ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 5, pp. 85-93, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.5.085

우리나라의 본인확인수단에 관한 신규 인증수단의 도입 적합성 검토 : Block Chain과 FIDO를 중심으로

신영진
배재대학교 산학협력단 교수

Review of the suitability to introduce new identity verification means in South Korea : Focused on Block Chain and FIDO

Young-Jin Shin
Professor, Industry-Academic Cooperation Foundation, Paichai University

요 약 본 연구는 우리나라에서 운영되고 있는 본인확인수단의 다양성을 확보하기 위해 비대면 본인인증수단 중에서 블록체인과 FIDO를 선택하여 본인확인수단으로서의 적합성 정도를 검토하였다. 이를 위해 7가지 적합성 기준(보편성, 지속성, 유일성, 편의성, 보안성, 적용성, 경제성)을 선정하여 분석하였는데, 모두 적합한 수준을 갖추고 있음을 검증하였다. 이에 따라 블록체인과 FIDO를 본인확인수단으로 적용하기 위해서는 관련 규정 및 고시의 개정으로 본인확인절차를 개선하여야 한다. 더욱이, 기존의 본인확인수단뿐만 아니라 다양한 본인인증수단을 적용할 수 있도록 서비스분야별로 차별화된 인증기준이 마련되어야 하고, 지속적으로 인증수단을 개발하여 서비스와 연계하여야 한다. 앞으로 본인확인수단은 사물인터넷시대에서 정보유통환경의 안전성을 가져올 것이므로, 본인확인수단의 적용 확대 및 자율적 도입을 지원하여 다양한 서비스에서 구현될 수 있어야 한다.

주제어 : 본인확인수단, 본인인증수단, 블록체인, FIDO, 적합성기준

Abstract This study investigates the suitability of the blockchain and FIDO among non-face-to-face authentication means in order to secure diversity of identfication means operated in South Korea. In order to do this, the study selected and analyzed seven conformance criteria (universality, persistence, uniqueness, convenience, security, applicability, and economics), and the results were appropriate. Accordingly, in order to apply the blockchain and FIDO as the identification means, the related regulations and notices should be revised to improve the identification procedure. In addition, differentiated certification standards should be established for each service field to apply various authentication means as well as existing identification means, and the authentication means should be continuously developed and linked with the service. In the future, the identification means will bring security of the information circulation environment in the IoT, so it should be implemented in a variety of services by supporting application of identification means.

Key Words : Identfication means, Authentication means, Blockchain, FIDO, Conformance criteria

*This work was supported by the research grant of Pai Chai University in 2017.
*Corresponding Author : Young-Jin, Shin(jinsyj@yahoo.com)
Received August 27, 2018 Revised September 20, 2018
Accepted October 20, 2018 Published October 31, 2018

1. 서론

우리나라는 국가정보화사업 및 전자정부사업을 진행하는 과정에서, 단일한 본인식별체계인 주민등록번호를 이용하여 대국민 서비스를 제공하게 되었다. 즉, 주민등록번호는 정부 및 기업의 모든 시스템에서 개인을 식별하는 고유키값으로써, 프로그래밍에 용이한 코드값으로 활용되었다. 그러나 인터넷서비스가 확대되면서, 개인정보의 오·남용, 악용 등 개인정보 침해사고가 급증하게 되었는데, 그 중 주민등록번호를 포함한 개인정보를 대상으로 한 침해사고가 50%이상을 차지하고 있었다.

이에 따라 2000년초부터 도입된 공인인증서를 비롯하여 아이핀(Internet Personal Identification Number: I-PIN), 휴대전화 등을 주민등록번호 대체수단으로서의 본인확인수단으로 적용하였다. 또한, 2014년 「정보통신망 이용촉진 및 정보보호에 관한 법률」(이하 「정보통신망법」),「개인정보 보호법」을 개정하여 법률 및 시행령에 근거하지 않고는 주민등록번호를 원칙적으로 처리하지 못하게 하였고, 주민번호대체수단의 사용규정을 강화하였다. 물론, 최근에는 신용카드를 본인확인수단으로 적용하였는데, 이는 본인확인수단에 관한 지정 및 운영에 대한 변화를 반영한 것이다. 더욱이, 비대면 금융서비스의 도입에 따라 비대면 본인확인수단의 적용가능성도 논의되고 있다.

따라서, 본 연구에서는 정보화환경의 변화에 따라 정부가 지정한 본인확인수단을 주민번호대체수단으로만 지정하기보다는 일정기준에 적합한 경우 다양한 인증수단을 활용하도록 제언하고자 한다. 특히, 기존의 본인확인수단이 소유기반과 지식기반으로 운영되고 있는데, 특징기반의 인증수단을 선정하여 본인확인수단으로서 적합성을 검토하고자 한다. 이를 위해 행태정보인증수단 중에서 Block Chain(이하 블록체인)과 생체정보인증수단 중에서 Fast IDentity Online(이하 FIDO)를 선정하여, 기존 연구에서 도출된 본인확인수단의 적합성 기준을 적용하여 검토하고, 그 결과에 따른 적용방안을 제시하고자 한다.

2. 관련 연구

2.1. 블록체인과 FIDO

2.2.1 블록체인 인증

블록체인은 거래에 참여하는 모든 사용자의 거래내역을 활용하는데, 거래마다 거래내역을 대조하여 데이터의 위조를 방지하는 기술이다[1]. 즉, 모든 거래기록을 시간적 순서대로 네트워크상의 공동 거래장부로서, 일정시간 동안 발생한 거래가 하나의 블록에 일괄 저장되고, 거래정보가 기록된 원장(Ledger)은 네트워크에 존재하는 모든 참여자가 공동으로 보관한다[2]. 블록체인기술의 특징은 탈중개성(분산성), 보안성, 투명성, 신속성, 확장성, 효율성 등이다. 블록체인이 암호기술과 융합된다면, 비밀성, 인증, 무결성, 부인봉쇄, 개인정보보호 등에 적합한 강력한 인증수단이 될 것이다[3]. 블록체인은 4개의 논리적 요소로 구성되며, 215byte~1Mbyte의 크기이며, 블록의 헤더는 6개 정보로 구성되어 모든 정보와 거래의 요약정보를 담고 있다[4]. Fig.1과 같이 블록체인의 인증방식은 기기등록 시 생성된 키를 이용하여 블록체인에 연결된 구성원에게 인증을 요청하여, 공동으로 기록보관하고 있는 인증값과 전달받은 인증값이 일치하면 사용자의 인증을 승인하여 진행된다.

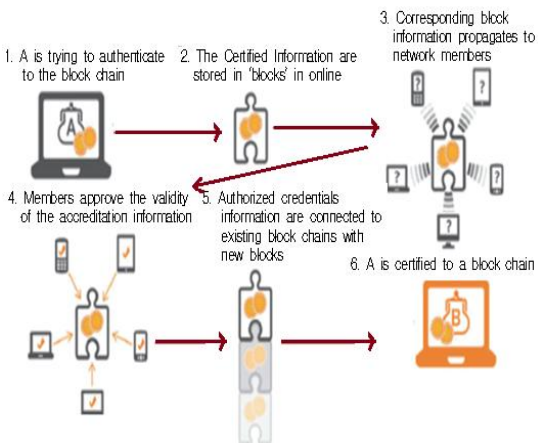

Fig. 1. Authentication process based on block chain

source: By the author, referring to S. H. Hong & S. H. Park. (2017). The Research on Blockchain-based Secure IoT Authentication. *Journal of the Korea Convergence Society*. 8(11): 61.

블록체인은 거래내용의 변경사항을 암호화된 인증방식을 통해 새로운 체인처럼 블록으로 연결하며, 참여자가 제3자의 개입없이 직접 거래기록을 분산된 환경에 기재하여 자유롭게 열람하는 탈중앙화된 금융서비스제공의 핵심기술로 활용되고 있다[5]. 이에 따라 블록체인은 온라인상 가상화폐인 비트코인의 유통안정성을 위해 도입되었으며, 거래내역인증을 통한 다양한 인증기반 서비스로 확대될 전망이다. 특히, 본인인증을 위해 별도의 관

리기관(Certificate Authorities: CA)없이도 분산화되어 있는 안전한 인증체계로 활용되고 있다. 따라서, 한국형 인증서 발급시스템의 한계를 블록체인으로 해결할 수 있다[6].

블록체인의 적용분야는 글로벌 금융회사, IT기업 등에서 관련 사업으로 확대되고 있다. 또한, 암호화폐, 국제송금, 무역금융, 손해보험, 주권위임투표, 물류산업, P2P 전력거래, 온라인 광고거래, 개인인증 등 다양한 분야에서도 사용될 수 있다[7]. 특히, 블록체인은 금융기관의 해외송금·증권거래·규제대응 등과 관련하여 2020년까지 연간 150~200억달러 인프라비용을 절감할 것으로 전망된다[8]. 이렇다보니, 전세계적으로 블록체인을 연계한 컨소시엄을 결성하여 지속적인 연구가 이루어지고 있다. 이미 미국, 유럽, 아시아를 중심으로 R&D가 확대되고 있으며, 핀테크와 협업한 금융서비스에서도 적용할 계획이다. 우리나라도 2016년 1월 한국은행의 '중장기 지급결제 업무 추진전략(지급결제 vision 2020)'을 발표하여 금융기관과의 R&D를 진행하고 있으며, LG CNS도 2015년 클라우드월렛, 바이터그룹과 MOU를 통해 전자증권 발행을 한 바 있다[9].

2.2.2 FIDO

FIDO는 지문, 홍채, 얼굴, 목소리, 정맥 등 생체정보를 사용한 인증시스템으로서, 해킹방지, 프라이버시보호 등과 같은 안정성을 확보하기 위해 도입되고 있으며, 인증프로토콜과 인증수단을 분리하고 있어 보안성과 편리성이 높다[1]. 또한, 생체인증을 활용하기 때문에 지식기반이나 소유기반의 인증수단보다 편의성을 향상시킬 수 있다.

FIDO표준기반의 원격인증을 수행하기 위해 공개키 암호가 사용되며, 개인키를 이용한 암호화문을 서버에 전송하여 저장된 공개키를 이용하여 검증하여 인증하고 있다[10]. FIDO의 인증방식은 UAF(Universal Authentication Framework)와 U2F(Universal 2nd Factor)로 운영되고 있다. U2F기술은 기존 아이디와 비밀번호 인증기반에서 2차 추가인증을 받을 때 사용자 로그인 시 추가 사용되는 프로토콜이며, 구글의 USB 보안키를 활용방식에서 제공하고 있다. UAF기술은 안드로이드 스마트폰에 탑재된 생체인증장치를 온라인 서비스와 연동하여 사용자를 인증하는 기술이며, 삼성페이의 지문인증결제서비스에서 제공되고 있다[1]. 특히, Fig.2와 같이 UAF프로토콜을 이용한 인증방식은 사용자 디바이스에 미리 설치된 인증키를 활용하여 사용자 서명 및 인증모듈의 사용을 검증하는 방식으로 운영된다.

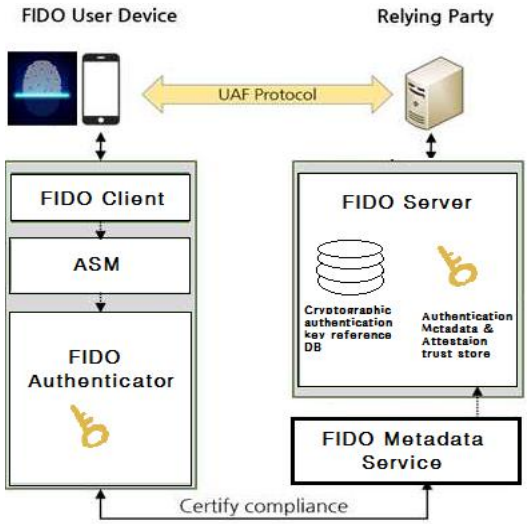

Fig. 2. Biometric Authentication method using UAF protocol in FIDO system

source: By the author, referring to Y. K. Kim, C. J. Chae & H. J. Cho. (2018). User Authentication Method using EEG Signal in FIDO System. *Journal of the Korea Convergence Society*. 9(1): 466.

FIDO는 구글·MS·페이팔 등 200여개 글로벌기업을 비롯하여 미국, 영국 등 정부가 참여한 FIDO Alliance에서 국제표준화 및 보급 활성화를 추진하고 있다. 우리나라에서도 금융사, 통신사, 인증서비스업체 등에서 도입되고 있으며, FIDO기반의 간편결재서비스, 카드사의 인증서비스 등에 도입할 것으로 전망된다[11]. 더욱이, IoT기기인증을 위해 FIDO를 적용될 경우 기업, 정보, 의료, 금융 등 다양한 분야에서 적용이 가능하다[12].

2.2 기존 연구 동향

블루체인을 인증수단으로 적용하기 위해 그동안 이루어진 연구들을 살펴보면, 박병주·이태진·곽진(2017. 4)은 IoT사물인터넷환경이 구현됨에 있어서 블록체인에 관한 램포트 해쉬체인, 램포트 서명, 블록체인을 분석하여 기존 인증프로토콜을 분석하고 인증, 무결성 및 부인방지 등을 위해 블록체인기반의 IoT기기인증 스킴을 제안하였다[13]. 오서영·이창훈(2017. 2)은 비트코인에서의 이중지불문제를 해결하기 위해 작업증명(Proof of work) 또는 소유증명(Proof of stake)기법으로 적용할 수 있다고 보았다(Marko, V. 2015)[14,15],

FIDO를 인증수단으로 검토한 연구들을 살펴보면, 김수형(2016. 1)은 핀테크보안기술로서 UAF기술을 중심으로 강력한 인증서비스를 제공함에 있어서 FIDO2.0기술의 웹브라우저 적용에 필요한 절차, 지침, 기준 등을 마련하고자 하였다[16]. 김재성·이성재·김병섭·이상우(2015. 8)는 스마트폰·테블릿PC 등 스마트기기에 생체정보탑재 기술이 접목되어 FIDO, ITU-T SG17Q9(텔레바이오인식) 국제표준화기구를 중심으로 표준화가 진행되었기 때문에, 스마트기기를 통한 비대면 인증기술수단으로서 뇌파·심전도 등 생체신호를 이용한 차세대 생체인증기술 및 표준화를 주장하였다[17]. 김수형·노종혁·김영삼(2017. 2)은 모바일 결제, 스마트뱅킹 등에 따른 핀테크서비스에서 FIDO를 추가적인 인증요소로서 활용하여 보안을 강화하고자 하였다[18].

이처럼 블록체인과 FIDO는 보안성을 고려하여 모바일 및 IoT서비스에서의 인증수단으로 적절하다고 주장하고 있다. 그러나, 관련된 연구들에서는 아직까지 어느 분야에서 적합한지 검토하는 단계이며, 본인확인수단의 적합성에 대한 검증이 이루어지지 않았다. 따라서, 본 연구에서는 블록체인과 FIDO가 본인확인수단으로 적합한지 기준을 검토하고, 이를 적용할 방안을 제언하고자 한다.

2.3 본인확인수단의 적합성 기준

본 연구에서는 최근 이슈가 되고 있는 블록체인과 FIDO를 새로운 본인확인수단으로 적용함에 있어서 적합성을 검증하고자 한다. 우리나라의 본인확인수단은 2006년 제정된 '인터넷상의 주민번호 대체수단 가이드라인'에 근거하여 도입되었으며, '본인확인기관의 지정에 관한 고시' 등을 통해 본인확인수단으로서의 안전성, 편의성, 법적 보장성 등을 종합적으로 고려하여 필요한 용도에 맞는 수단을 선택·활용하고 있다[19].

본인확인기관은 본인확인업무의 수행가능성, 대체수단의 범용성, 대체수단의 편의성, 대체수단의 안전성 및 신뢰성, 대체수단 이용자의 보호 및 불만처리에 관한 사항 등에 대한 심사기준에 따라 평가하여 지정한다[20]. 그러면, 본인확인수단으로 지정되는 기준을 살펴보면, 한국인터넷진흥원(2013)은 본인확인수단을 안전성, 편리성, 안정성, 이용성을 심사기준으로 하고 있다[21]. Joseph Bonneau 외(2012), 금융보안연구소(2013) 등은 적용성(적용가능성, 적용비용, 기술중립성, 기존인프라 활용성), 편의성(소지, 사용, 발급, 교육편의성), 보안성(오프라인 공격대응, 온라인 공격대응, 거래조작 공격대응)을 기준으로 검토하였다[22,23]. 이에 대해 한국인터넷진흥원(2015)은 적합성 평가기준에 부합한 수준을 갖춘 경우 본인확인수단으로서 적용이 가능하다고 제시한 바 있다[24]. 이러한 의견을 정리하면, Table 1과 같이 일정 기준을 선정할 수 있다[25].

Table 1. Conformance criteria of identification means

Div.		Details
Essential Criteria	universality	Everyone has a characteristic (All subjects are universal)
	Persistence	It does not change over time
	Uniqueness	It is no identical features except itself
Realistic Criteria	convenience	It is easy to carry and use, making it easy to use anytime, anywhere
	Security	It can prevent fraudulent transactions in response to continuously develop new hacking technology
	Applicability	It is suitable for new environment such as smart phone
	Economics	It can save money when using identification service

3. 연구의 분석 틀

제4차 산업혁명의 핵심기술인 사물인터넷, 인공지능, 클라우드 서비스 등가 제공되는 과정에서, 개인정보가 집적화되고 거래됨에 따라 본인여부를 입증해야 할 사항이 점차 증가하고 있다. 그러나, 기존의 본인확인수단을 모든 정보환경에 적용하기에는 서비스 유형에 따라 한계가 있으므로, 다양한 인증수단을 도입하기 위해 적절한 판단기준이 마련되어야 할 필요가 있다.

이에 따라 본 연구에서는 블록체인과 FIDO을 본인확인수단으로 적합한지 7가지 기준에 맞추어 평가하고자 한다. 즉, 본인확인수단에 관한 기존 연구논문, 연구보고서, 백서, 뉴스 등을 바탕으로 문헌조사를 하였고, 그에 따른 본인확인수단의 적합성기준을 본질적 기준(보편성, 지속적, 유일성)과 현실적 기준(편의성, 보안성, 적용성, 경제성)을 구분하였다. 이렇게 구분된 기준을 이용하여 블록체인과 FIDO의 특징을 고려하여 본인확인수단으로서의 활용가능성 뿐만 아니라 미래사회에서의 적용가능성을 검토해 Fig. 3과 같이 제시하고자 한다.

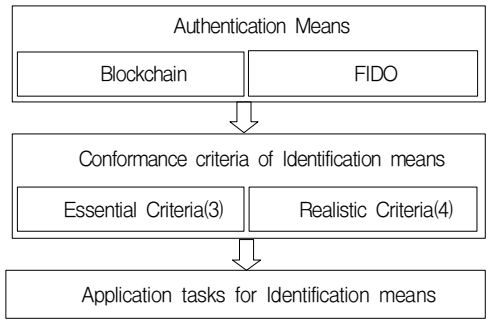

Fig. 3. Framework of this study

4. 연구결과

4.1 블록체인의 적합성분석 결과

본인확인수단의 적합성 기준 중에서 본질적 기준을 살펴보면, 첫째, 보편성에 대해서 블록체인은 거래정보를 기록하는 거래장부라고 하는데, 거래정보가 동의된 해당 기기 및 서비스 제공업체에 의해 자동으로 생성되어 활용되므로 별도의 기록을 관리할 필요가 없고, 분산네트워크 구조방식이어서 집중화된 중앙서버가 필요하지 않기 때문에 서비스가입자간의 연계로 사용이 가능하다. 현재 씨티은행, 도이치뱅크 등 42개 글로벌은행에서 블록체인을 도입하였으며, 에스토이나의 경우 디지털신원 시스템, 헬스케어시스템 등에 적용하고 있다[26]. 둘째, 지속성에 대해서 불록체인은 처리정보에 대해 변경이 불가능하고 시간이 지나도 거래정보를 변경하지 못하므로, 여러 분산된 정보를 결합하여 더 신뢰성 있는 정보를 형성할 수 있다. 따라서, 거래정보를 지속적으로 결합하여 본인확인이 가능하다. 셋째, 유일성에 대해서 블록체인은 본인의 행태정보를 거래행위로 분석하여 인증하기 때문에 다른 사람과 동일한 행태정보를 형성하지 않고 유일한 개인식별정보로 운영된다.

본인확인수단의 현실적 기준을 검토해 보면, 첫째, 편의성에 관하여 블록체인은 분산형 네트워크환경에서 거래정보를 확인하고, 별도의 거래정보를 저장하지 않고 연계하기 때문에 거래정보가 개방되고 투명하여 관리가 편하다. 또한, 언제어디서나 거래정보가 생성되면 식별정보로 활용가능하기 때문에 별도의 인증체제가 요구되지 않으므로 편리하다. 둘째, 보안성에 대해서 블록체인은 거래정보를 공동 소유하여 공개된 정보를 조작할 수 없고 분산된 네트워크구조로 결합하기 때문에 여러 정보 중에서 하나의 정보가 소실되더라도 서비스제공에 문제가 되지 않고, 거래정보의 오류가 발생하더라도 전체정보에 영향을 미치는 범위가 미비하여 서비스의 안전성을 갖는다. 셋째, 적용성에 관해서 블록체인은 공개된 오픈소스 프로그램을 활용하고 거래환경에서 발생하기 때문에 서비스를 이용할 경우 핀테크서비스와 연계하여 생성될 수 있기 때문에 기업뿐만 아니라 정부에서도 비용절감 및 위험율을 낮추는데 효과적이어서 보편적으로 사용가능하다. 이에 따라 정부기관의 14%는 2017년까지 적용할 계획이며, 정부관계자의 70%도 블록체인 비용, 시간, 위험 등을 줄이는데 효과적이라고 인식하고 있으며, 정부관계자의 90%도 2018년까지 관련 금융거래, 자산관리, 계약관리 규정 준수 등에 블록체인기술을 연계할 계획이다[26]. 넷째, 경제성에 관해서는 블록체인을 도입하면 신뢰된 중앙서버 및 중앙인증기관 없이도 서비스가 가능하기 때문에 기관설립 및 유지, 시스템의 유지보수, 거래 양성화 및 규제 등에 따른 비용을 절감할 수 있다. 또한, 블록체인을 위해서 사용자가 별도의 비용을 지불하기 않기 때문에 재정부담 없이 도입 가능한 인증서비스임을 알 수 있다[27-29]. 이렇게 블록체인을 대상으로 본인확인수단으로서의 적합성을 검토한 결과는 Table 2와 같다.

Table 2. Comparison of conformance criteria for Blockchain

Div.		Analysis Results
Essential Criteria	Universality	· It is possible to automatically execute approval record of the transaction by multiple participants
	Persistence	· It is increase accuracy of recording due to no change and cancellation of blockchain
	Uniqueness	· It is discriminated behavior information because personal transaction information is recorded and approved
Realistic Criteria	Convenience	· It is possible to trade in a distributed network environment without a trusted central server (third party) · It is open, transparent and traceable because of disclosing all transaction records
	Security	· It prevents manipulation of data transaction and ensures integrity by jointly possessing the account of the transaction history with all network participants · It is no failure as a decentralized network structure · It is not affected by the entire network if it occurs errors or performance

		degradation in some additive systems
	Applicability	· it has high scalability with open source program · It is possible to apply technology development(construction, connection, and expansion) to proper various purposes such as asset transaction, ownership verification, etc.
	Economics	· it reduces commission for establishment and operation of a third institution · It has a positive impact on transaction growth and regulatory costs. · It reduces the cost of operation, maintenance, etc for centralized system

4.2 FIDO의 적합성 분석 결과

FIDO는 금융거래를 비롯하여 통신사, 개인거래 등에서 인증수단이 확산되고 있으므로, 본인확인수단의 적합성 기준을 연계하여 검토하였다.

먼저, 보편성에 관하여는 현재 삼성전자, 구글, MS, 페이팔 등 200여개 글로벌 기업뿐만 아니라, 미국, 영국 등 해외정부 등이 가입된 FIDO Alliance를 중심으로 국제표준화하여 적용하고 있다[29]. 이에 대해서 현재 스마트폰사업자들은 FIDO기반의 생체인증서비스 기능을 탑재하여 제공하고 있다. 따라서 누구나 본인생체정보를 활용한 서비스를 이용할 수 있다. 둘째, 지속성에 관하여는 주요 신체정보 중에서 지문, 홍채 등과 같이 변화가 쉽지 않은 정보를 사용하기 때문에 시간이 지나도 지속적인 서비스가 가능하다. 셋째, 유일성에 대해서는 생체정보를 기반으로 하며, 정보유출로 인한 변경정보도 본인정보이기 때문에 본인식별정보로서의 유일성을 갖는다. 물론, 생체정보를 공유하는 상황이 발생하더라도 인증과정에서 추가인증을 통해 본인임을 확인할 수 있다.

그렇다면, 현실적 기준을 검토해 보았는데, 첫째, 편의성에 대해서는 패스워드를 별도로 기억할 필요가 없고 별도의 모듈을 설치할 필요없이 본인확인이 쉽게 이루어질 수 있다. 둘째, 보안성에 관하여는 별도의 패스워드를 기억하거나 별도의 장비에 생체정보를 저장하지 않고, 사용자의 단말기에서 처리한 결과값을 서버에서 검증받는 인증절차로 진행되므로, 외부해킹으로 인한 분실 또는 탈취되는 문제를 해결할 수 있다. 일례로, 삼성페이는 결재과정에서 지문인식을 활용한 FIDO기반 서비스를 제공하고 있으며, 결재요청 시 필요한 정보를 1회용 토큰으로 변환하여 결제대행업체나 카드사로부터 승인을 받는다. 이처럼 생체정보를 기록하지 않고 매번 새로운 토큰을 생성하기 때문에 전송과정에서 탈취되더라도 재사용이 불가능하며, 인증과정에서 추가 본인확인수단을 적용하므로 보안성이 높다[30]. 이외에도 한국인터넷진흥원에서는 'FIDO연계 기술가이드라인'을 제공하고 있어 표준화된 기준에 맞추기 때문에 FIDO의 안전성과 적절성을 확보할 수 있다. 셋째, 적용성에 대해서는 현재 공인인증서를 의무적으로 적용하지 않지만, 공인인증기술을 기반으로 한 기존서비스를 생체정보인증으로 대체하고 있다. 더욱이 FIDO는 핀테크와 함께, 모바일 결재 및 금융서비스에서의 본인확인수단으로 이용되고 있다. 넷째, 경제성에 대해서는 FIDO가 본인의 생체정보를 활용하기 때문에 별도 서버, 인증키, 보안토큰 등을 생성할 필요가 없어 기존의 인증수단보다 비용절감의 효과를 가져 올 수 있다[10]. 이처럼 FIDO를 본인확인수단으로 적용가능한지 적합성을 검토한 결과는 Table 3과 같다.

Table 3. Comparison of conformance criteria for FIDO

Div.		Analysis Results
Essential Criteria	universality	· It is possible to provide universal service by using PC, smart phone, etc.
	Persistence	· It is almost impossible to change the biometric information as authentication means, although it is a change in the device
	Uniqueness	· It is not possible to share biometric information, and it is not same characteristics in using personal information
Realistic Criteria	convenience	· It is unnecessary to remember PW · It is perfect response by non-ActiveX because of no module to install on PC · It is provided to convenient user identification process
	Security	· It is prevented abuse by losing PW · It is to reduce the risk of theft and is not forged with biometric authentication such as fingerprint, speaker, face, etc.
	Applicability	· It is supply scalability with FIDO UAF v1.0 Framework and certified authentication technology · It is possible to replace the PKI and PW with the biometric authentication. · It keeps the certificate private key in the secure area of the mobile phone
	Economics	· It is possible to save cost when using your identification service

5. 본인확인수단으로의 적용방안

본 연구에서는 블록체인과 FIDO를 대상으로 본인확인수단의 적합성 기준을 통하여 적용 가능성을 평가하였

다. 그 결과, 블록체인과 FIDO가 본인확인수단으로 적용할 수 있으며, 향후 신기술을 도입한 일반적인 서비스에도 적용할 수 있다. 따라서, 블록체인과 FIDO를 본인확인수단으로 적용하기 위해서는 다음과 같은 사항이 개선되어야 한다.

첫째, 블록체인과 FIDO를 본인확인수단으로 적용하기 위해서는 관련된 규정사항을 정비하여야 한다. 방송통신위원회의 '본인확인기관 지정에 관한 고시(이하 지정고시)'는 본인확인기관을 지정하고, 본인확인수단에 부합한 인증수단을 선정하였다. 물론, 기존에 지정된 본인확인기관은 주민등록번호를 기반으로 하기때문에, 적합성기준에 부합할 수밖에 없다. 즉, 우리나라는 지정고시에서 명시된 경우 외에는 본인확인수단으로 인정하지 않고 있다. 그러나 최근 아이핀, 공인인증서 및 휴대전화 외에 인터넷금융서비스의 확대로 인한 신용카드도 본인확인수단으로 지정되었다. 본인확인수단이 주민등록번호 기반에서 제공하고 있는 것과 달리 행태정보나 생체정보가 주민등록번호 없이도 본인확인이 가능하므로 기존의 규정이 개정되어야 한다.

둘째, 본인확인수단은 반드시 대면확인방식으로 판단하지 않고, 행태정보, 생체정보 등과 같이 특징정보를 활용하여 비대면확인방식으로도 본인임을 입증할 수 있다. 본 연구에서는 특징정보를 활용한 블록체인과 FIDO를 검토하였는데, 본인인증수단뿐만 아니라, 본인확인수단으로도 적합하다. 물론, 아직까지 정부는 비대면확인방식이 갖는 위험성때문에 대면확인방식에 기반을 둔 본인확인수단만을 인정하고 있다. 그러나, 전세계 IT기술의 확산과 더불어 스마트기기의 보급으로 구글 가입자 15억명, 드롭박스 사용자 10억명 등이 비대면 서비스를 이미 사용하고 있다[31], 따라서, 우리나라도 잠재적인 서비스이용자를 고려한다면, 블록체인과 FIDO를 본인확인수단으로 적용하여야 한다.

셋째, 본인확인수단을 적용하는 서비스범위를 검토하여 본인확인수단과 본인인증수단을 구분하여 적용하는 방안이 마련되어야 한다. 현재 우리나라는 「개인정보보호법」 제24조의 2, 「정보통신망법」 제23조의 2 등에 근거하여 본인확인수단을 제공하고 있다. 그러나, 지정고시에 근거한 본인확인수단만을 인정하다보니, 그 밖의 본인인증수단의 시장을 넓히는데 제약이 되고 있다. 즉, 과도한 본인확인수단의 적용은 해외거래를 제한할 뿐만 아니라, 과도한 비용발생으로 인해 기업의 재정 및 서비스 부담을 증가시키고 있다. 따라서 우리나라가 본인확인수단을 의무적으로 적용하기보다는 적절한 서비스의 범위를 한정하여 공공, 금융 등 업무상 필요한 분야에만 본인확인수단을 적용하고, 그 외 전자거래 및 엔터테인먼트 분야 등에서는 본인인증수단을 적용할 수 있도록 차별화된 적용규정이 필요하다.

넷째, 블록체인과 FIDO의 적절한 적용기준을 제시하여 안전성이 높은 인증수단으로 활용해야 한다. 본인인증수단에 관한 연구가 지속되고 있으며, 사물인터넷시대에 맞추어 본인인증수단의 개발이 이루어지고 있다. 더욱이, 정부는 인터넷 서비스의 제약요인이 되고 있는 공인인증서를 폐지하겠다고 발표하였다. 그러나, 공인인증서를 대체할 본인확인수단을 제시하지 못하고 있으며, 해외의 경우 스마트기기의 안전성과 편리성을 고려하여 생체인증기반 공인인증서를 제공하고 있다. 따라서, 블록체인과 FIDO를 연계한 인증기술을 개발하고 결합인증수단으로 활용한다면, 보다 강력하게 보안성을 높일 수 있다. 이처럼 지정고시에 명시된 본인확인수단으로 한정하기 보다는 '나'라는 입장에서 본인확인을 위한 기준으로 적용하기 보다는 '나의 행위'를 통한 본인임을 증명하는 기준으로 해석할 수 있어야 한다. 앞으로 거래상의 혼란을 방지하고 신뢰성있는 인터넷서비스 및 거래가 이루어진다면, 사물인터넷시대에서 다양한 정보유통 및 서비스가 안전하게 제공될 수 있으리라 본다.

6. 결론

우리나라는 「개인정보 보호법」 및 「정보통신망법」을 개정하여 법령상에 근거없이 주민등록번호를 사용하지 못하도록 하였으며, 서비스제공기관은 주민번호 대체수단인 본인확인수단을 적용하도록 의무화하고 있다. 따라서, 본 연구에서는 우리나라가 주민등록번호 및 대면확인방식만을 본인확인수단으로 한정하기 보다는 적합성 기준에 따라 다양한 본인인증수단을 적용해야 함을 주장하고자 하였다. 특히, 특징정보를 활용한 블록체인과 생체정보를 활용한 FIDO가 핀테크를 비롯하여 정부, 금융사, 통신사, 제조사, 카드사 등에서 데이터 위·변조방지 및 본인인증을 위해 사용되고 있어, 본인확인수단의 적합성기준(보편성, 지속적, 유일성, 편의성, 보안성, 적용성, 경제성)에 따라 적용 가능성을 검토하였다. 그 결

과, 블루체인과 FIDO는 본인확인수단으로 적절하며, 이미 잠재적 고객을 확보하고 있어 향후 활용가능성이 높음을 검증하였다.

블록체인과 FIDO를 본인확인수단으로 적용하기 위해서는 기존 관련 규정 및 기준을 개선하여야 하며, 반드시 주민등록번호 및 대면확인방식이 아닌 비대면 방식으로 가능함을 인정하여야 한다. 이미 핀테크를 비롯하여 금융서비스에서는 비대면확인방식이 적용되고 있으며, 본인거래의 안전성을 높이기 위해 인증수단을 결합하는 방식도 운영되고 있다. 이처럼 우리나라가 지정고시에 근거하여 본인확인수단을 지정하기보다는 서비스환경에 적합한 다양한 인증수단이 이용되도록 정책적 지원이 필요하다.

우리나라는 인터넷 서비스의 시작부터 정보화기반의 주요키값으로 주민등록번호가 사용되어 실명인증이 보편화되었다면, 해외의 경우 실명인증보다 본인인증이 인터넷서비스의 기반이 되었다는 데 차이가 있다. 따라서 우리나라가 기존에 갖고 있는 본인확인수단의 한계와 제한보다는 본인인증수단의 적용확대 및 자율적 도입을 지원해 나가는 정책과제들이 마련되어야 한다.

REFERENCES

[1] Naver wikipedia. *Blck chain anf FIDO*, https://terms.naver.com

[2] J. H. Yang. (2018). A Study on the Effect of Block Chain Application and Legal Issue in Logistics Industry. *Journal of Convergence for Information Technology, 8(1),* 187-199.

[3] S. J. Park. (2017). Blockchain paradigm and FIntech Seuciryty. *The Journal of The Korean Institute of Communication Sciences, 34(3),* 23-28.

[4] H. J. Mun. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology, 8(3),* 85-90.

[5] H. Y. Han. (2015). Features and Application Examples of Block Chain Technology. *KFTC Payment trends.* Korea Financial Telecommunications & Clearings Institute.

[6] S. Choi. et al. (2016). *Excavating research areas of FinTech through the analysis of its relevant technologies and policy trends at home and abroad.* Korea Internet & Security Agency.

[7] S. G. Lee. (2017). BlockChain Technology and market trend report. *S&T Market Report.* 47, Commercializations Promotion Agency for R&D Outcomes.

[8] Y. G. Kim. (2015). Blockchain technology and change in Finance. *KB knowledge Vitamin.* KB Financial Group Inc. Research Institute..

[9] Y. S. Kim, S. L. Cho & S. H. Kim. (2016. 5. 11). Concept and Application Status of Blockchain Technology. *Weekly ICT Trends.* Institute for Information & communications Technology Promotion

[10] S. S. Kim. (2018). *The more compatible and safer authentfication service using bio verification as like fingerprint, iris, face. etc.* Dreamsecurity. http://www.dreamsecurity.com/fido/

[11] Eugene Investment Co., LTD. (2016). *Next Generation Authentication FIDO and Biometric Authentication.*

[12] M. .K. Kim. (2016). Introduction of next-generation medical information authentication system using biometric information (fingerprint, iris, facial recognition, etc.). *21st Healthcare Korea Forum Conference Proceeding.* http://www.healthcarekorea.com/2016_21th/pdf/02_raon.pdf

[13] B. J. Park, T. J. Lee & J. Kwak. (2017). Blockchain-Based IoT Device Authentication Scheme. *Journal of the Korea Institute of Information Security & Cryptology, 27(2),* 343-35. DOI : 10.13089/jkiisc.2017.27.2.343

[14] S. Y. Oh & C. H. Lee. (2017). Block Chain Application Technology to Improve Reliability of Real Estate Market. *The Journal of Society for e-Business Studies, 22(1),* 51-64. DOI : 10.7838/jsebs.2017.22.1.051

[15] M. Vukolié. (2015). The quest for scalable block-chain fabric: Proof of work vs. BFT replication. *International Workshop on Open Problems in Network Security, Springer International Publishing.*

[16] S. H. Kim. (2016. 1). Fintech authentication technology based on FIDO. *The Journal of The Korean Institute of Communication Sciences, 33(2),* 59-65.

[17] J. S. Kim, S. J. Lee, B. S. Kim & S. W. Lee. (2015). Standardization trend of non-face authentication technology based on telebio recognition. *REVIEW OF KIISC, 25(4),* 43-50.

[18] S. H. Kim, J. H. Rho & Y. S. Kim. (2017) Next-generation Fintech authentication technology. *The Journal of The Korean Institute of Communication Sciences, 34(3),* 29-36.

[19] Ministry of Information Telecommunication. (2005).

Develeopment Status for Alternative menas of resident registration number and related research results.

[20] S. K. Kim. (2017). Authentication by creditcard from this mony. *Newso of Moneytoday.* http://news.mt.co.kr/mtview.php?no=2017031517435012042&outlink=1&ref=https%3A%2F%2Fsearch.naver.com

[21] Korea Internet & Security Agency. (2013). *Research on the Actual Condition of Electronic Signature System Usage.* Korea Internet & Security Agency.

[22] J. Bonneau et al. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. Proceedings of the *IEEE Symposium on Security and Privacy,* 553-567.

[23] Finance Security Institute. (2013). *Compliance assessment of new authentication technology.*

[24] Korea Internet & Security Agency. (2015) *Research on the Actual Condition of Electronic Signature System Usage(in Electronic Signature User).* Korea Internet & Security Agency.

[25] Y. J. Shin et al. (2015). *The Research for Alternatives of the Resident Registration Numbers and Improvement of Authentication Process.* Korea Internet & Security Agency.

[26] U. S. Kim. (2017). High-Trust government operation through Blockchain : possibility and case. *E-government research seminar in Korean Association for Public Administration.*

[27] Santander Innovatntures. (2015). *The FinTech 2.0 paper.* http://santanderinnoventures.com/fintech2/

[28] Korea Internet & Security Agency. (2016). *Top 10 internet issues in 2017*

[29] Y. S. Go & H. S. Choi. (2017). Change of business paradigm and its application: Focusing on block chain technology. *Korea Science & Art Forum Proceeding,* 13-29.

[30] D. G. No. (2015). *Easy-to-use payment market, 'FIDO'.* News of IT Chosun. http://it.chosun.com/site/data/html_dir/2015/10/14/2015101485009.html

[31] W. H. Choi. *FIDO. in facebook.* https://www.facebook.com/kftctiger?fref=ts

신 영 진(Shin, Young-Jin) [정회원]

- 1996년 2월 : 성결대학교 행정학과(행정학학사)
- 1998년 2월 : 단국대학교 일반대학원 행정학과(행정학석사)
- 2004년 2월 : 성균관대학교 일반대학원 행정학과(행정학박사)
- 2004년 10월 ~ 2012년 7월 : 행정안전부 정보화전략실 전문위원
- 2012년 8월 ~ 2013년 2월 : 고려대학교 정보보호대학원 연구교수
- 2013년 3월 ~ 현재 : 배재대학교 산학협력단 조교수
- 관심분야 : 개인정보보호, 정보보호정책, 전자정부, 4차 산업기술
- E-Mail : jinsyj@yahoo.com