블록체인 기술을 활용한 전자신원인증 방법에 관한 연구

지도교수 : 한 상 훈
연 구 자 : 서 보 성

< 목 차 >

요 약

기술의 발전으로 인해 많은 작업들을 온라인에서 할 수 있게 되었고 그로 인하여 디지털 신원증명에 대한 중요성이 높아졌다. 가장 대표적인 방법으로 공인인증서가 있지만 많은 문제점을 가지고 있고 그로 인해 새로운 대체 방법의 필요성이 높아졌다. 본 논문에서는 블록체인 기술을 활용한 디지털 신원증명 대체 방법을 제안한다.

주요어 : 블록체인, 전자인증, 인증서, 네트워크. 트랜잭션

1. 서론

1.1 배경 및 목적

공인인증서는 가장 전통적이며 오랫동안 사용되어 왔던 디지털 신원증명 방법 중의 하나이다. 대표적으로 인터넷의 발전에 따른 온라인 뱅킹 같은 금융 업무에 사용되며 이 뿐만 아니라 정부에서 제공하는 전자민원, 전자정부 업무 등 공공기관 관련 서비스에도 사용된다. 공인인증서의 첫 취지는 온라인상에서 주민등록번호 사용으로 인한 유출을 막기 위해 이를 대체하는 서비스로 사용되었지만 시간이 지남에 따라 많은 보안 위협과 불편함을 동반해 왔다. 그렇기에 지난 2020년 5월 통과된 전자서명법 개정안에 따라 공인인증서와 사설인증서를 구별하는 제도가 폐지되어 일정 평가기준을 충족한 민간 기업이 전자서명 사업자로 활동이 가능하게 되었고 그 결과물로 '패스', '카카오', '네이버' 등 여러 민간 기업들이 전자서명 서비스를 선보였고 금융권에서는 공인인증서의 명칭을 '공동인증서'로 바꾸어 서비스를 하기 시작했다. 이처럼 민간기업도 조건을 갖추면 인증사업에 참여 할 수 있게 됨으로 인해 여러 서비스들 간의 경쟁으로 새로운 인증기술의 등장이 기대되고 있다.[1]

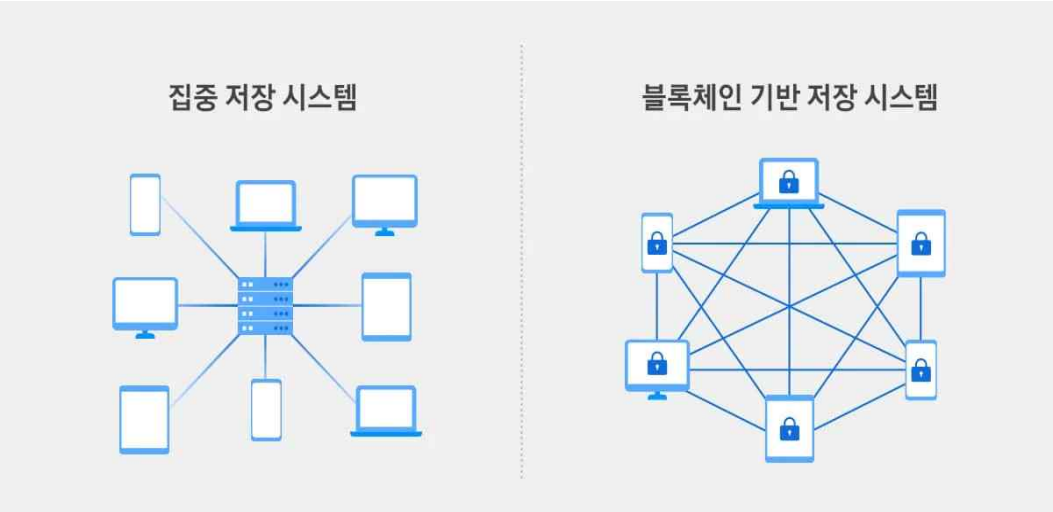
본 연구는 현재 많은 논란과 관심을 받고 있는 비트코인의 배경 기술인 블록체인과 그 특성을 활용해 새로운 디지털 신원증명 방법을 제시한다. 현재는 신원증명 서비스를 이용할시 사용자의 정보가 해당 서비스를 제공하는 기업의 중앙시스템에 의해 통제되며 관리된다. 이렇게 사용자의 모든 정보가 중앙에 집중되어 통제될 경우 개인정보 유출사고 등이 발생 할 수 있고, 그 경우 매우 큰 피해를 입을 수밖에 없는 구조가 발생된다.[1] 이러한 문제점을 해결하기 위해 블록체인을 통해 새로운 방식의 디지털 신원증명 방법을 제안한다.

2. 관련연구

블록체인 기술을 활용한 전자신원인증 방법에 대한 연구를 진행하기 위해선 선행적으로 우선 블록체인 기술 그 자체에 대한 지식과 현재 사용되고 있는 인증방법들에 대해 알아야 하기에 이를 알아보고자 한다.

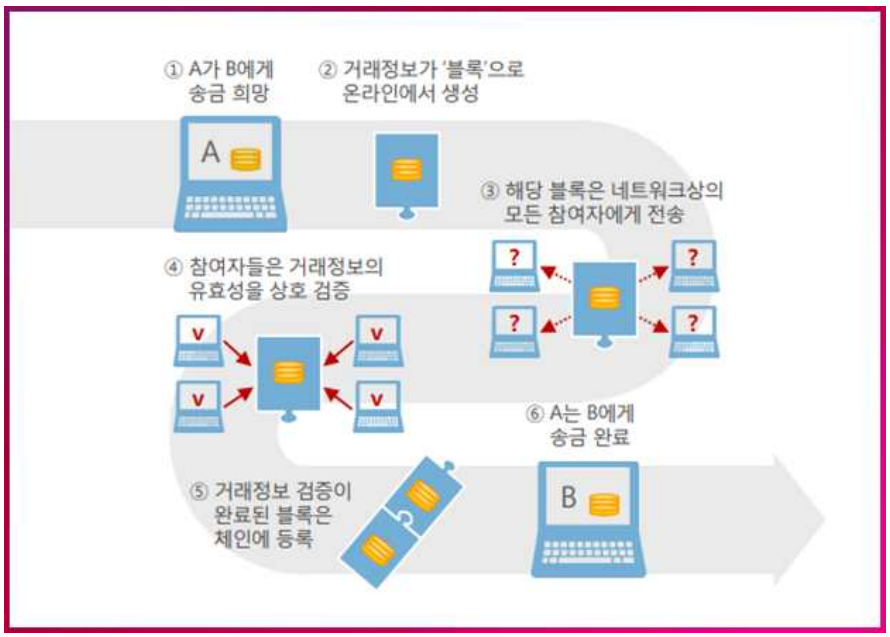
2.1 블록체인

블록체인은 데이터 분산 처리기술을 의미한다. P2P(Peer-to-Peer) 방식을 기반으로 하여 블록체인 네트워크에 참여한 모든 참여자의 데이터를 분산, 저장하여 누구도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있게끔 만들어 무결성을 보장한다.[2]



[사진 1] 블록체인 기반 저장 시스템 예시

이게 가능한 이유는 트랜잭션, 즉 거래가 발생할 때 해시 함수를 적용하고 생성된 해시 값을 거래 참여자 사이에서 이루어진 거래 정보를 저장한 단위인 '블록'에 저장하고, 추가로 생성한 해시 값은 다음 블록에 저장하여 이전 해시 값이 저장된 블록과 연결 지어 체인을 형성한다.[2] 이 때문에 하나의 거래정보, 즉 블록의 정보가 변경되면 연달아 체인으로 연결된 뒤의 블록에 저장된 해시 값들이 모두 변경되어 정보의 조작이 어렵기 때문에 무결성이 유지되고 블록에 블록을 연결 지어 체인을 형성하기 때문에 블록체인이란 이름으로 이 기술이 불리게 되었다.



[사진 2] 블록체인 기반 트랜잭션 처리 예시

2.1.1 특성 및 핵심 기술

블록체인의 가장 중요한 기술적 특성인 탈 중앙성은 기존의 중앙 집중식 엔터티에서 분산 네트워크로 제어 및 의사 결정을 이전하는 것을 의미하며 이에 따라 거래 기록이 담긴 원장을 은행과 같은 제 삼자에 맡기지 않고 블록체인 네트워크에 참여하고 있는 참여자들이 직접 검증과 승인, 합의 등의 활동을 통하여 만들고 관리한다. 이를 인하여 새로운 블록이 만들어질 때마다 참여자들에게 모두 전송되어 공유되기 때문에 투명성이 지원되며 이때 참여자들의 실명은 알 수 없기에 익명성도 유지된다. 또한 블록체인은 데이터 분산처리 기술이기에 블록체인의 데이터는 모든 참여자의 노드에 분산 저장되고 그렇기에 만약 그 중 어느 하나가 문제를 일으키더라도 전체 시스템은 유지되며 중단되지 않는다.[2] 이러한 특성이 존재하게 해주는 데는 P2P 네트워크, 암호화, 분산장부, 분산합의라는 4개의 핵심 기반 기술이 존재하기에 가능하다.[3]

기술	정의
P2P 네트워크	기존 클라이언트 서버 방식에서 탈피한 동등한 계층의 참여자들로 이루어지는 네트워크
암호화	블록체인에서는 데이터의 무결성 검증을 위한 머클 트리(Merkle Tree)와 거래의 부인방지를 위한 공개키 기반 디지털 서명기법 사용
분산 장부	블록체인 네트워크 참여자들 간의 합의에 의해 복제되고 공유, 동기화된 정보의 기록 저장소
분산 합의	분산 컴퓨팅과 멀티 에이전트 시스템 등의 분야에서 결함이 있는 프로세스가 있는 경우, 전반적인 시스템의 신뢰성을 달성하기 위해 프로세스나 에이전트 간의 특정 데이터 값에 의한 동의를 이끌어내는 프로토콜

[표 1] 블록체인 핵심기술

2.1.2 유형

1. 퍼블릭 블록체인 네트워크

퍼블릭(Public)의 뜻인 공공의에 걸맞게, 일반 대중들이 자유롭게 참여할 수 있는 형태의 네트워크를 말하며 어떠한 조직의 승인절차 없이 누구든지 다양한 컴퓨터 장비를 이용하여 참여 가능하다. 이러한 네트워크에 참여하는 개별 컴퓨터를 노드라고 부르고 이 노드들은 각 블록체인에 저장된 데이터를 복사하여 저장하고, 위에서 설명한 트랜잭션 발생 시 일어나는 해시 연산을 통해 새로운 블록의 생성에도 참여할 수 있다. 퍼블릭 블록체인 같은 경우는 블록체인 기술을 기반으로 탄생한 비트코인과 매우 밀접한 연관을 가지고 있는데 블록

체인이 계속해서 생성되기 위해 신뢰할 수 있는 노드에 의해 검증되는 단계를 반드시 거쳐야 하는데 이 노드들이 일한 대가를 보상하기 위해 내부 화폐, 즉 코인이 발행되어 지급된다.

2. 프라이빗 블록체인 네트워크

프라이빗(Private)은 퍼블릭 블록체인과 반대되는 개념이다. 제한 없이 일반 대중들이 자유롭게 참여가 가능했던 퍼블릭 블록체인과는 달리 허락된 소수의 사람들만 참여할 수 있도록 설정된 개방되지 않은 블록체인이다. 퍼블릭 블록체인 같은 경우는 모두가 제한 없이 자유롭게 참여할 수 있고 또 블록체인의 특성상 트랜잭션이 발생하여 노드가 생성될시 모든 참여자에게 전송되어 공유가 되기 때문에 보안을 중요한 은행이나 공공기관 등에서 많이 사용한다. 특정 사람들만 참여가 가능하기에 소수의 노드만이 운영되어 저렴하고 빠른 거래 처리 속도를 장점으로 가진다.

3. 하이브리드 블록체인 네트워크

사실 퍼블릭과 프라이빗 블록체인 네트워크 같은 경우는 그 성질과 장/단점이 매우 극명하다. 그렇기에 이러한 한계를 보완하기 위해 개발된 것이 하이브리드 블록체인 네트워크이며 퍼블릭 블록체인의 보안성, 투명성, 불변성, 탈중앙화 등의 중요 기능을 제공하면서, 거래 내용 접근이나 공개 및 거래 변경에 대해선 제한할 수 있는 기능을 가진다.

4. 컨소시엄 블록체인 네트워크

컨소시엄은 하나의 집단이란 뜻을 가지고 있고 그에 걸맞게, 여러 기관 또는 기업이 하나의 그룹을 이뤄 블록체인 네트워크를 구성하는 구조를 가지고 있다. 하이브리드 블록체인과 비슷하게 퍼블릭과 프라이빗 블록체인의 성격 모두 가지고 있으며 합의 과정에는 선별된 한 집단의 노드들만이 참여할 수 있지만, 그 외 노드들은 거래를 생성하거나 확인이 가능하다.

2.2 인증서

인터넷이 보편화 되고 발전함에 따라 인터넷 뱅킹, 인터넷 쇼핑, 전자정부 시스템 등 여러 가지 편리한 시스템들을 사용할 때 본인인증에 대한 필요성이 증가하게 되자 온라인 상에서의 주민등록번호 노출을 최소화 하기 위해 그걸 대체하기 위한 방법으로 인증서, 대표적으로 공인 인증서가 제안되었다. 하지만 ActiveX 기술을 필수요소로 사용하며 이 때문에 초기에는 오직 윈도우즈 OS의 IE를 제외하고는 인증이 불가능 하다는 단점을 가지고 있었고 이 외에도 안정성, 접근성 및 보안을 위해 제안되었지만 보안성이 떨어진다는 여러 문제점에 따라 결국 2020년 5월 개정된 전자서명법에 의해 폐지가 결정되었고 그 결과 공인인증서 뿐만이 아닌 여러 가지 인증서 서비스가 탄생하게 되는 계기가 되었다.

2.2.1 유형

종류	설명
공인인증서	-인터넷 상의 주민등록증, 온라인 인감증명서 -공동인증서로 명칭 변경(2020-12-10)
공동인증서	-공인인증서의 변경된 이름 -1년 유효기간
금융인증서	-발급시 휴대용 저장매체가 아닌 클라우드에 저장 -모든 은행에서 사용 가능 -3년 유효기간
은행 발급 인증서	-발급받은 은행에서만 사용가능
네이버인증서	-제휴된 경우에 사용가능 -3년 유효기간
카카오페이인증서	-제휴된 경우 사용가능 -2년 유효기간
PASS인증서	-제휴된 경우 사용가능 -3년 유효기간
KB모바일인증서	-제휴된 경우 사용가능 -유효기간 없음
사설인증서	-행안부 공공분야 전자서명 사업자로 선정된 업체에서 발급한 인증서 -공동인증서, 금융인증서를 제외한 대부분의 인증서가 포함됨
간편인증	-사설인증서를 통한 인증

[표 2] 인증서 유형

이렇듯 여러 가지 유형의 인증서들이 존재하고 위의 공인인증서외의 모든 인증서들은 2020년 5월 개정된 전자서명법 이후에 등장하여 서비스 되고 있는 방식들이다.

2.2.2 인증서 문제점

위에서 소개된 여러 가지 방식의 인증서들은 모두 하나 둘씩 문제점을 포함하고 있다. 우선 가장 보편적으로 사용되었던 공인인증서 같은 경우는 불편한 사용성 및 접근성, 특정 운영체제에서만 동작하게 되는 기술구성, 인증서가 저장되는 저장 매체가 제한이 되지 않아 개인용 컴퓨터 또는 이동식 메모리 등 다양한 장치에 저장 및 복사가 가능해 해킹에 따른 유출이나 분실의 위험이 커 취약한 보안 등 여러 문제점을 가지고 있어 폐지되었다.

그 후 등장한 여러 가지 사설 인증서들 같은 경우는 이러한 문제점들을 해결하기 위해 인증서가 직접적으로 사용자가 가지고 있는 매체에 저장되는 것이 아닌 서비스 제공자가 관리하는 클라우드에 저장되는 방식, 접근 및 사용 편의성, 다양한 OS에서의 지원등 많은 부분에 있어서 개선이 이루어졌지만 인증이 필요한 경우 법으로 이러한 공인인증서(현: 공동인증서), 금융인증서를 제외하고 사설인증서또한 지원해야 하도록 명시되지 않았기에 이러한 사설인증서 제공업체와 제휴된 곳에서만 사용이 가능하다는 단점을 가지고 있다.

3. 제안기법

본 논문의 메인 아이디어인 블록체인 기술을 활용한 전자인증방법에 대해 알아보기 전에 현재 블록체인 기술이 활용된 사례에 대해 알아보고자 한다.

3.1 블록체인을 이용한 인증 활용예시

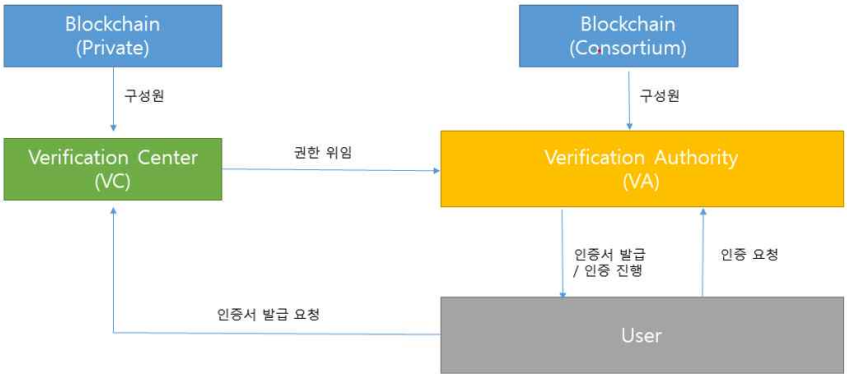
1. COOV 앱

코로나19가 매우 심할 당시 정부는 백신 접종에 대한 증명을 확인하기 위해 접종증명서가 발급 저장되어 확인이 가능하고 QR코드를 이용하여 출입 증명을 할 수 있는 앱인 COOV 앱을 개발하여 배포하였다. 다른 모바일 서비스 업체인 카카오, 네이버 등에서도 이러한 기능들을 제공하였지만 COOV 앱을 이러한 앱들과 다르게 만들었던 점은 1. 정부에서 제공하는 공식 앱이며, 2. 별도의 인증서 발급과 정보 제3자 제공 동의 등이 필요 없었으며, 3. 빠르고 간편하며, 마지막으로 블록체인 기반 시스템이었다는 것이다. 블록체인 기술을 이용하여 증명서의 위변조를 불가능 하게 하였으며 탈중앙화를 통해 사용이력이 서버에 남지 않도록 하여 프라이버시도 보호가 가능하게 설계되었다. 이렇듯 COOV 앱은 블록체인 기술을 활용하여 증명 및 인증이 가능하다는 것을 공식적으로 보여준 활용예시 중 하나이다.

2. NFT 기술을 통한 인증서

NFT란 대체 불가능 토큰을 뜻하며 블록체인 기술을 이용하여 디지털 자산의 소유주를 증명하는 가상의 토큰이다. 이 NFT 기술을 이용하여 명품에 대한 보증서를 발행하거나 학위증, 졸업장등 공식문서를 발급하기도 한다. 실제로 성균관대에서 공모전을 통한 상장 수여에 이 NFT 기술을 사용하기도 했고 호서대학교 같은 경우는 졸업생들에게 NFT 학위증과 상장을 발급하기도 하였다. 이렇게 발급된 NFT는 개별 고유번호를 통해 위변조 및 소유권이 인증된다.

3.2 프라이빗 블록체인을 활용한 신원인증 방법



[사진 3] 블록체인을 활용한 신원증명 방법 제안

1. Private Blockchain

프라이빗 블록체인은 허락된 소수의 사람들만 참가할 수 있는 개방되지 않은 블록체인 네트워크다. 그렇기에 디지털 신원증명의 주체가 되어야 하는 정부가 해당 네트워크를 구성하여 구성원으로서 인증센터인 Verification Center를 넣는다. 이렇게 프라이빗 블록체인 네트워크가 이 기술의 시작이 됨으로서 기존 퍼블릭 블록체인의 문제점 중 하나인 모든 사람이 참가하고 이루어지는 모든 거래를 확인할 수 있기에 개인정보 같은 민감 정보에 대한 보안이 어렵다는 문제가 해결이 가능하다.

2. Verification Center(VC)

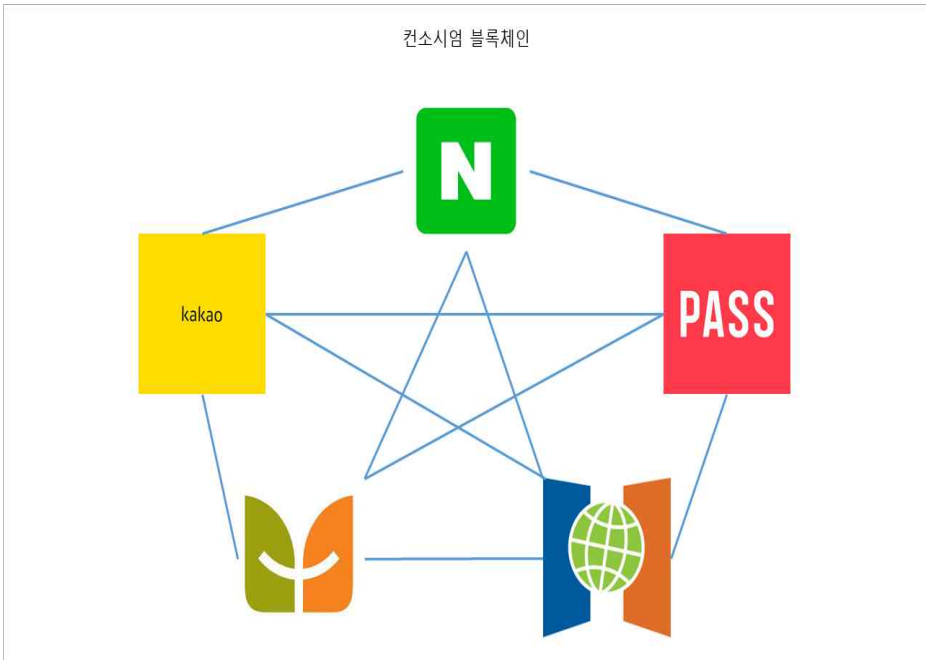
정부로부터 프라이빗 블록체인에 구성원으로서 초대받아 인증센터로서의 역할을 한다. 이 Verification Center(VC)는 과거 공인인증서부터 발급주체가 되었던 한국정보인증(KICA)가 맡는다. 이 VC는 신원인증 인증서를 직접 발급해주는 것이 아닌 신뢰할 수 있는 인증서 서비스 업체(예: 네이버, 카카오) 등에게 권한을 위임하여 인증서 발급 및 인증 확인 등이 이루어질 수 있도록 하고 이러한 작업들이 원만하게 이루어지고 보안이 유지되는지에 대한 관리감독을 한다.

3. Verification Authority(VA)

인증센터로부터 권한을 위임받아 실질적으로 인증서 발급과 인증을 진행하는 기관으로서 현재 인증서 서비스를 제공하고 있는 네이버, 카카오, KB 등 사설인증서 발급기관을 말한다.[4] 전자서명법 개정으로 인해 공인인증서가 폐지됨과 동시에 공인과 사설인증서에 대한 구분이 없어졌기에 이러한 사설인증서 서비스 제공기관들은 현재 서비스 협약이 맺어진 곳에서만 인증이 가능하다는 단점을 해결하기 위해 컨소시엄 블록체인 네트워크를 구성하여 가입하여, 어떠한 기관에서 인증서를 발급을 받던지 간에 구별 없이 인증이 가능하게 만든다.

4. User

인증서가 필요할 시 인증서 발급을 요청하여 사용자가 사용하기 편한 서비스 제공업체에서 인증서를 발급 받는다. 현재 널리 사용되는 스마트폰에 wallet 형 앱이 설치되며 인증서가 저장되며, 필요시 이 앱을 통해 사용할 수 있다. 컴퓨터에서 인증이 필요할 시 현재 보안을 위해 사용되고 있는 2단계 인증 방법처럼 등록된 핸드폰으로 앱을 통해 알림이 오고 앱에 저장된 인증서를 이용해 인증 시 컴퓨터에서도 인증이 되는 방식을 통해 컴퓨터의 운영체제와는 관계없이 사용가능 하도록 설정한다.



[사진 4] Verification Authority

위의 그림에서 볼 수 있듯이 협업을 통해 컨소시엄 블록체인 네트워크에 구성된 구성원끼리 VA로서 인증서 발급과 발급된 인증서를 통한 인증을 한다. 사실 제안된 아이디어 자체는 현재 사용되고 있는 통합인증 과정과 크게 차이가 없다. 보통 블록체인 기술을 사용하여 기술을 제안할 때는 블록체인의 가장 중요한 특징인 '탈 중앙화'를 이용하여 구성하지만 이 아이디어에서는 블록체인 기술이되 '탈 중앙화'와는 거리가 먼 프라이빗 블록체인 기술을 사용하기에 일반적인 통합인증 과정과 큰 차이를 보이지 않는다. 사실 개인정보 같은 개인정보를 다루는 경우에 퍼블릭 블록체인을 이용할 경우 그 특성상 블록체인 네트워크에 제한 없이 누구나 가입하고 이뤄지는 거래 와 그 내용들을 확인 할 수 있기에 보안에 적합하지 않다. 그렇기에 어느 정도 통제가 가능한 프라이빗 블록체인 네트워크를 사용하여 인증을 구현하는 것이다.

4. 결론 및 향후 과제

이렇듯 블록체인을 통해 전자인증을 구현함으로 운영체제에 종속적이지 않으며 보안성을 갖춘 전자인증이 완성되었다. 사실 아이디어로 제안된 형태는 현재 이루어지고 있는 인증과정과 블록체인을 이용한다는 점을 제외하고는 크게 다르지 않다. 그 이유는 가장 기본이 되는 블록체인 네트워크에 퍼블릭 블록체인 네트워크가 아닌 프라이빗 블록체인 네트워크를 사용하여 블록체인의 가장 큰 특징 중 하나인 탈중앙화와는 거리가 멀기 때문이다. 그렇기에 앞으로는 제안된 아이디어에서 좀 더 발전 시켜 탈중앙화라는 특징을 살린 블록체인 기반 인증과정이 제안될 필요성이 있다. 사실 블록체인 기술은 그 파생물인 비트코인에 의해서 많은 주목을 받은 기술 중 하나이지만 비트코인을 제외한 부분에서는 크게 활용성에 대한 두각을 기술이 가지고 있는 포텐셜에 비해서는 나타내지 못하고 있는 상황이다. 그렇기에 기술의 발전과 그를 통한 인간의 삶의 편의성 증가를 위해 전자 인증뿐만이 아닌 블록체인 기술을 활용한 여러 가지 기술과 방식이 제안되기를 바라며 본 논문을 마친다.

참고문헌

[1] 블록체인기반 모바일 신원증명 서비스의 수용의도에 영향을 미치는 요인에 관한 연구. 김지영. 국내박사학위논문 숭실대학교 대학원(2021), 1-124

[2] 블록체인 기반의 디지털 신원증명 동향. 이정현, 서화정. 2020 온라인 춘계학술발표대회 논문집 제27권 제1호 (2020. 5), 218-221

[3] 블록체인 핵심 기술과 국내외 동향. 이동영, 박지우, 이준하, 이상록, 박수용. 정보과학회지(2017. 6), 22-28

[4] 블록체인 기반 새로운 신원확인 체계. 정용훈. Journal of the Korea Academia-Industrial cooperation Society Vol. 22, No. 2(2021), 452-458

[5] 공인인증서 대체를 위한 블록체인 기반 개인인증 방안 연구. 김진석, 강정호, 전문석, 김은환. 2017년 추계학술발표대회 논문집 제24권 제2호 (2017. 11), 357-359

[6] 분산 ID 기반 모바일 학생증 구현과 활용. 조승현, 강민정, 강지윤, 이지은, 이경현. Journal of The Korea Institute of Information Security & Cryptology VOL.31, NO.6(2021. 12), 1115-1126

[7] 블록체인 기술 동향에 관한 연구. 박찬홍, 이영실. 한국융합신호처리학회논문지 Vol. 20, No. 4(2019. 12), 218~225