 동향 및 정책과제
- 현대경제연구원(2016), 리걸테크(Legaltech) 산업 현황과 시사점

- 김신영(2015), 전자금융거래의 사용자 인증 방법 평가 및 선택 가이드, 금융보안원 전자금융과 금융보안 제2호, 62-65
- 김영한(2018), 핀테크와 행동재무 - 「기업재무 6」
- 김현식(2019), 지능정보통신 VOL.20. 한국정보통신학회
- 고철수, 김춘규(2017), 업무에 활용하는 자금세탁방지 가이드, 한국금융연수원
- 박만성(2017), RegTech 전망과 도입 필요성, 금감원 레그테크 포럼
- 이효익, 김한수, 이종은(2018), New ISA 회계감사, 신영사
- 윤지영(2019), 형사정책연구원, 제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(II) - IoT와 블록체인
- 이병욱(2018), 비트코인과 블록체인, 탐욕이 삼켜버린 기술, 에이콘 출판사
- 이병욱(2019), 블록체인 해설서, 에이콘 출판사
- 정병석(2007), 사법제도 개혁추진위원회 자료집, 기업의 준법관리제도 도입방안
- 장병화 · 박이락(2015), 「전자금융총람」. 한국은행 금융결제
- 조상래 외(2014), "패스워드 없는 인증기술-FIDO", 전자통신동향분석, 29권 4호
- 조창훈(2017), 「국내 레그테크의 시장성 검토 및 도입 시 고려사항」. 전자금융과 금융보안, 제8호
- 조휘갑 (2002), 전자서명 이용방법 안내, 한국정보보호진흥원
- 조현준(2018), 2018 정보보안기사 & 산업기사, 탑스팟

- Janos Barberis 외 2명(2019), The REGTECH Book. John Wiley & Sons Ltd.

MEMO

교재 집필 위원

고광선 | 제1~5장

- 성균관대학교 정보공학 학사
- 성균관대학교 전기전자및컴퓨터공학 석사
- 성균관대학교 컴퓨터공학 박사
- (전) 케이엘넷 IT본부 대리
- (전) 성균관대학교 대학원 이동통신공학과 연구교수
- (전) 금융보안연구원(현 금융보안원) 기획총괄팀 팀장
- (현) 성균관대 소프트웨어대학 정보통신대학원 겸임교수
- (현) 김·장 법률사무소 금융IT&핀테크그룹 전문위원

이병욱 | 제6~9장

- 한국과학기술원(KAIST) 전산학과
- (전) BNP 파리바 카디프 전무
- (전) 삼성생명 주식회사 마케팅 개발 수석
- (전) 주식회사 보험넷 Founder & CEO
- (현) 인공지능연구원(AIRI) 부사장
- (현) 서울과학종합대학원 디지털금융 주임교수
- (현) 한국금융연수원 겸임교수
- **저서** 2019, 블록체인 해설서(에이콘 출판사) – 2019 대한민국학술원 선정 교육부 우수학술도서
  2018, 비트코인과 블록체인, 탐욕이 삼켜버린 기술(에이콘 출판사)

정지열 | 제10~14장

- 한양대학교 경영학 박사(Finance 전공) 재학
- (전) 금융감독원 레그테크 포럼 자문위원
- (현) 하나은행 자금세탁방지섹션 유닛리더
- (현) 한국자금세탁방지 전문가협회 협회장
- (현) 한국투명성기구 정책위원
- (현) 성균관대-새금융사회연구소 금융지도자(AML) 과정 교수
- (현) 경찰수사연수원 외래교수
- (현) 한국금융연수원 강사
- **저서** 1993, 프로그래밍으로 배우는 베이식의 세계 (하이테크정보사)
  2020, 가상자산 사업자의 가상자산 거래 시 송금 규정 준수를 위한 방법론 연구(법경제학연구)

감수자

김흥재

- 단국대학교 이학사(컴퓨터전공)
- 아주대학교 경영대학원 경영학석사
- (전) 코스콤 미래사업TF 혁신기술팀장
- (전) 코스콤 자본시장기술연구소 선임연구원
- (전) 금융감독원 레그테크포럼 위원
- (현) 코스콤 데이터테크본부 데이터오피스사업부 팀장

헬로, 핀테크!

보안인증·블록체인

초판 발행 2020년 10월 14일
개정 1판 2021년 11월 29일
집필 위원 고광선, 이병욱, 정지열
감 수 자 김흥재
발 행 인 변영한
발 행 처 사단법인 한국핀테크지원센터
(04213) 서울시 마포구 마포대로 122, 11층, 12층
전 화 02) 6375-1550
홈페이지 www.fintech.or.kr
등 록 2020년 7월 24일(제879-82-00208호)
ISBN 979-11-92068-07-7 05320
979-11-92068-02-2 05320(세트)

「헬로, 핀테크」도서의
보조학습자료로서 동영상 강의를
FinEDU에서 제공하고 있습니다.

finedu.fintech.or.kr

「헬로, 핀테크」시리즈 외에도
한국핀테크지원센터에서
엄선하여 기획한 핀테크 전문 커리큘럼
FinEDU 코스를 경험하세요!

HELLO, FINTECH

헬로, 핀테크! 7종 시리즈

헬로, 핀테크!
입문
핀테크 개요, 기술, 시장, 핀테크 관련 법률,
금융회사와 핀테크 기업의 협업 등
한국핀테크지원센터 지음

헬로, 핀테크!
지급결제·송금
핀테크 지급결제·송금 기술, 규제 및 정책 동향,
시장 및 산업 동향 등
한국핀테크지원센터 지음

헬로, 핀테크!
금융플랫폼·금융데이터
금융정보플랫폼, 오픈뱅킹플랫폼, P2P플랫폼,
금융빅데이터 기술 및 활용사례, 마이데이터 산업 등
한국핀테크지원센터 지음

헬로, 핀테크!
자산관리·보험
자산관리테크 및 인슈어테크 서비스,
기반 기술, 규제 및 정책 등
한국핀테크지원센터 지음

헬로, 핀테크!
보안인증·블록체인
보안인증 핵심기술 및 사례, 블록체인 기술,
정책 및 산업 동향, 레그테크 기술 및 사례 등
한국핀테크지원센터 지음

헬로, 핀테크!
개인신용정보 관리 및 활용
개인신용정보 관련 법규, 개인신용정보 수집 및 관리
실무, 개인신용정보 기술현황, 시장 및 산업 동향 등
한국핀테크지원센터 지음

헬로, 핀테크!
핀테크 기반기술
빅데이터와 인공지능 기술, 클라우드 서비스 등
한국핀테크지원센터 지음

HELLO, FINTECH

금융위원회
한국핀테크지원센터
Fintech Center Korea
한국금융연수원
KOREA BANKING INSTITUTE