블록체인 위의 암호화 정보는 개인정보인가? : 블록체인 기반의 분산신원인증 서비스를 중심으로

Is the encrypted information on the blockchain personal information?
: Focusing on blockchain-based distributed identity authentication service

류채연
위촉연구원
산업정책연구팀
cyryu@spri.kr

Executive Summary

블록체인(Blockchain)은 특정인의 신원을 인증하거나 금전을 이체하는 것처럼 '신뢰성 있는 서비스 구현'할 때 활용하기 적합한 분산화 기술이다. 분산원장을 활용하여 신뢰성을 확보하고, 블록 위 정보의 열람으로 인해 발생할 수 있는 피해를 막고자 암호화 기술을 기반으로 구현한다. 최근에는 이러한 블록체인 기술을 분산신원인증 서비스를 만드는데 이용하고 있다. 분산신원인증 서비스의 구현시 반드시 블록체인 기술이 이용되어야 하는 것은 아니지만, 신원인증 당사자가 중심이 되는 탈중앙 구조가 블록체인의 분산원장 기술구조와 유사해 유용하게 활용하는 것으로 보인다.

이용자가 블록체인 기반의 가상화폐·신원인증 등 서비스를 이용하기 위해서는 가입 절차를 거쳐야 한다. 그 과정에서 특정 개인을 식별하는 값들은 휘발되고 암호화된 임의의 대푯값을 부여받아 서비스를 이용한다. 또한 임의의 대푯값은 블록 위에 공개 저장되고 누구나 열람할 수 있다. 이해관계인들은 공개된 저장소에 개인을 대표하는 값이 저장됨에도, 암호화된 사정만으로 해당 정보가 재식별될 여지가 없는 안전한 정보라고 신뢰한다.

과연 블록체인 위 암호화 정보는 재식별이 불가능한 정보(익명정보)인가? 개인정보(식별가능정보 내지 가명정보)에 해당하지는 않는가? 암호화가 비식별 조치의 수단으로 이용된다는 전제에 비춰보면 식별이 곤란하거나 쉽지 않은 정보라는 점에는 이론의 여지가 없다. 다만 재식별이 불가능할 정도의 익명정보라면 해당 서비스를 제공하는 사업자는 개인정보보호법상의 보호조치를 이행할 의무가 없다. 반면 식별가능성이 있는 개인정보 내지는 가명정보라면 개인정보보호법에 따른 보호대상이 되는 만큼, 서비스 제공자는 해당 법률의 수범자로서 관련된 의무를 이행해야 한다.

본 보고서에서는 이러한 관점에서 블록체인 기반의 분산신원인증 서비스를 중심으로, ① 블록 위 암호화 정보가 무엇이고 ② 이 암호화 정보가 개인정보에 해당하는지를 검토하고자 한다. 그 결과에 따라 자격 검증 발급정보는 개인정보보호법상의 개인정보가 아니고, DID와 공개키는 가명정보는 아니지만 식별가능정보가 될 여지가 있다는 견해를 제시한다. 따라서 분산신원인증 서비스 제공자들은 DID와 공개키에 대하여 주의를 기울일 필요가 있다고 판단한다.

디지털 전환 흐름이 가속화되고 블록체인 등 신기술이 발전하는 만큼, 개인정보보호법과 하위 법령 및 관련 지침을 바탕으로 각 사안별로 구체적 타당성을 꾀하는 노력이 필요하다. 본 보고서는 연구자의 관점에서 이러한 내용을 살펴보았으며, 블록체인 기반의 서비스에 대한 개인정보보호법 적용 여부를 검토할 때 하나의 참조자료로 활용될 수 있길 기대한다.

Blockchain is a decentralized technology suitable for 'implementing reliable services', such as authenticating a specific person's identity or transferring money. It is implemented based on encryption technology to secure reliability by using distributed ledger and to prevent damage that may occur due to the reading of information on blocks. Recently, such blockchain technology is being used to create a distributed identity authentication service. Although blockchain technology does not necessarily have to be used when implementing a distributed identity authentication service, it seems that the decentralized structure centered on the identity authentication party is similar to the distributed ledger technology structure of the blockchain and is usefully used.

In order for users to use services such as blockchain-based virtual currency and identity authentication, they must go through a registration process. In the process, the values that identify a specific individual are volatilized and given an encrypted arbitrary representative value to use the service. In addition, arbitrary representative values are publicly stored on the block and can be viewed by anyone. Stakeholders trust that even though a value representing an individual is stored in a public storage, it is safe information that cannot be re-identified only by encrypted circumstances.

Is the encrypted information on the blockchain really unrecognizable information (anonymous information)? Is it not personal information (identifiable information or pseudonymous information)? Given the premise that encryption is used as a means of de-identification, there is no question that information is difficult or difficult to identify. However, if the information is anonymous to the extent that re-identification is impossible, the service provider is not obligated to implement the protection measures under the Personal Information Protection Act. On the other hand, if identifiable personal information or pseudonymous information is subject to protection under the Personal Information Protection Act, the service provider must fulfill the relevant obligations as a beneficiary of the applicable law.

From this perspective, this report intends to review ① what is encrypted information on the block and ② whether this encrypted information corresponds to personal information, focusing on the blockchain-based distributed identity authentication service. According to the results, the issue of qualification verification information is not personal information under the Personal Information Protection Act, and the DID and public key are not pseudonymous information, but suggest that there is room for identifiable information. Therefore, it is judged that distributed identity authentication service providers need to pay attention to DID and public key.

As the flow of digital transformation is accelerating and new technologies such as blockchain develop, it is necessary to make an effort to find specific validity for each case based on the Personal Information Protection Act, subordinate statutes, and related guidelines. This report looked at these contents from a researcher's point of view, and it is expected that it can be used as a reference when examining whether the Personal Information Protection Act is applied to blockchain-based services.

I 논의의 배경

▨ 금융거래나 신원인증과 같은 서비스에서 생성된 데이터는 서비스 이용 당사자의 개인정보*를 포함하기 때문에, 제3자가 이러한 데이터를 수집하고 처리할 때 개인정보주체의 권리를 보호하기 위해 제정된 개인정보보호법의 규제를 받게됨

* 개인정보보호법 제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

○ 개인정보처리자가 개인정보 주체로부터 개인정보의 수집·유통·처리 등에 대한 사전동의를 얻어야 하고*, 이를 위반하면 과태료 등의 제재*가 부과됨

* 개인정보보호법 제15조(개인정보의 수집·이용)에서 개인정보처리자가 개인정보 주체의 동의를 받거나 동조 1항 2호 내지 6호의 예외 요건에 해당하는 경우여야 수집·이용·제공을 허용

* 개인정보보호법 제75조(과태료) 제1항 제1호에서는 제15조 제1항에 위반하여 개인정보를 수집한 경우, 5천만 원 이하의 과태료를 부과

○ 또는 개인정보처리자가 가명처리*(개인정보보호법상의 비식별화 조치)를 통해 해당 정보를 가명정보로 바꾸어 개인정보를 활용해야 함

* 개인정보보호법 제2조(정의) 1의2호 "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

○ 블록체인 기반의 분산신원인증 서비스에서 참여자를 대표하는 암호값이 포함된 데이터가 생성 및 블록에 저장되는데, 암호값의 경우 제3자가 본래 암호화 이전의 내용을 알아보기 어렵다는 특징 때문에 개인정보보호법 상의 보호대상(개인정보)에 해당하는지가 모호

- 개인정보보호법은 ① 이름·주민번호와 같은 특정인의 식별 정보(개인정보보호법 제2조 제1호 가목)나 ② 식별가능한 정보(개인정보보호법 제2조 제1호 나목) 또는 ③ 추가 정보의 결합을 통해 식별할 수 있는 가명정보(개인정보보호법 제2조 제1호 다목)를 보호 대상으로 삼음

- 블록체인 기반의 분산신원인증서비스에서 참여자를 대표하는 암호값은 성명·주민번호와 같은 식별정보에 해당되지 않으나, 식별가능정보 또는 가명정보에 해당할 여지가 있음

- 만약 재식별 가능성을 검토한 결과 나열한 개인정보 유형 중 어디에도 해당되지 않는다면, (재)식별가능성이 없는 익명정보에 해당하여 개인정보보호법상 보호대상이 아님

▨ 따라서 개인정보보호법의 개인정보에 대한 요건을 기초로, 암호화 정보의 재식별 가능성을 포렌식 기술 현황을 고려하여 개인정보 해당성을 판단해야 함

- (법률적 측면) 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보(식별가능정보)인지, 추가 정보를 결합해 재식별이 가능하지만 추가 정보를 별도로 보관함으로써 재식별 가능성을 통제가능한 정보(가명정보)인지를 검토

- (포렌식 기술 측면) 완전무결한 암호화는 있을 수 없기에, 해당 암호화 정보가 현 시점에는 식별이 곤란하더라도 이후 기술 발전 흐름에 따라 기타 정보와의 결합을 통해 포렌식 기법으로 재식별 될 여지가 있음을 고려해야 함

▨ 이번 보고서에서는 블록체인 기반의 분산신원인증 서비스를 중심으로 블록 내 암호화 정보가 무엇인지 살핀 후, 해당 암호화 정보가 익명정보인지 아니면 개인정보(식별가능정보 내지 가명정보)에 해당하는지 검토하겠음

○ 분산신원인증 서비스에서 블록 위에 공개 저장되어 제3자가 열람할 수 있는 암호화 정보에는 무엇이 있는가?

○ 블록 위 암호화 정보는 제3자에 의해 재식별될 여지가 없는 익명정보인가?
아니면 기타 블록체인 위에 노출된 정보의 결합을 통해 식별될 수 있거나 암호화가 가명처리에 해당하여 가명정보로 볼 수 있는가?

○ 개인정보해당 여부에 따라 블록체인 기반의 분산신원인증 서비스 제공 주체에게 부여되는 주의의무와 책임의 유무가 결정됨

▨ 검토 결과는 블록체인 기반의 분산신원인증 서비스를 제공하는 사업자들에게 개인정보보호법의 적용 여부에 대한 예측가능성을 확보하여, 이와 관련된 전략을 수립할 때 참고 자료로 활용할 수 있다는 점에서 의의가 있음

II 암호화 기반의 블록체인 기술

1. 분산 원장 기술로서의 블록체인

▨ 블록체인의 의의

○ 블록체인(Blockchain)은 최근 WEB3.0과 함께 새롭게 조명을 받고 있는 기술로, 현재는 스마트 컨트랙트·NFT(Non-Fungible Token)·분산신원인증 서비스까지 다양한 영역에서 활용

○ 계좌 이체·신원 인증과 같이 일정한 형식의 데이터가 지속적으로 생성되는 환경에서 활용하기 적합함

○ 새로운 정보가 생성될 때마다 블록이 하나씩 생겨나며, 각 블록들은 앞뒤 블록의 주소값을 포함하고 있어 블록들이 체인처럼 연결됨

- 따라서 특정 블록의 내용을 삭제하거나 변경하면 앞과 뒤의 블록도 연쇄적으로 영향을 받아 결과적으로 체인이 끊어지게 되므로, 위변조가 곤란

○ 최근에는 질병관리청의 COOV·경찰청과 행정안전부의 모바일운전면허증과 같은 분산신원인증서비스에 블록체인이 활용되고 있음

▨ 분산 원장 기술(Distributed Ledger Technology)

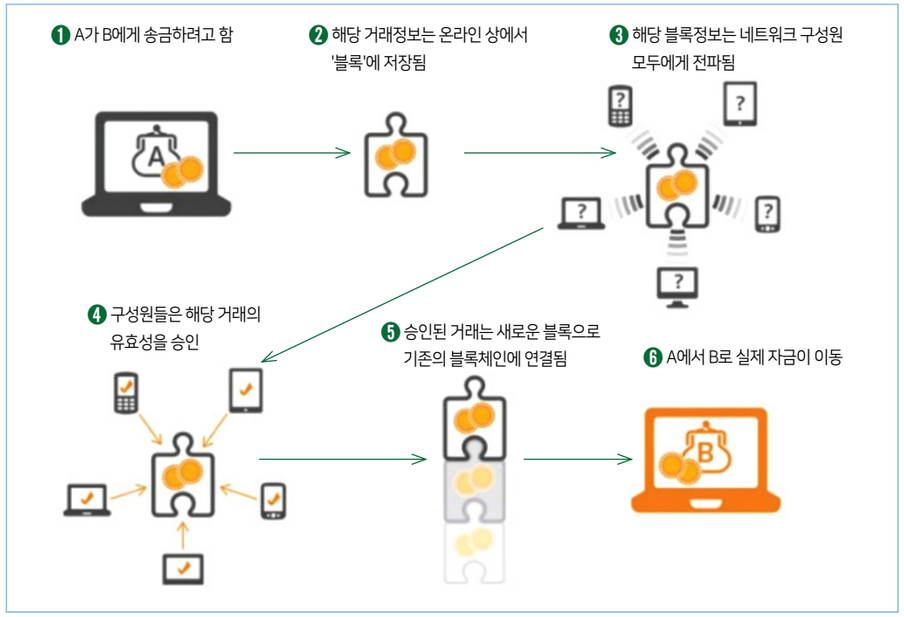
○ 누구나 열람할 수 있는 장부에 거래 내역을 투명하게 기록한 후, 기록된 장부를 네트워크 참여자 모두가 나누어서 보관

○ 새롭게 블록을 생성할 때에는 각 참여자들이 보관 중인 장부 사본과 대조하는 작업을 통해 진위 여부를 검증

- 네트워크 참여자들이 보관 중인 장부를 모두 동일 내용으로 위변조하지 않는 이상 제3자에 의한 임의 조작이 불가함

○ 이처럼 중앙기관이 없이 참여자들만으로도 신뢰도 높은 데이터 고리를 형성할 수 있다는 점에서 의의가 있음

[그림 1] 블록체인 기술의 금전 거래 절차



Financial Times - Thomson Reuters(2016. 1. 16), "lock-chain technology: Is 2016 the year of the block-chain" 번역

2. 블록체인에 활용된 암호화 기술

▨ 블록체인 내 암호화 기술

○ 성명·주민번호와 같이 특정인을 식별하는 정보를 직접 이용하지 않거나, 회원 가입 과정에서 성명·주민번호를 입력했더라도 이는 가입과 동시에 대푯값을 부여받으면서 휘발되어 별도로 저장되지 않음

○ 또한 특정인을 대표하는 임의의 값을 생성하여 이를 활용하며, 그 대푯값 또한 암호화시킨 후 블록 위에 저장

○ 결국 블록체인 내 암호화 과정은 공개 저장된 정보를 제3자가 열람시 발생할 수 있는 위험 상황을 사전에 예방하기 위한 안전 장치로서의 역할로 보임

- 암호화를 통해 얻어진 정보는 본래의 내용을 알기 위해 복호화 및 복호화된 결과를 재식별하는 노력이 필요함
- 따라서 외부에서 암호화 정보를 침해(열람 및 이용) 여부를 결정할 때 하나의 장벽으로 기능

▨ 공개키 암호화(비대칭 암호화 방식) 기술

○ 1976년 당시 미국의 암호학자 베일리 휫필드 디피(Bailey Whitfield Diffie)와 미국 수학자 마틴 에드워드 헬만(Martin Edward Hellman)이 학계에 발표한 것이 학술상 최초의 공개키 암호화 이론

○ (내용) 이해관계인 및 그 이외의 자들이 모두 공유하는 공개키와 당사자만 보유하는 개인키를 한 쌍으로 삼아 이를 활용하는 암호화 방식

- 공개키와 개인키가 같지 않아 비대칭 암호화 방식으로 불리며, 상대적으로 보안성이 높음*

  * 이와 반대로 비밀키(대칭) 암호화 방식의 경우 한글 파일에 암호를 걸 때처럼 쌍방이 동일한 암호를 주고 받으며 열람하는 방식을 취하므로, 암호 전달 과정에서 제3자가 암호키를 해킹시 암호화된 정보의 복호화를 통한 유출 사고로 이어질 수 있음

- 가상화폐 관련 블록체인 서비스에서는 가상계좌의 생성을 위해 당사자에게 임의로 개인키를 발급하고, 이를 통해 가상계좌번호에 대응하는 공개키 및 지갑주소값을 생성

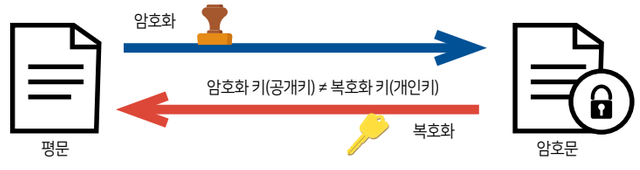
○ (키종류) 누구나 알 수 있는 공개키와 당사자만 보관·관리하는 개인키를 이용

- 공개키(Public Key) : 메시지의 전달을 위한 암호화 및 전자서명 용도의 복호화에 활용되며 공개된 정보로 비밀로 보관할 필요가 없음

  * 누구나 알 수 있는 값이므로 키 전달 과정에서 유출 위험을 고려할 필요가 없음

- 개인키(Private Key) : 전달받은 메시지의 복호화 및 전자서명 용도의 암호화에 사용되며, 자신만이 알 수 있게끔 스스로 보관 및 관리

[그림 2] 블록체인 공개키 암호화 및 복호화 과정



금융보안원 - 금융부문 암호기술 활용가이드 44면 (2019.1)

○ (공개키 암호화의 용도) 공개키 암호화 방식은 메시지 전달 및 전자서명의 용도로 활용됨

- (메시지 전달 용도) 계좌 이체와 같이 특정 메시지를 전달하는 과정에서 공개키 암호화를 활용

  * 공개키는 모두가 알 수 있는 암호로 은행 계좌 번호, 개인키는 계좌에 설정된 4~6자리 비밀 PIN 번호와 같이 이해할 수 있음

  * 예를 들어 송금을 하려는 자 A가 "A가 B에게 300달러를 이체한다"라는 이체 거래 내용의 메시지를 상대방 B에게 보내려 한다면, B의 공개키(B의 계좌번호와 같이 공개된 정보)를 사용해 암호화(잠금)한 후 수신자 B에게 보내고, 수신자 B는 해당 공개키에 대응하는 B 자신의 개인키(B 자신만이 보관하는 비밀번호)를 이용하여 복호화(해제)를 진행함

  * 별도로 수신자에게 비밀키(개인키)를 전달하는 과정이 없어서 암호의 유출로 인한 문제 상황을 막을 수 있고, 메시지도 암호화되어 있어 전달 과정에서 보안성을 높일 수 있다는 점에서 의의가 있음

- (전자서명 용도) 본인 인증 용도로 공개키 암호화를 활용

  * 예를 들어 개인키를 가진 A가 자신의 정보를 A의 개인키를 통해 암호화(잠금)하여 전달하면, 이를 수신한 B는 송신자 A의 공개키를 통해 복호화(해제)함으로써 메시지가 A에 의해 작성되었다는 사실의 진위를 검증함

  * 송신자의 개인키와 공개키를 활용하여 송신자의 신원을 인증한다는 특징이 있음

▨ 해시 함수 암호화 기술

○ (내용) 해시 함수(알고리즘)*에 특정한 입력값을 집어넣으면 알파벳과 특수 기호 및 숫자가 무작위로 조합된 일정한 길이의 출력이 만들어짐

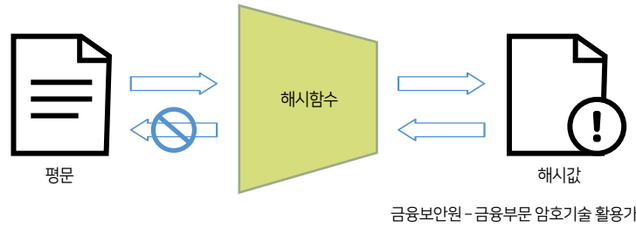
- 공개키 암호화와 달리 암호화 과정에 키(Key)를 사용하지 않음

  * 해싱 알고리즘은 SHA-256 등 다양한 종류가 있음

○ (특징) 일방향 함수이기 때문에 해시 암호값은 복호화를 통해 원래값으로 복원이 불가함

- 따라서 가장 보안성이 높은 암호화 유형에 해당

[그림 3] 블록체인 해시 함수 암호화 과정



금융보안원 - 금융부문 암호기술 활용가이드 45면 (2019.1)

○ (용도 - 진위 여부 검증) 거래 과정에서 생성된 데이터가 위변조되었다고 의심이 될 때, 해싱값을 대조해봄으로써 그 진위 여부를 검증할 수 있음

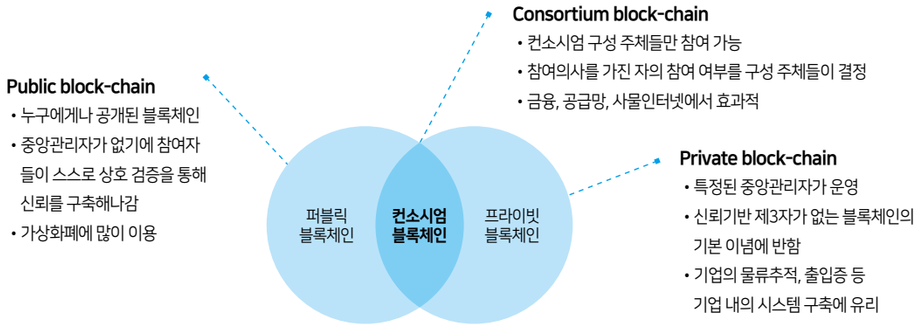
- 해시함수는 입력값이 완전히 일치하지 않는 이상 출력값이 동일할 가능성이 매우 낮기 때문에, 의심되는 해싱값을 원데이터에서 얻어진 해싱값과 같은지 확인해 봄으로써 진위를 확인

- COOV 앱*에서 백신접종 사실에 대한 진위를 확인할 때, 이 해시 함수값을 이용함

*블록체인 기반의 코로나19 예방 접종 인증 시스템으로서 코로나 백신 예방접종 사실을 질병청을 통하여 전자문서로 입증

II 블록체인의 유형 및 활용 현황

[그림 4] 유형에 따른 블록체인 활용



▨ 개방형 블록체인(Public Blockchain)

○ 누구나 자유롭게 참여 및 탈퇴가 가능한 블록체인 네트워크

○ 특징

- 별도로 신뢰기관을 두지 않아도 각 참여자들이 P2P 방식으로 검증 기관으로서의 역할을 하므로 높은 신뢰도를 확보할 수 있음

- 단, 모든 참여자들의 검증을 거치다 보니 속도가 느리다는 단점이 있음

○ 활용 예시

- 비트코인, 이더리움 등 가상화폐 : 신뢰 기관의 승인을 얻지 않아도 누구든지 새로운 블록 생성에 참여 가능하며, 가상화폐 보상액을 참여 유인으로 설정함으로써 블록체인 네트워크가 자생적으로 운영될 수 있게끔 구현

▨ 컨소시엄 블록체인(Consortium Blockchain)

○ 신뢰기반 제3자인 기관 여러 개가 모여 컨소시엄을 구성한 형태의 블록체인

○ 퍼블릭 블록체인과 프라이빗 블록체인의 혼합 형태

○ 특징

- 신뢰 기반 제3자인 인증 기관이 여러 개 존재
- 분산형 구조인 블록체인에 기존의 중앙집권형 시스템을 추가한 모델이다 보니 진정한 블록체인의 형태는 아니지만, 퍼블릭 블록체인에서 해결되지 못한 책임자 불특정의 문제점을 개선할 수 있음
- 다만, 이로 인해 신뢰기반 제3자 없는 서비스를 표방하는 블록체인의 기본 이념에 반하는 측면이 있음

○ 활용 현황

- 모바일 운전면허증* : 행정안전부와 경찰청이 인증기관으로 참가하여 가입자의 운전면허 자격에 대하여 검증하며, 가입자는 휴대폰 단말기에 해당 자격검증정보를 저장한 후 스스로 이를 관리 및 사용함

  * 가입자가 자신의 휴대폰 분실신고시 해당 서비스 이용이 제한된다는 점에서 이용자의 참여 여부를 결정하는 신뢰기반 제3자가 존재하는 컨소시엄 블록체인의 특징을 확인할 수 있음

▨ 폐쇄형 블록체인(Private Blockchain)

○ 기관 내지 조직과 같은 권한자에 의해 승인을 받지 않으면 접근할 수 없는 비공개 블록체인 네트워크

○ 특징

- 참여자가 제한되다 보니 공개형 블록체인에 비해 작업 처리속도가 빠르고 신뢰도가 높음
- 참가 여부를 결정하는 중앙기관을 두기 때문에 개인정보처리자의 명확한 특정이 가능함
- 다만, 블록체인의 기본 이념인 완전한 분권형 네트워크에서 벗어나 신뢰기반 제3자를 상정하다보니 진정한 블록체인과는 궤를 달리하는 측면이 있음

○ 활용 현황 및 사례

- 홈넘버(Home Number) : 온라인 플랫폼 업체의 개인정보보호조치 미흡 사례를 기회로 삼아 블록체인 기술을 이용해 고객정보의 암호화를 통한 판매구조를 만든 보안플랫폼 솔루션
- 투버스(Tubers) : 블록체인 기반 농산물 유통이력관리 플랫폼으로 농작물 재배에 필수적인 종자의 생산·유통·소비 과정의 이력 정보를 표준화하고 통합관리토록 함

▨ 탈중앙화 구조를 표방하는 블록체인의 기술 사상을 그대로 구현한 개방형(퍼블릭) 블록체인부터, 블록체인을 기반으로 중앙집권적 구조로 회귀한 폐쇄형(프라이빗) 블록체인까지 다양한 유형이 존재

▨ 제공하고자 하는 서비스의 내용과 특성에 따라 블록체인 유형을 선택하여 구현

III 블록체인 기반의 분산신원인증 서비스

1. 분산신원인증(DID: Decentralized Identity)의 의의

▨ 자기주권 신원(SSI, Self-Sovereign Identity)모델을 실현할 수 있는 기술

○ (자기주권 신원 모델, SSI) 신원정보의 소유와 이용 권한을 개인정보주체가 스스로 가짐으로써 자신의 정보에 대한 주권을 실현하는 모델

- 기존 신원 모델(개별 신원 모델, 연합 신원 모델)의 개인정보 유출 위험에 대한 취약점을 보완한 신원 모델

- 자신을 증명하기 위해 각 서비스 제공자 혹은 제3기관에게 매번 개인정보를 제출하던 기존의 구조를 탈피하여, 개인이 하나의 통일된 양식으로 자신의 개인정보를 직접 관리하다가 필요시에 이를 제출

[그림 5] 블록체인 기반 자기주권 신원 모델(SSI)의 형태와 특징

<자료> NIST, 'A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems'('20.01)을 재구성한 정보통신기획평가원, 'Post-코로나 시대의 뉴노멀 기반 DID와 디지털화폐 동향' 17면 자료 기반

▨ 개인정보주체가 자신의 개인정보에 대한 통제권을 갖되, 개인정보와 관련된 매개값을 암호화하여 분산원장에 기록함으로써 해당 정보의 신뢰성을 확보하는 기술

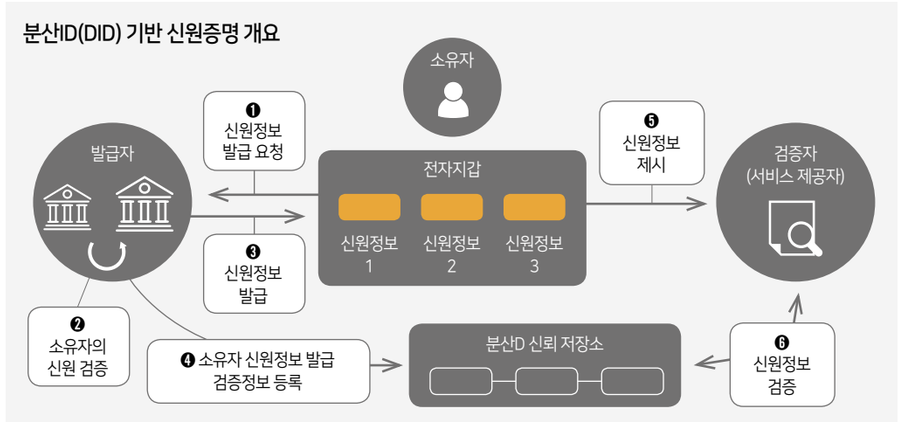
○ (개인정보의 보안성을 확보) 중앙관리자에 의해 신원정보가 관리되는 것이 아니기에 서비스 이용자의 개인정보는 중앙관리자 또는 외부의 제3자에 의해 수집되거나 악용될 염려가 줄어듬

○ (개인정보를 선택적으로 공개 가능) 필요 최소한의 정보만으로 자격을 증명하거나 본인임을 인증할 수 있어 불필요한 개인정보의 노출을 줄일 수 있음

- 예를 들어 백신접종 사실을 인증하기 위해서는 개인정보주체가 백신접종 증명서를 통하여 접종 사실 이외에도 접종자에 대한 이름·주민번호·주소 등의 정보를 제시하게 됨

- 하지만 분산 신원인증 서비스를 이용하면 전자 문서를 통하여 접종 여부에 대한 최소 정보 (접종일자·회차·접종병원·백신종류)만을 제공함으로써 코로나 백신 예방접종 사실을 증명할 수 있음

[그림 6] 분산ID(DID) 기반 신원증명 개요



금융보안원이 개발한「분산ID 신원관리 프레임워크」, 정보통신단체표준(TTA표준)으로 채택, 금융보안원, "보도자료", 2020.12.14.자. 수정본

2. 분산신원인증(DID) 서비스의 활용 모델 및 현황

▨ 분산신원인증(DID) 서비스 활용 모델

○ 신원확인

- 편의점에서 주류를 구매하기 위하여 성인 인증이 필요한 경우와 같이 나이 등의 신분 정보를 확인하기 위하여 분산신원인증을 이용

* 당사자는 주민등록증·운전면허증·사원증 등의 실물이 없이도 본인을 식별할 수 있는 정보를 발급받아 모바일 등의 단말기 내에 저장 및 관리하다가 필요한 경우가 발생하면 이를 사용

* 신원인증을 요구할 필요가 있는 기관들은 이와 연계된 서비스 앱을 추가로 개발함으로써 신원확인용 분산신원인증 서비스 활용에 참여

- 이를 쿠팡 등 O2O(Online to Offline, 온라인·오프라인 연계 서비스)에 적용하면, 주문·배송 단계에서 연령·주소 등의 필요최소한의 정보만 제공함으로써 개인정보 유출 우려를 감소시키는 모델을 구현 가능
- 간편하면서도 정확하게 진위 여부를 확인할 수 있다는 이점이 있음

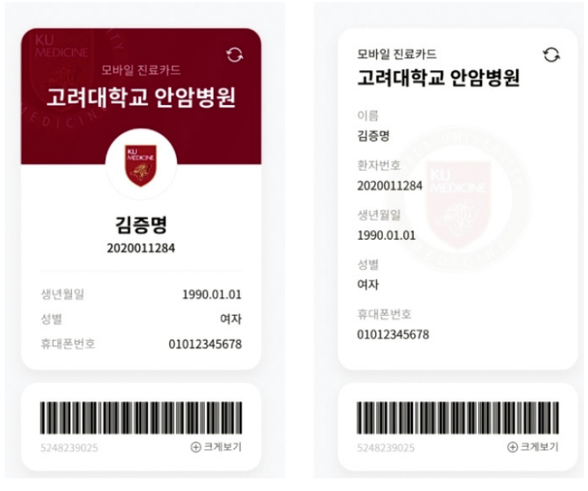
○ 본인인증

- 전자금융서비스 상에서 로그인 후 자금 이체를 원하는 경우처럼, 가입자 본인확인이 필요한 경우에 분산신원인증을 이용
- 분산신원인증 기반의 개인정보인증서를 발행하면, 제3자의 개입 없이도 사용자가 직접 비대면 인증 요청 및 본인 확인을 진행할 수 있음

○ 제증명서 발급

- 종래 종이 증명서를 통해 발급한 증명서류를 분산신원인증 앱을 통해 발급
- (고려대학교 병원 모바일 진료카드) 병원에 방문한 환자가 전자문서발급 기능을 가진 모바일 진료카드를 통해 처방전을 발급받고, 해당 앱을 통해 연계된 병원에 제출
- 종전에 비해 절차가 간소화되고 발급 횟수가 줄어들어 제증명 발급시 필요한 비용을 절감 가능

[그림 7] 고려대학교의료원에서 제작한 분산신원증명(DID) 진료카드



[자료] 뉴스원 2022.05.17. "진료 접수부터 방전까지…SKT '이니셜' 앱으로 관리한다" 기사 참조

○ 자격증명

- 병무청의 복무 증명서, 코로나19 백신 접종 증명서 등 개인의 자격을 확인하기 위하여 분산신원인증을 이용
- (e-병무지갑) 입영통지서·전역증·사회복무원증 등 병역 관련 문서를 발급받아 온라인으로 제출할 수 있으며, 장병내일준비적금 가입시 은행을 방문하지 않아도 상품에 가입하거나 군장병 혜택의 휴대폰 요금제에 가입할 수 있음
- 각종 우대 및 편의 서비스에 대한 병역의무자들의 접근이 용이해졌고, 자격증명 문서의 진위에 대한 신뢰를 확보할 수 있음

[그림 8] 병무청에서 제작한 e-병무지갑 서비스

[자료] e-병무지갑 서비스 개요도, 병무청 제공

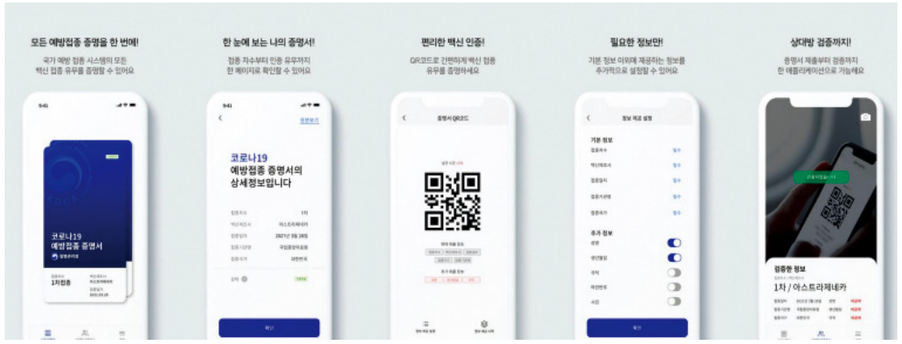
▨ 블록체인 기반의 COOV 서비스

○ (앱 이용자의 증명서 발급 요청) 질병관리청이 접종 정보를 서명값과 함께 제공하고, 이를 수령한 앱 이용자는 전자지갑 내에 접종 정보를 저장

○ (앱 이용자가 증명서를 이용) 제3기관이 자격증명을 요청시 앱 이용자는 자격증명 중 필요 부분만을 추려서 앱 이용자의 서명값과 함께 요청기관에 전달

○ (자격증명 요청기관의 확인) 요청기관은 수령한 값 중 서명값을 통해서는 출처의 진위를 확인하고, 자격증명 내용은 블록 위에 저장된 자격증명 발급사실 정보와 대조를 통해 진위 여부를 검증한 후 앱 이용자의 접종 정보를 확인

[그림 9] 백신 접종 정보가 저장되는 앱 COOV



[자료] 질병관리청, COOV 서비스 매뉴얼 참조

▨ 블록체인 기반의 모바일 운전면허증

○ (앱 이용자의 발급 요청) 모바일 운전면허증 앱 이용자가 발급 요청시 행정안전부와 경찰청이 요청자의 운전 자격을 서명값과 함께 발급하고, 앱 이용자는 이름·주민 번호·주소·운전면허종류 등 받은 값을 휴대폰에 저장

○ (앱 이용자의 운전면허증 이용) 앱 이용자는 신원인증을 요구받으면 필요한 항목만을 추려서 자신의 서명값과 함께 요구기관에 전달

○ (신원인증 요구기관의 확인) 요구기관은 서명값을 통해 출처의 진위를 확인하고, 운전자격 내용을 블록 위 발급정보 값과 대조해 진위 여부를 검증 후 신원정보를 확인

○ 신원인증을 요구하고자 하는 기관들은 모바일 운전면허증과 연계된 서비스 앱을 추가로 개발함으로써, 모바일 운전면허증의 활용에 참여 가능

Ⅳ 블록체인 위 암호화 정보는 개인정보인가?

1. (블록체인 기반의 분산신원인증 서비스) 암호화 과정

▨ 앱 사용자(소유자)와 발행기관은 각자의 휴대폰을 통해 인증 및 가입에 성공하면 알파벳과 숫자가 임의로 조합된 개인키를 부여받는데, 이를 통해 암호값인 공개키와 DID(Decentralized Identity)*값을 생성함

* 생성주체는 각 신원인증이 하나의 대표성을 갖는 경우라면 동일한 DID를 계속 사용하지만, 각기 다른 대표성을 검증하기 위한 경우라면 동일 주체가 각 신원인증별로 다른 DID를 생성하여 사용할 수도 있음

○ 앱 가입시 인증 과정에서 사용된 이름·생년월일·휴대전화번호 등의 개인정보는 서비스 제공자에게 저장되지 않음

○ 개인키 또한 각자 앱이 설치된 휴대폰 등의 개인 단말기에만 저장되어질 뿐 사업자나 외부 관계자에게 공개되지 않기 때문에, 외부 유출 가능성이 낮음

○ 결국 공개키와 DID만 블록 위에 저장되는데, DID는 각 주체들의 식별값일 뿐 신원정보가 아니므로 블록 위에 저장되거나 분산원장에 기록되어도 문제가 없음

[그림 10] 블록체인 기반의 모바일 운전면허증

모바일 신분증 개발지원센터 내 연계서비스 활용 사례 :
편의점에서 주류 구입시 성인임을 인증하기 위해 모바일 운전면허증의 QR코드를 스캔하고 확인

▨ **앱 사용자가 접종 사실에 대한 증명을 발행기관인 질병관리청에 요청하면, 질병관리청은 자신의 개인키를 통해 암호화한 서명값과 앱 이용자의 접종 사실에 대한 자격증명(VC: Verifiable Credential)*을 함께 묶어서 앱 사용자의 공개키를 통해 암호화한 후 앱 이용자에게 제공하고, 동시에 DID문서 내에 질병관리청의 공개키와 신원인증을 요청한 앱 사용자의 DID를 넣어서 블록 위에 공개적으로 저장**

* 발급기관에서 발급 요청한 앱 사용자에게 발급하는 신원인증 데이터로 물리적 증명서와 같은 역할을 수행하며, 백신 접종 관련 증명서를 예로 들면 龥.07.03., 서울 ○○이비인후과 병원, 3차, 화이자, 질병관리청 발급, 2023.07.02.에 만료"등의 신원정보가 포함

○ 이를 수령한 앱 사용자는 본인의 개인키를 이용해 자격증명(VC)을 복호화시킨 후 전자지갑 내에 저장

▨ **인증기관이 자격증명을 요청하면 앱 사용자는 자격증명 중 필요한 부분만을 추린 자격제출(VP: Verifiable Presentation)*을 자신의 개인키로 암호화한 서명값과 함께 제3기관의 공개키를 이용해 암호화한 후 전달함과 동시에, 블록 위에 저장된 DID문서 내에 앱 사용자 자신의 공개키를 추가함**

* 신원인증을 하려는 당사자가 인증 요구 기관에게 전달하는 신원인증 데이터로, "2022.07.03.,3차, 화이자"처럼 필요 부분만을 추출한 정보

○ 인증기관은 수령한 암호값(자격증명 중 필요한 부분, 질병관리청 서명값과 앱 이용자 서명값)을 자신의 개인키로 복호화 후, 서명값 부분은 앱 사용자의 DID를 통해 공개된 블록 위 DID문서를 찾아 그 안에 저장된 질병관리청과 앱 사용자의 공개키를 통해 진위를 검증

○ 자격증명은 발급을 요청한 앱 사용자 내지 인증기관에게 넘겨질 뿐, 앱 제공자나 기타 제3자에게 노출되지 않아 유출 위험이 낮음

▨ **또한 블록체인에는 자격 증명이 발급된 사실(VC 발급정보)이 해시 암호화된 후 블록 위에 공개적으로 저장**

○ 제3기관은 블록체인 내 VC 발급정보(해시값)와 수령한 발급 정보를 통해 추측한 값을 대조하는 방법을 통해 접종증명서 발급 사실의 진위 여부를 확인

2. (블록체인 기반의 분산신원인증 서비스) 암호화 정보

▨ **(개인키, 서명값, VC, VP) 발급 당사자가 직접 관리하거나 당사자가 열람을 허용한 자에게만 이전될 뿐, 블록 위에 저장되지 않음**

○ 개인키는 발급 당사자만이 보관 내지 관리할 수 있는 암호화 정보로, 제3자가 합법적인 방법으로는 열람할 수 없음

○ 서명값과 VC, VP는 발행기관·앱 사용자·인증기관을 이동할 뿐, 서비스 제공자가 별도로 이를 수집하거나 저장하지 않음

○ 결국 상기 암호화 정보들은 블록 위에 공개적으로 저장되지 않을 뿐만 아니라 분산신원인증 서비스 제공자가 수집 내지 처리하지 않으므로 개인정보보호법 상의 보호 대상 여부를 검토할 필요가 없음

▨ **(공개키, DID, VC발급정보) 공개 저장소인 블록 위에 암호화하여 저장하는 정보로서, 정보처리주체는 물론이고 누구나 열람이 가능**

○ 블록체인 기반의 분산신원인증 서비스에서는 DID문서 내에 공개키와 DID가 포함되고, 이는 블록 위에 저장되어 누구나 열람 가능

- 공개키(Public key) : 디지털 증명서의 유효성을 검증하는데 이용되는 값으로서, 신원인증 내지 자격증명을 발행하는 기관의 공개키나 앱 사용자의 공개키가 블록 위에 저장됨

- DID : 앱 사용자 및 발행 기관 등 각 주체의 대푯값이자 DID문서의 식별자로서 각 주체는 하나 내지 여러 개의 DID를 가지고 관련된 작업을 수행함

  * DID는 집 주소처럼 누군가의 대푯값임을 알 수 있으나 정확히 그곳에 누구의 정보가 있는지까지 확인하려면 공개키를 활용한 신원인증 내용의 검증을 해야함

- 예를 들어 김갑동이 하나의 앱에서 백신접종증명서와 운전면허증를 각각의 DID를 부여받아 발급받는다면, 블록 위에는 ① 백신접종증명을 위한 DID문서(김갑동의 백신접종용 DID와 질병관리청의 공개키, 김갑동의 공개키가 포함)와 ② 운전면허증을 위한 DID문서(김갑동의 운전면허증용 DID와 행정안전부 내지 경찰청의 공개키, 김갑동의 공개키가 포함)가 저장

○ 자격증명(VC) 발급정보 : 자격증명(VC)을 발급시 해당 내용의 진위 확인을 위하여 유효기간, 자격증명 식별ID 등의 발급한 사실에 대한 정보를 해시암호화한 후 블록 위에 저장

▨ 블록 위에 저장된 정보는 제3자에게 공개 및 무단 이용될 수 있어 그 대상이 개인정보보호법상 개인정보인지 검토할 필요가 있으므로, 공개키·DID·자격증명(VC)발급정보를 중심으로 개인정보보호법상의 개인정보에 해당하는지를 검토

[표 1] 블록체인 기반의 분산신원인증 서비스에서의 암호화 정보 및 블록 내 저장 여부

암호화값	특 성	블록 내 공개 저장 여부
개인키	분실시 재발급이 불가하고, 개인 단말기 내에 저장하여 보관·관리함	×
공개키	개인키에 대응하여 한쌍으로 형성되는 값으로, 디지털 증명서의 유효성 검증에 활용	○
DID	신원인증 서비스에 참여하는 각 주체를 대표하는 값이자 DID문서의 식별자	○
서명값	발급 내지 전달되는 정보에 대한 발신인의 신원을 인증하기 위한 값으로, 발신자로부터 수신자에게 전달될 뿐 별도 저장되지 않음	×
자격증명(VC)	신원인증에 대한 구체적인 정보로서, 발급기관이 자격증명 당사자에게 전달	×
자격제출(VP)	신원인증 받은 정보 중 요청 기관에 제출하고자 하는 부분만을 추린 정보로, 자격증명 당사자가 요청기관에 전달	×
자격증명(VC) 발급정보	유효기간·자격증명 식별ID 등 자격증명이 발급된 사실에 대한 정보를 해시 암호화한 값으로서, 자격증명 발급의 진위를 확인하기 위해 이용됨	○

3. 개인정보보호법에 의한 개인정보 해당성 여부

▨ 공개키와 DID

○ (식별정보* 해당여부) 공개키와 DID는 알파벳과 숫자로 이뤄진 의미없는 암호화 정보에 불과하며, 그 자체로는 성명이나 주민등록번호와 같이 특정인을 식별할 수 없음

* 개인정보보호법 제2조 제1호 가목 : 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

- 앱 가입시 성명·주민번호 등의 정보를 입력하고 확인하는 과정을 거쳐 공개키와 DID를 발급하지만, 입력된 정보는 발급되는 값에 반영되지 않고 휘발됨

- 공개키와 DID는 개인정보(식별정보)에는 해당하지 않음

○ (식별가능정보* 해당여부) 공개키와 DID는 식별가능정보로서 개인정보에 해당할 여지가 있음

* 개인정보보호법 제2조 제1호 나목 : 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

* 개인정보위원회의 개인정보보호법령 및 지침·고시 해설서(2020.12.) 12,13면 : ① 다른 정보 : 해당 정보와 결합하여 특정 개인을 알아볼 수 있도록 하는 정보라면 처리하는 자가 보유하고 있거나 합법적으로 접근·입수할 수 있는 정보 모두가 다른 정보가 될 수 있음, ② 쉽게 결합 : 현재의 기술 수준이나 충분히 예견될 수 있는 기술 발전 등을 고려하여 시간이나 비용, 노력이 비합리적으로 과다하게 수반되지 않아야 함, ③ 입수가능성 : 두 개 이상의 정보를 결합하기 위해 그 결합에 필요한 다른 정보에 합법적으로 접근하여 이에 대한 지배력을 확보할 수 있어야 하며 해킹·절취(切取) 등 불법적인 방법으로 취득한 정보까지 포함한다고 볼 수 없음

- 다른 정보 : 특정 주체가 DID를 반복적으로 발급시* 그 발급패턴, 요청 처리 과정에서 노출될 수 있는 IP주소*가 이에 해당

* 분산신원인증 서비스를 제공하는 앱에 가입한 자가 하나의 대표성을 위해 여러 DID를 발급받았다면, 동일한 공개키가 포함된 여러 DID문서가 블록 위에 공개 저장됨

* 앱 이용시 네트워크 접속을 통해 서비스를 이용하므로 블록 위 저장 단계에서 IP주소가 노출

- 입수가능성 : DID 발급 패턴 및 IP주소는 블록 위에 저장되거나 저장되는 단계에서 노출되므로 '합법적 입수'요건을 충족

- 쉽게 결합 : 향후 분산신원인증 서비스의 보편화로 특정 주체가 여러 DID를 반복적으로 발급 받는다면, "공개키 + DID 발급 패턴 + IP주소"를 통해 앱 사용자의 특정이 가능해질 여지가 있음

* 가상화폐 거래의 경우 반복된 거래패턴을 기반으로 네트워크상 노출된 IP주소를 통해 할당받은 기기의 대략적인 위치정보 · 접근 가능한 인원 내지 서비스를 이용한 시간대와 같은 다른 요소를 함께 고려하면, "공개키/지갑 주소값 + 반복거래패턴[1]+ IP주소"를 통해 "해당 공개키/지갑 주소값을 가진 IP를 할당받은 누구"로 특정이 가능[2]

* 이에 반해 분산신원인증의 경우 "공개키 + DID발급패턴 + IP주소"로 주체를 특정해야 하는데, 현재 분산신원인증 서비스 활용현황에 비춰보면 DID의 발급패턴은 가상화폐 거래패턴에 비해 이용자를 특정할 단서가 미약한 상황

* 다만 향후 분산신원인증 서비스의 대중화로 DID 발급 및 이용이 보편화된다면, 이러한 단서 확보가 합리적 선상에서 가능해지고 '쉽게 결합'요건도 충족될 여지가 있음

1) 가상화폐의 경우 반복되는 가상화폐 거래 기록(트랜잭션) 횟수와 송수신자, 금액 등을 통해 맵을 그려보면 특정인의 지갑주소값을 추정해낼 수 있다. : 과학기술정보통신부 정보통신기획평가원, "블록체인의 트랙잭션 모니터링 및 분석 기술 개발 최종보고서", 2021.2.12. 70-75면)

2) 실제로 2014년 미국에서 설립된 대표적인 블록체인 데이터 추적 분석 기업인 체이널리시스(Chainalysis)는 블록체인 포렌식을 이용해 전세계 금융기관, 수사기관, 암호화폐 거래소에서 자금세탁 등 불법행위 단속을 위한 데이터와 소프트웨어를 제공하고 있으며, 2021년 2월에는 한국법인을 설립 해 국내에서도 서비스를 제공하고 있음 : 박근모 "체이널리시스, 한국 법인 설립",코인데스크코리아, 2022.03.18.자

- 공개키와 DID는 향후 분산신원인증 서비스의 보편화로 앱을 통해 다양한 신원인증 서비스가 제공된다면, 개인정보(식별가능정보)에 해당될 가능성이 있음

○ (가명정보* 해당여부) 블록체인 내 암호화 기술은 개인정보보호법상의 비식별조치로서의 가명처리가 아니므로, 공개키와 DID는 가명정보에 해당하지 않음

* 개인정보보호법 제2조 제1의2호 : "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것

* 개인정보보호법 제2조 제1호 다목 : 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용 · 결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

* 개인정보위원회의 개인정보보호법령 및 지침·고시 해설서(2020.12.) 13면 : ① 추가정보 : 가명처리 과정에서 개인정보의 전부 또는 일부를 대체하는데 이용된 수단이나 방식(알고리즘 등), 가명정보와의 비교 · 대조 등을 통해 삭제 또는 대체된 개인정보 부분을 복원할 수 있는 정보/ 가명처리 과정에서 생성 · 사용된 정보로 제한됨 / 해당 정보를 가명처리 전 정보로 되돌릴 수 있는 정보(복원(復元)할 수 있는 정보)

* 개인정보위원회의 개인정보보호법령 및 지침·고시 해설서(2020.12.) 14면 : 처리 결과 해당 정보만으로는 특정 개인을 알아볼 수 없어야 제대로 된 가명처리가 이루어졌다고 볼 수 있다. 즉, 성명이나 주민등록번호, 주소 중 일부를 삭제하고 휴대 전화번호와 전자우편주소는 다른 정보로 대체하였으나 해당 정보를 통해 특정 개인을 알아볼 수 있다면 가명처리가 제대로 이루어졌다고 볼 수 없다.

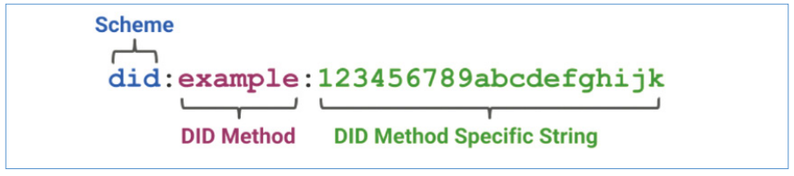
- 개인키의 공개키로의 암호화*는 개인키를 '전부 대체하는 작업'에 해당하지만,개인키는 알파벳과 숫자로 이뤄진 임의의 값으로서 이미 특정 개인에 대한 것임을 알아볼 수 없어 '개인정보'가 아니므로, 개인정보보호법 제2조 제1의2호상의 가명처리 대상에 해당하지 않음

* 개인키를 타원곡선암호(ECC: Elliptic Curve Cryptography) 방식을 통해 전부 다른 값으로 대체하고, 이를 통해 얻어진 값은 인코딩을 통해 혼동가능성이 있는 문자나 숫자를 제거함

- DID의 생성*은 아래의 표준 형식에 따라 생성되는 값일 뿐, 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 가명처리된 정보가 아님

* W3C이 승인한 DID는 "DID Scheme + Method + Method-Specific Identifier"로 구성되며, 그 의미는 "DID임을 나타내며 항상 did로 시작 + DID의 저장방법(분산원장이나 네트워크) + DID가 저장된 실제 주소"임

[그림 11] DID example



- 가사 공개키와 DID를 가명처리한 값이라고 보더라도 그 과정에서 생성 내지 사용된 정보(추가정보)는 타원곡선암호 연산과 인코딩 함수 등에 불과하여, 이를 통하여 특정인에 대한 정보로 재식별하는 것 또한 곤란함

▨ 자격증명(VC) 발급정보

○ (식별정보 해당여부) 자격증명이 검증기관에 의해 이뤄졌다는 진위 확인을 위해 발급 정보를 해시암호화한 값으로, 그 자체로는 성명이나 주민등록번호와 같이 특정인을 식별할 수 없음

- 자격증명 발급정보는 개인정보(식별정보)에 해당하지 않음

○ (식별가능정보 해당여부) 자격증명 발급정보는 다른 정보와의 결합을 통해 식별가능한 개인정보에 해당하지 않음

- 자격증명 발급정보는 해싱값이므로 추측값을 통해 확인 대상값이 원본과 동일한지만 확인할 수 있고, 블록 위 앱 이용자의 공개키·DID 등을 다른 정보로 이용하여 원래 정보로 복원(복호화)은 불가

- 자격증명 발급정보는 해싱암호값으로 특정인이 반복적으로 발급한 정보인지를 판단하기 곤란하고, 앱 서비스 이용과정에서 IP주소가 노출될 수 있으나 해당 정보를 해싱암호값에 결합하는 것만으로는 특정 개인을 식별하기 곤란

○ (가명정보 해당여부) 자격검증 발급정보는 개인정보보호법상의 가명정보에 해당하지 않음

- 해시암호값*은 자격증명 발급정보를 해시함수에 입력하면 출력되는 값으로 '전부 대체 작업'에 해당

- 해시암호화 과정에서 생성·사용된 정보로서 해시암호화 구현을 위해 사용된 프로그램의 함수 라이브러리 내의 데이터 세트를 '추가 정보'로 볼 수 있음

- 다만 이 경우 해시함수 내 데이터 세트를 통해 추측한 값과 해싱값의 비교함으로써 자격증명 발급정보의 진위 여부만 판별할 수 있을 뿐, 이를 추가정보로 결합하여 특정 개인을 식별할 수는 없음

- 따라서 개인정보보호법 제2조 제1호 다목의 개인정보(가명정보)에 해당하지 않음

○ (익명정보 해당여부) 향후 기술 발전에 따라서 추가정보의 결합 등의 방법으로 재식별 될 여지가 있는 만큼 익명정보로 단정하지 말고, 개인정보가 될 수 있는 가능성을 열어두고 지속적으로 검토할 필요가 있음

V 시사점

▨ 최근 COOV·모바일 운전면허증 등 블록체인 기반의 분산신원인증 서비스가 보급및 활용되는 추세

○ 분산신원인증(DID)은 자기주권 신원 모델(SSI)을 실현할 수 있는 기술

○ (자기주권 신원모델,SSI) 개인정보주체가 신원정보에 대한 통제권을 갖는 모델

○ (분산신원인증,DID) 탈중앙화 신원증명으로 중앙관리자에 의해 통제되지 않으면서 개개인이 자신의 정보에 대해 완전한 통제권을 갖는 기술*

* 개인정보주체가 자신의 신원정보를 스스로 보관 및 활용하되, 개인정보 주체로부터 신원정보를 전달받은 요청기관은 블록 위에 공개적으로 저장된 신원정보 관련 매개값을 통해 해당 정보의 신뢰도를 확인

○ 탈중앙화 구조 측면에서 블록체인의 기술 사상과 유사해 블록체인 기반으로 분산신원인증 서비스를 구현하는 것으로 보임

▨ 블록체인 기반의 분산신원인증 서비스에서 신원정보 관련 값들이 개인정보보호법상의 개인정보에 해당하는지 검토가 필요

○ 신원정보에는 성명·나이·자격취득여부 등 특정인을 식별하거나 식별할 수 있는 정보가 포함

○ 다만 분산신원인증 서비스의 경우, 신원인증자가 자신의 신원정보를 스스로 보관·관리하므로 정보 주체의 의사에 반하여 신원정보가 활용될 여지가 적음

○ 또한 블록체인 기반으로 구현되어 블록 위에 공개 저장되는 신원정보 관련 매개값들은 임의의 대푯값이나 암호화된 값들로 본래 내용을 알아보기가 곤란해 개인정보보호법의 보호대상(개인정보)인지가 모호

○ 블록체인 기반의 분산신원인증 관련 사업자들이 개인정보보호법상 수범자인지검토하기 위해서는 분산신원인증 서비스에서 블록 위에 저장되는 정보들이 개인정보보호법상 개인정보인지에 대한 검토가 선행되어야 함

▨ DID문서 내의 공개키와 DID, 자격증명(VC) 발급정보가 블록 위에 저장되고 누구나 열람가능하므로, 해당 정보를 중심으로 개인정보해당성을 검토

- 블록체인 기반의 분산신원인증 서비스에서 생성되는 신원정보 관련값은 개인키·공개키·DID·서명값·VC·VP·VC발급정보가 있음

- 그 중 블록 위에 저장되는 DID문서 내의 공개키와 DID·VC 발급정보는 해당 정보주체의 의사와 무관하게 누구나 열람이 가능해, 개인정보에 해당시 개인정보주체의 사전동의를 얻어 수집·이용·제공해야 하는 개인정보보호법상 규정에 반할 여지가 있음

- 따라서 DID문서 내의 공개키와 DID·VC 발급정보가 개인정보보호법상 보호대상인 개인정보인지 검토

▨ 검토 결과에 따르면 자격증명(VC) 발급정보는 개인정보보호법상의 개인정보가 아니고, DID와 공개키는 가명정보는 아니지만 식별가능정보가 될 여지가 있음

○ DID문서 내의 DID와 공개키

- DID와 공개키는 성명이나 주민번호처럼 특정인을 식별하는 식별정보가 아님

- DID는 표준 형식에 따라 생성되는 값이고 공개키는 개인키를 암호화한 값으로, 둘 다 가명처리된 가명정보가 아님

- 다만 분산신원인증 서비스가 보편화되고 포렌식 기술이 발전하면 DID 발급 패턴 및 IP주소(다른 정보)를 공개키와 결합함으로써 특정인을 식별하게 될 여지가 있어 식별가능정보로서의 가능성을 열어두고 검토할 필요가 있음

○ 자격증명 발급정보

- 자격증명 발급정보는 해시암호값으로 그 자체로는 성명이나 주민등록번호와 같이 특정인을 식별할 수 없어 식별정보가 아님

- 해싱값인 자격검증 발급정보는 블록 위 앱 이용자의 공개키·DID·IP주소를 다른 정보로 이용하여 원래 정보로 복원(복호화)도 불가하므로, 식별가능정보가 아님

- 자격증명 발급정보는 해시함수 내 데이터 세트를 이용하여 추측한 값과 비교를 통해 진위 여부만 판별할 수 있을 뿐, 이를 추가정보로 결합하여 특정 개인을 식별할 수는 없으므로 가명정보도 아님

▨ 다만 개인정보 해당성이 없다고 하더라도 익명정보라고 단정하기 보다는, 향후 기술발전 흐름에 따라 개인정보가 될 수 있는 가능성을 열어두고 지속적으로 검토할 필요가 있음

▨ 향후 등장하게 될 블록체인 기반의 서비스에서도 관련 내용을 검토함으로써 이해관계자들에게 법적인 예측가능성을 확보해주는 노력이 필요함

참고 문헌

1. 국내문헌

• 이대희, “블록체인 기술과 개인정보 쟁점”, 「정보법학」 제22권 제3호, 2018.

• 이대희, “블록체인 기술의 제도권 진입 동향에 관한 고찰 -암호화폐를 기준으로-”, 「경영법률」 제29권 제2호, 2019.

• 정진명, “블록체인 기술과 개인정보 보호의 법률문제”, 「법조」 제68권 제2호, 2019.

• 박민정, 채상미, 이명준, “개인정보보호법제 관점에서 본 블록체인의 법적 쟁점 GDPR 및 국내 개인정보보호법을 바탕으로”, 「한국정보기술응용학회」 제25권 제2호, 2018.

• 손태진, “개정 개인정보보호법에서 블록체인 관련 정보의 개인정보 여부”, 「정보과 학회지」, 제38권 제7호, 2020.

• 김선남, “블록체인 기술 활성화를 위한 법정책적 연구”, 「단국대학교 IT법학 박사 학위논문」 2020.

• 김현경, “블록체인과 개인정보 규제 합리화 방안 검토”, 「법학논집」 제23권 제1호, 2018.

• 신지혜, “블록체인의 성립과 운용에 있어서 민사법적 쟁점 - 블록체인에 대한 기술 적 이해를 기초로 -”, 「비교사법」 제28권 제3호, 2021.

• 이영은, 김혜원, 이명준, “FinDID : 금융 분산ID 표준을 지원하는 DID 서비스”, 「컴 퓨터정보학회」 제27권 제5호, 2022.

• 전승재, “개인정보, 가명정보 및 마이데이터의 활용 범위-데이터 3법을 중심으로”, 「선진상사법률연구」 제91호, 2020.