발표 자료 준비

1. DID

등장배경

데이터경제, 빅데이터 시대에서 데이터는 굉장히 중요하다. 그리고 이러한 데이터 시대에 개인정보에 대한 주권 즉 자신의 데이터가 어디서 어떻게 어떤 목적으로 사용될 지 스스로 결정할 수 있는 권리가 중요해지고 있다.

기존 신원인증방식의 문제점.

1.불필요한 정보 노출

->기존 신분증에는 성인 여부 외에도 이름, 주소지 주민번호 등 개인정보가 있다.

2.개인정보 관리 어려움

-> 서비스마다 회원가입. 복잡한 인증 과정을 거치고 몇몇 아이디와 비밀번호를 돌려씀.

3. 해킹 시 정보 대량의 정보 유출

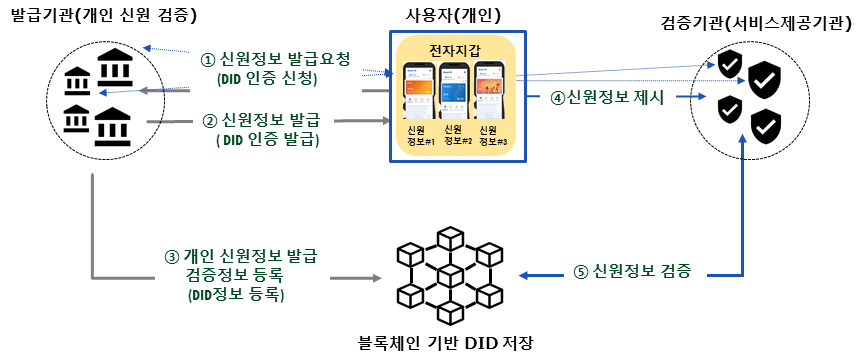
4. 내 개인정보 활용 어떻게 하는지 모름

->내 개인정보를 활용해 수익창출하면서 내 개인정보를 어떻게 사용하는지 알 수 없음.

DID(Decentralized Identifier)란 무엇인가?

DID란 주민등록증, 운전면허증 등 실생활의 신분증처럼 온라인 환경에서 정보 주체(사용자)가 직접 자신의 신원 정보를 관리, 통제하는 디지털 신원 관리 체계. 중앙화된 기관을 거치지 않으면서도 검증이 가능하여 인증이 요구되는 상황에서 다양한 방식으로 활용될 수 있도록 하는 개념

어떻게 가능한가? - 개요, 원리



① 사용자가 필요시 발급기관에게 자신의 신원정보 발급을 요청

발급기관은 신원정보 발급 요청자와 사용자가 동일인임을 검증(본인인증)

② 발급기관은 사용자의 신원을 검증 후 신원정보를 사용자에게 발급

사용자는 자신의 전자지갑에 발급받은 신원정보를 저장 및 관리

③ 발급기관은 사용자의 신원정보 발급 검증정보를 블록체인 기반 DID 저장소 등록

④ 사용자는 필요한 서비스 이용시 신원정보를 직접 검증기관(서비스 제공기관)에 제출

⑤ 검증기관(서비스 제공기관)은 DID 저장소에서 사용자의 신원을 확인

장점

크게 3가지.

1. 회원가입이나 금융서비스에서 **신원증명 절차를 간소화**한다. 사용자는 서비스를 간편하게 이용할 수 있고, 서비스 제공자는 간편한 절차 덕분에 비용 절감.
2. **신원 정보를 블록체인의 노드에 분산 저장하여 정보의 보안성을 높일 수 있다**. 중앙 DB에 저장될 경우 한번 해킹에 성공하면 많은 정보를 빼돌림. 블록체인에 저장할 경우 데이터의 위변조가 불가능하며, 분산 저장되어 있어 해킹의 유인을 낮출 수 있다.
3. **정보를 각각의 노드에 저장함으로써 개인의 프라이버시와 데이터 주권을 보호 가능.** 공증 받은 데이터를 개인이 저장하고 관리함으로써, 특정 상황에 적절한 정보만 제공하여 불필요한 정보 노출을 줄일 수 있다. 또한 누가 개인정보를 열람했는지 확인할 수 있어서 데이터 주권을 보호하고 데이터 산업의 패러다임을 바꾸는 계기가 될 것이다.

어려움 -> 피피티에 넣어야 하나? 알고는 있어야 하는데...

1.표준화 준비중. DID 시스템 간에 호환이 가능해야함. 그렇지 않으면 현재처럼 개인이 여러 정보를 관리해야함. 이는 장점을 무색하게 만듦. DID 표준을 위한 DID 얼라이언스에 대한 투자가 활발하게 이루어지고 있음. 마소는 오픈소스로 DID 개발해 표준화 시도.

2. 개인 뿐 아니라 기업에게도 중앙 시스템보다 더 큰 효용이 있어야 함. 기업은 고객 정보를 활용하고 싶어한다. DID에서는 신원정보를 개인의 노드에 저장. 기업에게 중앙 시스템보다 효용이 있어야 DID 시스템을 사용하고 결국 산업이 성장할 것이다. **기업입장에서 장점은 보안 비용을 감축하고, 절차 간소화해 소비자에게 어필 가능. 개인의 정보를 가명 처리하여 활용하는 방법도 제시할 수 있다**.

3. 개인키의 사용성을 높여야 한다. 블록체인에서 개인키 잃어버리면 복구 불가능. 중앙 시스템은 비밀번호 변경 가능한데, 블록체인 개인키는 기존 시스템에 익숙한 사람에게 불편할거고, 지갑, 개인키, 공개키, 전자서명 등 낯선 개념은 진입장벽이 될 것.

4. 개인키 보안성 또한 중요한 문제. 블록체인은 데이터 위변조를 막는다는 점에서 보안성이 높지만, 개인키를 다른 사람이 활용하거나 해킹될 경우 대해 보안이 약하다. 이에 대한 해결책으로 개인키에 사용자의 생체 정보를 활용하거나 HSM(?)의 보안성을 높이는 방법. HSM은 하드웨어 보안 모듈로 디지털 키를 안전하게 보호하고 관리하는 기능. HSM은 개인키를 암호화하고 안전하고 분리된 곳에 저장하며, 키의 사용이력을 추적하는 기능을 제공.

1. 활용사례

1. 병무청의 블록체인 기반 전자지갑 서비스 구축 사업

* 기존에 병무청 홈페이지에서 발급받던 각종 병역이행 관련 증명서와 확인서를 DID 기반으로 발급해 병무 민원을 모바일로 빠르고 안전하게 이용할 수 있도록 하는 것이 핵심
* KB은행, 중앙대학교, 군인공제회C&C 등과 연계해 군인 전용 금융상품 가입, 대학 휴·복학 신청, 군인 전용 복지 서비스 이용 시에도 오프라인으로 증명서를 제출할 필요 없이 모바일 전자지갑을 통해 비대면으로 처리 가능

2.행정안전부 모바일 운전면허증

* 신분증 사용 이력은 본인만 확인할 수 있도록 개인의 스마트폰에 저장되며, 중앙 서버에는 저장되지 않는다. 정부는 신분증 발급의 공신력은 갖되, 개인의 사용 및 검증과정에는 개입하지 않음으로써 사생활 침해 등 우려는 해소될 것으로 기대된다.

3.질병청 백신접종 증명서비스

* 질병관리청은 한국인터넷진흥원(KISA)에서 블록체인 시범사업 예비 우선협상자로 지정된 ‘SK텔레콤·라온시큐어·아이콘루프·코인플러그 컨소시엄’도 백신 접종 인증을 분산신원증명(DID)방식으로 할 수 있게 한다는 계획이어서, 이용자의 편의와 보안은 더 증대될 전망이다.

1. 아이디어

1.게임 아이디 인증

게임을 하다보면 중국인같은 외국인 또는 같은 한국인에게 게임아이디를 해킹당하는 경우가 많습니다. 그래서 현재는 OTP나 휴대폰인증, 2차 비밀번호 같이 보안을 강화하지만 OTP, 휴대폰인증 같은 경우는 게임을 할때마다 해줘야되서 번거로울 수 있습니다.

따라서 여기에 DID를 적용하면 어떨까 생각합니다. 게임아이디가 해킹당하는 이유는 게임아이디의 정보가 한곳에 모여있기 때문이라고 생각합니다. 이를 DID를 이용해 게임아이디 정보를 저장하게 된다면 간편하게 로그인 할수 있고 해킹당할 걱정도 안할 수 있을것입니다.

1.무슨 문제를 풀었나

2.그 문제가 중요?

3.어떻게 풀었나?\*\*

2.병원용 신분증.

1) 문제 : 응급환자의 접수소요시간의 비효율성

당장에 아파서 진료를 받고싶은 환자들에게 개인정보 수집시간 소요+과한 정보 수집

2)활용 :

-119대원이 있는상황: 환자 위치(GPS제공), 주소 및 전화번호, 환자 상태와 숫자, 위험요소 유무 등

파악한 정보를 천천히 정확 하게 전달해야함

=> 신속성(서류작성하는 과정)과 정확성을 높이기 위해

-최근에는 코로나 관련 질문(기침증상,종교활동,해외체류 등)이

있고 응급실에 들어갈 때 필요로하는 기본정보들이 있다.

3) 미래에는 누구나 가지고 다니는 내원신분증 겸 응급구조장치가 될 것임

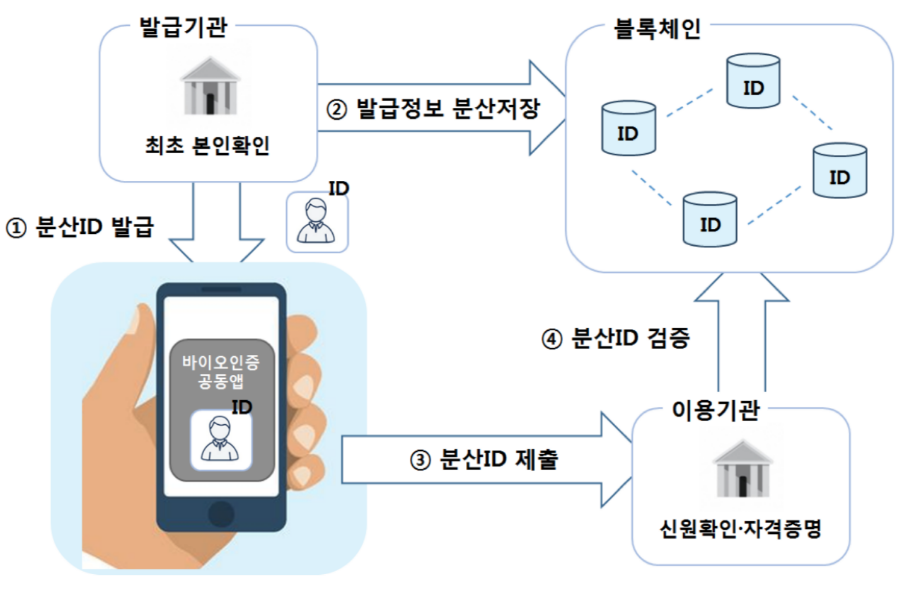
3. 대기업용 인증시스템 -> 그냥 아이디어.

대기업은 계열사가 많고. 각 계열사마다 회원정보 관리 시스템이 있다. 이를 통합하기 위해서는 비용과 시간이 많은데 DID를 사용한다면 시스템 구축에 비용과 시간을 절감할 수 있지 않을까?

발표 자료 준비 끝---------

개념

DID란 개인 정보를 사용자의 단말기에 저장해, 개인 정보 인증 시 필요한 정보만 골라서 제출하도록 해주는 전자신원증명 기술입니다. 개인들이 자신의 데이터를 직접 관리하는 구조로, 중앙화 된 기관을 거치지 않으면서도 검증이 가능하여 인증이 요구되는 상황에서 다양한 방식으로 활용할 수 있도록 하는 개념입니다.

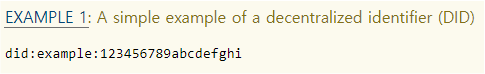


원리

1. DID의 아이디는 DID 문서의 위치를 나타냅니다.

DID의 아이디 형식

먼저 DID에서 사용하는 아이디는 아래와 같이 생겼습니다.



콜론(:)으로 구분된 세 파트로 이루어집니다.

“did” : 무조건 did로 시작하며, 이 주소가 DID 스키마를 따를 것임을 나타냅니다.

“example” : DID 메소드 이름입니다. DID는 메소드 별로 다르게 처리되며 등록된 DID 메소드는여기에서 찾아볼 수 있습니다. (비트코인, 이더리움 등등)

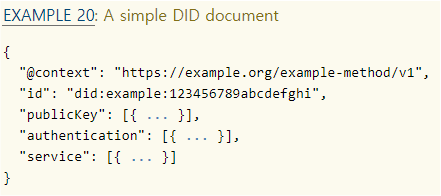
“123456789abcdefghi” : DID 메소드 안에서 사용되는 고유 아이디입니다.

DID의 아이디가 주는 가장 중요한 정보는 “DID 문서가 어디 있는지”입니다. 이 아이디와 관련된 정보는 DID 문서에 들어있습니다.

2. DID 문서에는 아이디를 인증하기 위한 정보가 들어 있습니다.

DID 문서에 담겨 있는 내용

DID 문서는 다음과 같은 형태를 띄고 있습니다. 보통 블록체인과 같은 분산원장에 저장되지만, 꼭 블록체인에 저장해야 하는 것은 아닙니다.



DID 문서에 들어 있는 정보들 다음과 같습니다. 가장 핵심이 되는 정보는 아이디의 제어권, 소유권 등을 증명할 수 있는 공개키와 인증 정보입니다.

id : 이 DID 문서가 설명하고 있는 아이디입니다.

공개키 : 이 아이디와 관련된 공개키의 리스트가 있습니다.

인증 정보 : 이 아이디의 소유권을 증명하기 위한 정보입니다. 예를 들어 “나열한 공개키 중 첫번째 공개키로 이 아이디를 인증할 수 있다”는 정보가 들어 있습니다.

서비스 : 이 아이디와 상호작용이 가능한 서비스들의 리스트를 나타냅니다.

참고로실제 DID 문서는 다음과 같이 생겼습니다.



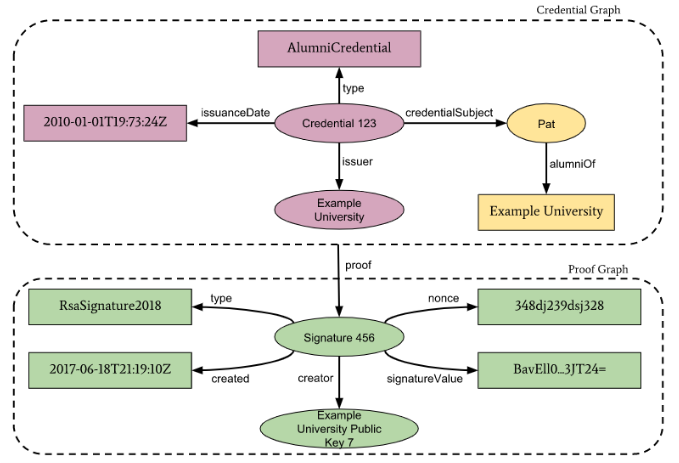
3. DID 문서는 (보통) 블록체인에 저장됩니다.

4. 개인 정보는 Verifiable Credential에 들어 있습니다.

5. Verifiable Credential은 (지갑과 같은) 안전한 곳에 저장됩니다.

6. Verifiable Credential 중 증명하고 싶은 정보만 모아 제출합니다.

DID 문서에는 신원을 증명하기 위한 개인 정보가 들어 있지 않습니다. 그렇기 때문에 블록체인과 같은 공개된 공간에 저장할 수 있습니다. 실제 신원과 관련된 정보는 Verifiable Credential(증명가능자격)에 나타나 있습니다.



Verifiable Credential 구조 예시 (https://www.w3.org/TR/vc-data-model/#credentials)

Verifiable Credential에는 크게 다음과 같은 정보가 포함됩니다.

발급자 정보 : 발급자의 아이디, 이름 등의 정보가 들어갑니다.

자격 정보들 : 신원에 대한 정보가 여기 포함됩니다. 이름, 나이, 학위 등과 같은 정보 뿐 아니라, 부모, 친구와 같은 관계 정보도 포함할 수 있습니다.

발급자 서명 (proof) : 발급 정보를 증명하기 위한 발급자의 서명입니다.

당연한 이야기지만 다양한 발급 기관으로부터 Verifiable Credential을 받을 수 있습니다. 신원 정보를 여러 개의 Verifiable Credential로 나누어 발급 받는 것도 가능합니다.

Verifiable Credential에는 개인 정보가 들어 있기 때문에 지갑과 같은 안전한 곳에 저장하거나 암호화된 형태로 저장해야 합니다.

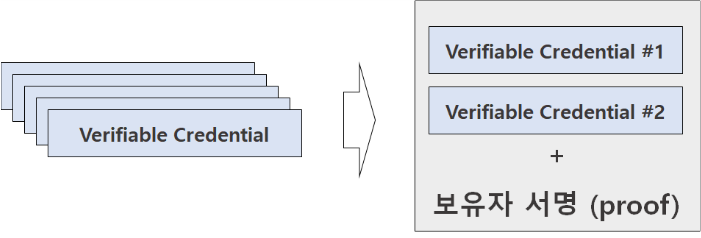
7. 모아서 제출하는 증명 정보를 Verifiable Presentation이라고 부릅니다.

Verifiable Presentation

신원을 증명할 때에는 Verifiable Credential을 직접 제출하지 않고 증명하고 싶은 정보만 모아서 제출하게 됩니다. 예를 들어 나이만 증명하고자 한다면 나이 정보가 포함된 Verifiable Credential만 제출하고 이름이나 다른 추가 정보가 들어 있는 Verifiable Credential은 제출하지 않을 수 있습니다.

즉 필요한 Verifiable Credential을 모아서 제출하게 됩니다. 이를 Verifiable Presentation이라고 합니다.

verifiable Presentation 개념



Verifiable Presentation에는 제출하는 사람의 서명이 포함됩니다. Verifiable Presentation을 받은 사람(검증자)은 제출한 사람의 서명과 Verifiable Credential의 서명을 검증하여 제출한 사람의 신원을 확인하게 됩니다.

장점

1. 회원가입이나 금융서비스에서 신원증명 절차를 간소화할 수 있습니다.

2. 신원 정보를 블록체인의 각각의 노드에 분산 저장하여 정보의 보안성을 높일 수 있습니다. 중앙 DB에 저장할 경우 한번 해킹에 성공하면 많은 정보를 빼돌릴 수 있습니다. 하지만 정보를 블록체인에 저장할 경우 데이터의 위변조가 불가능하며, 해킹의 가능성을 낮출 수 있습니다.

3. 정보를 각각의 노드에 저장함으로써 개인의 프라이버시와 데이터 주권을 보호할 수 있습니다. 공증받은 데이터를 개인이 저장하고 관리함으로써, 특정 상황에 적절한 정보만 제공하요 불필요한 정보노출을 줄일 수 있습니다. 또한 개인의 신원 정보 중에 어떤 것을 누가 열람했는지 확인할 수 있어 데이터 주권을 보호하고 데이터 산업의 패러다임을 바꾸는 계기가 될 것입니다.

단점

1. 개발하고 있는 DID 시스템 간에 호환이 가능해야 합니다.

서로 호환이 불가능하면 결국 현재의 ID와 PW처럼 개인이 여러 정보를 관리해야 할 것입니다. 이는 DID의 사용성과 장점을 무색하게 만들 것입니다. 이러한 바탕에서 DID의 표준을 만드는 DID얼라이언스에 대한 투자가 활발하게 이루어지고 있습니다. 또한 마이크로소프트사는 오픈소스로 DID를 개발하여 표준화를 시도하고 있습니다.

2. 개인 뿐만 아니라 기업에게도 회원 정보를 중앙 DB에서 관리하는 것보다 더 큰 효용이 있어야 합니다.

기업은 고객의 정보를 중앙DB에 저장하여 마케팅이나 새로운 산업에 활용하고 싶어합니다. 하지만 DID시스템에서는 신원정보를 개인의 노드에 저장합니다. 기업에게 그 이상의 효용이 있어야 DID시스템을 사용하고 DID산업이 팽창할 수 있을 것입니다. DID시스템 하에서 기업이 얻는 이익으로는 보안 비용을 감축하고 간단한 절차로 더 많은 소비자를 모집할 수 있다는 점이 있습니다.

3. 개인키의 사용성을 높여야 합니다.

블록체인 상에서는 사용자가 개인키를 분실할 경우 복구가 불가능합니다. 여태까지 PW를 분실하면 중앙 DB를 조회하거나 다시 만들어 왔던 시스템에 익숙한 사용자에게 블록체인의 개인키는 불편하게 느껴질 것입니다. 또한 지갑, 개인키, 공개키, 전자서명 등은 아직 낯선 개념이며 진입장벽을 높이기도 합니다.

또한 개인키의 보안성 역시 중요한 문제입니다. 블록체인은 데이터의 위변조를 막는다는 점에서 보안성이 높지만, 개인키를 다른 사람이 사용하거나 해킹될 경우에 대해 보안이 약합니다. 이에 대한 해결책으로는 개인키에 사용자의 생체 정보를 활용하는 방법 등이 있습니다.

4. 사용처가 확보돼야 하며 법·제도도 정비돼야 합니다.

잠재력. (미래, 보완)

DID에 대한 시각은 두 부류로 나눠진다. DID도 인증수단 중 하나로만 존재할 것이라는 부류와 단순한 인증수단을 넘어 거의 모든 곳에 쓰일 것이라고 주장하는 사람들도 있다.

1. 인증수단으로 남을것이라는 사람들은 DID가 만능은 아니며 은행이나 통신사 등 종전 소셜 로그인을 쓰지 않던 서비스들에서 비중이 높아질 것이며 구글이나 네이버 등 특정 기업이 운영하는 인증 서비스가 죽거나 점유율이 떨어지지는 않을 것이라고 생각한다.

또한 공인인증은 인증의 비중이 중요한 곳으로 옮겨갈 것이며 DID는 간편 식별 등의 영역을 차지하게 될 것이라고 주장한다.

2. DID의 활용이 거의 모든 영역에서 이용될 것이라는 의견도 있다.

이들은 DID를 단순 인증으로 보아서는 안 된다는 점과 정보의 디지털화에 주목해 DID의 확산을 예상했다.

회사 측면에서는 서비스 개발에 백엔드(사용자 데이터 관리 등)팀이 사라지게 될 것이며 개인적 차원에서는 사이트 로그인 기능이 사라지게 될 것. DID가 포괄적이고 어려운 개념이지만 반대로 적용할 수 있는 분야는 어마어마하게 넓다

개인 데이터 주권이 거대 기업에서 개인으로 자연스럽게 돌아오고 있는 상황. DID를 통해 사용자 아이덴티티를 중심으로 모든 서비스가 모일 것이고 비즈니스의 흐름을 바꿀 것으로 예상된다.

DID가 단순 인증을 넘어 데이터 주권의 문제로 확장돼 폭넓게 적용될 것이라는 주장이다.

향후 여권까지 DID를 통해 대체할 수 있을 것으로 전망된다. 다만 다른 국가들과도 연계가 필요한 부분이어서 실제 상용화까지는 시간이 걸릴 것으로 보인다. 시간이 걸리겠지만 신분증 대체는 물론이고 여권 없이도 DID를 통해 해외로 나갈 수 있는 세상이 분명히 온다. 단순 인증을 넘어 필요한 정보만 이용해 나를 증명하는 가장 확실한 시스템이 DID이기 때문

DID 업계가 성장하려면 기업이 DID만의 특·장점을 알리는 데 힘써야 한다. DID와 다른 IT 기술을 결합한 융합 서비스를 만드는 것도 DID 확산을 위한 한 가지 방법.

DID는 온라인에 특화된 기술이지만 결국 오프라인으로 사용처가 확대될 것이다. DID를 통해 모바일 신분증만 있으면 오프라인 결제와 금융 서비스를 받을 수 있는 시대가 곧 열릴 것

활용예시.

1. SK텔레콤에서 블록체인 기술과 IoT 기술을 융합한 DID(Decentralized Identifier, 분산신원확인) 서비스를 시작한다고 밝혔다. (노후건물 안전진단)

DID는 온라인에서 블록체인 기술을 기반으로 신원증명을 관리하는 전자 신분증 시스템을 일컫는 용어로, 그동안 개인의 신원 증명을 위해 이용됐는데 이번에 국내 최초로 사물의 식별자 확인에도 이용 가능하게 된 것이다.

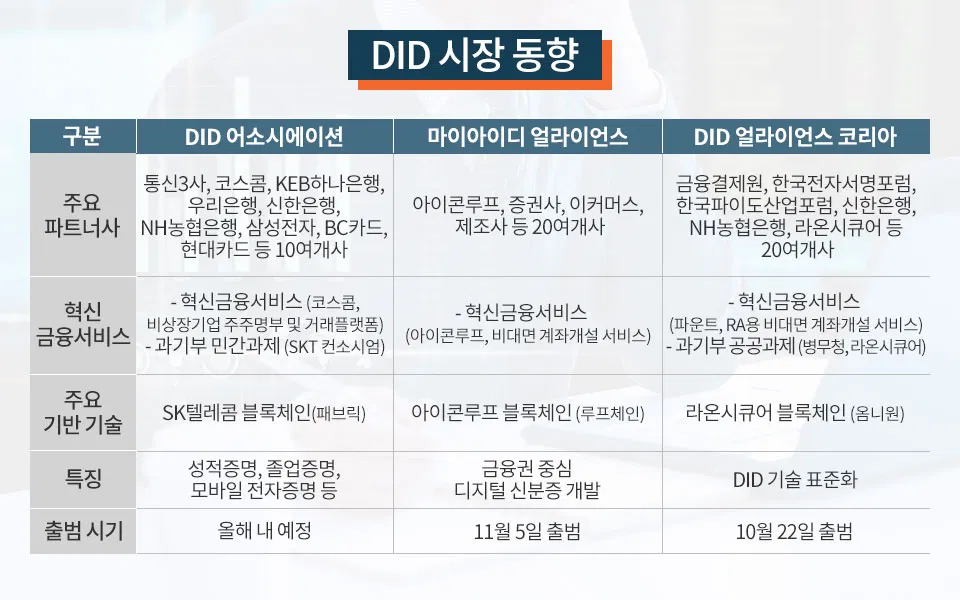
SKT의 DID 서비스는 시티랩스, 씽크제너레이터, 지노시스, 방재시험연구원으로 구성된 ‘시티랩스 컨소시엄’의 블록체인 기반 위험구조물 안전진단 플랫폼 사업에 자사의 블록체인 기반 모바일 전자증명 서비스인 ‘이니셜’을 지원한다.

특히 이니셜은 다양한 IoT 디바이스에 사물 DID를 부여할 수 있어, 블록체인을 통한 데이터 수집 및 전송 시 위·변조 위험성이 없고 진본 데이터 확인이 용이하다는 장점이 있다.

이번 사업은 한국인터넷진흥원이 2021년 블록체인 시범선도사업으로 지정한 것으로, 시티랩스 컨소시엄이 중랑구청과 함께 국내 최초로 위험구조물 안전진단 시범사업을 수행하고 있다.

SKT는 시티랩스 컨소시엄에 ‘이니셜’의 DID기술 지원을 통해 건축물의 DID 구현과 IoT기술을 기반으로 한 노후건축물의 기울기 및 크랙 모니터링을 담당한다.

2. 코인플러그가 선보인 무인 결제 솔루션 '마이키핀 무인숍 게이트는 DID와 인공지능 기술을 결합해 모바일 신분증만 있으면 누구나 무인 편의점에서 물건을 구매할 수 있는 서비스다.



1. 병무청의 블록체인 기반 전자지갑 서비스 구축 사업

* 기존에 병무청 홈페이지에서 발급받던 각종 병역이행 관련 증명서와 확인서를 DID 기반으로 발급해 병무 민원을 모바일로 빠르고 안전하게 이용할 수 있도록 하는 것이 핵심
* KB은행, 중앙대학교, 군인공제회C&C 등과 연계해 군인 전용 금융상품 가입, 대학 휴·복학 신청, 군인 전용 복지 서비스 이용 시에도 오프라인으로 증명서를 제출할 필요 없이 모바일 전자지갑을 통해 비대면으로 처리 가능

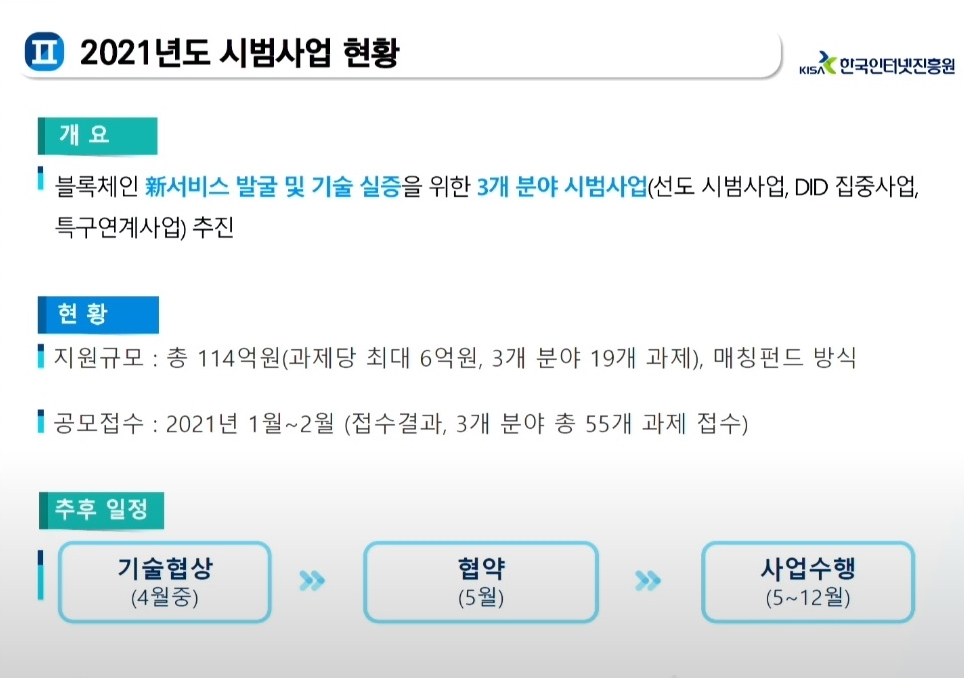
1. 행정안전부 모바일 운전면허증

* 신분증 사용 이력은 본인만 확인할 수 있도록 개인의 스마트폰에 저장되며, 중앙 서버에는 저장되지 않는다. 정부는 신분증 발급의 공신력은 갖되, 개인의 사용 및 검증과정에는 개입하지 않음으로써 사생활 침해 등 우려는 해소될 것으로 기대된다.

1. 질병청 백신접종 증명서비스

* 질병관리청은 한국인터넷진흥원(KISA)에서 블록체인 시범사업 예비 우선협상자로 지정된 ‘SK텔레콤·라온시큐어·아이콘루프·코인플러그 컨소시엄’도 백신 접종 인증을 분산신원증명(DID)방식으로 할 수 있게 한다는 계획이어서, 이용자의 편의와 보안은 더 증대될 전망이다.

참고. 2021년 시범사업 현황



활용 아이디어.

게임을 하다보면 중국인같은 외국인 또는 같은 한국인에게 게임아이디를 해킹당하는 경우가 많습니다. 그래서 현재는 OTP나 휴대폰인증, 2차 비밀번호 같이 보안을 강화하지만 OTP, 휴대폰인증 같은 경우는 게임을 할때마다 해줘야되서 번거로울 수 있습니다. 따라서 여기에 DID를 적용하면 어떨까 생각합니다. 게임아이디가 해킹당하는 이유는 게임아이디의 정보가 한곳에 모여있기 때문이라고 생각합니다. 이를 DID를 이용해 게임아이디 정보를 저장하게 된다면 간편하게 로그인 할수 있고 해킹당할 걱정도 안할 수 있을것입니다.

1. 문제 : 응급환자의 접수소요시간의 비효율성

당장에 아파서 진료를 받고싶은 환자들에게 개인정보 수집시간 소요+과한 정보 수집

2. 활용 :

-119대원이 있는상황: 환자 위치(GPS제공), 주소 및 전화번호, 환자 상태와 숫자, 위험요소 유무 등

파악한 정보를 천천히 정확 하게 전달해야함

=> 신속성(서류작성하는 과정)과 정확성을 높이기 위해

-최근에는 코로나 관련 질문(기침증상,종교활동,해외체류 등)이

있고 응급실에 들어갈 때 필요로하는 기본정보들이 있다.

3. 미래에는 누구나 가지고 다니는 내원신분증 겸 응급구조장치가 될 것임

조사 1.

DID란 무엇인가

블록체인 기반 분산 신원증명 기술

기존에는 제 3자(기업, 기관)이 개인정보 관리. 문제점 : 해킹 대상 명확. 이를 블록체인에 저장하면 해결할 수 있다. 또한 내 개인정보가 어떻게 사용되는지 알 수 없다.

또한 개개인의 자기 개인정보를 안전하게 관리하고 통제할 수 있다.

개인정보의 중요

개인정보는 중요하나 쉽게 다뤄지는 경향이 있음. 스팸 문자, 전화 같은 사생활 뿐 아니라 자산과 안전에도 위협을 당할 수 있다.

did는 그 대안.

우리가 지갑에 신분증을 넣어 다니다가 필요할 때 꺼내서 보여주는 것 처럼, 개인 블록체인 월렛(wallet, 지갑)에 내 개인정보를 담고 **필요한 한 때, 필요한 만큼만 나를 증명**하는 식이에요. 서비스 이용 관점에서 보면 사용자가 서비스 제공 기업에 **필요한 정보만 선택적으로 제공**할 수 있어요. 예를 들면 성인인증을 할 때 DID를 통해 만19세 이상인지 여부만 확인 시켜주고, 생년월일까지는 보여주지 않는 식이에요.

DID는 ‘[**블록체인**](https://blog.naver.com/markany_idea/222156224585)’으로 사용자 신원을 증명 하기 때문에 서비스 기업이나 기관에 개인정보를 모두 제공할 필요가 없어요.

(‘블록체인’이라는 단어가 나타나면 ‘1.데이터를 여러 곳에 나눠서 관리, 2.데이터를 마음대로 조작하지 못함, 3.데이터를 믿을 수 있음’ 정도로 생각해 주시면 돼요.)

기존 개인정보 관리 방식과는 다르게 개인정보 소유자인 **개인이 스스로 정보를 관리하고 통제할 수 있다는 특징**이 있어요. DID를 도입하면 개인이 특정 기관과 상호작용할 때, 신원정보 주인인 **개인이 정보 제공여부를 통제할 수 있어서 신원정보를 투명하게 관리할 수 있게 돼요.**

조사 2.

기존 신원 관련 문제점들.

기존 신분증에는 성인 여부 외에도 이름, 주소지 주민번호 등 개인정보가 있다. -> 불필요한 정보 노출

서비스마다 회원가입. 복잡한 인증 과정을 거치고 몇몇 아이디와 비밀번호를 돌려씀. -> 개인정보 관리 어려움.

그리고 서비스마다 내 개인정보를 자기의 데이터베이스에 저장하는데. 해킹당할 수도 있고. 이들이 내 회원정보를 활용해 수익을 창출하는데 내 개인정보가 어떻게 활용되는지, 어떤 수익을 내는지 모름. -> 내 개인정보를 활용해 수익창출하면서 내 개인정보를 어떻게 사용하는지 알 수 없음.

did 시스템

did란 분산 ID 시스템으로 블록체인을 적용해 중앙기관 없이 신원을 증명하는 시스템. 절차는 다음과 같다.

영희(holder)가 사이트(verifier)에 가입하려고 한다. 사이트는 영희가 실존인물인지, 믿을만한 사람인지 알고자 한다. 기존 시스템에서는 주민번호, 휴대폰 번호로 실명인증을 하고 부가적인 정보를 입력하지만 DID 시스템 에서는 영희는 사이트로 자신의 개인키로 암호화된 정보와 공개키를 보내기만 하면 된다. 사이트는 영희의 공개키로 정보를 열람하고, 해당 정보는 은행(Issuer)의 개인키로 전자서명되어 있다. 쇼핑몰은 해당 은행의 공개키를 이용해 복호화한다. 복호화 성공하면 해당 정보는 은행이 공증한 정보이니 믿을만하다. 그러면 영희는 해당 사이트의 서비스를 이용할 수 있다. Verifier가 직접 개인정보를 수집하지 않으니 전자서명을 발급하는 Issuer라는 중앙기관이 필요한다는 점에서 합의 알고리즘은 주로 PoA를 사용한다.

장점

크게 3가지.

1. 회원가입이나 금융서비스에서 **신원증명 절차를 간소화**한다. 사용자는 서비스를 간편하게 이용할 수 있고, 서비스 제공자는 간편한 절차 덕분에 비용 절감.
2. **신원 정보를 블록체인의 노드에 분산 저장하여 정보의 보안성을 높일 수 있다**. 중앙 DB에 저장될 경우 한번 해킹에 성공하면 많은 정보를 빼돌림. 블록체인에 저장할 경우 데이터의 위변조가 불가능하며, 분산 저장되어 있어 해킹의 유인을 낮출 수 있다.
3. **정보를 각각의 노드에 저장함으로써 개인의 프라이버시와 데이터 주권을 보호 가능.** 공증 받은 데이터를 개인이 저장하고 관리함으로써, 특정 상황에 적절한 정보만 제공하여 불필요한 정보 노출을 줄일 수 있다. 또한 누가 개인정보를 열람했는지 확인할 수 있어서 데이터 주권을 보호하고 데이터 산업의 패러다임을 바꾸는 계기가 될 것이다.

활용방안

1. 공익신고 제보자 보호. 공익 신고 내용에 제보자를 공증하는 Issuer가 서명을 남기는 방식. 내용이 신고되었고 제보자도 확실하지만 제보자의 신원을 확인할 수 없도록 하는 것.
2. 증명서 발급과 인증을 간소화하는 데 활용 가능.

잠재력

1. 블록체인 서비스의 촉매제가 될 것이다. 상용화 가능성이 높고 실제로 정부와 여러 기업에서 서비스 준비중. 블록체인 진입장벽을 낮추는 계기가 될 것이다. 또한 여태까지의 신원증명 서비스는 중앙화 시스템을 거치는 반쪽짜리 시스템이지만, DID 시스템이 상용화된다면 다양한 블록체인 서비스가 DID와 연계하여 발전한 것이다.
2. 국제적인 파급력이 매우 클 것이다. 표준 DID가 수립될 경우, 국경에 관계없이 단일 DID로 간편하게 신원을 인증 가능하게 될 것. 특히 기존 인프라가 낙후된 개도국에서 발전 가능성이 높음. 페이스북도 이를 노리고 리브라 개발중.

극복해야할 문제들.

1. DID 시스템 간에 호환이 가능해야함. 그렇지 않으면 현재처럼 개인이 여러 정보를 관리해야함. 이는 장점을 무색하게 만듦. DID 표준을 위한 DID 얼라이언스에 대한 투자가 활발하게 이루어지도 있음. 마소는 오픈소스로 DID 개발해 표준화 시도.
2. 개인 뿐 아니라 기업에게도 중앙 시스템보다 더 큰 효용이 있어야 함. 기업은 고객 정보를 활용하고 싶어한다. DID에서는 신원정보를 개인의 노드에 저장. 기업에게 중앙 시스템보다 효용이 있어야 DID 시스템을 사용하고 결국 산업이 성장할 것이다. **기업입장에서 장점은 보안 비용을 감축하고, 절차 간소화해 소비자에게 어필 가능. 개인의 정보를 가명 처리하여 활용하는 방법도 제시할 수 있다**.
3. 개인키의 사용성을 높여야 한다. 블록체인에서 개인키 잃어버리면 복구 불가능. 중앙 시스템은 비밀번호 변경 가능한데, 블록체인 개인키는 기존 시스템에 익숙한 사람에게 불편할거고, 지갑, 개인키, 공개키, 전자서명 등 낯선 개념은 진입장벽이 될 것.
4. 개인키 보안성 또한 중요한 문제. 블록체인은 데이터 위변조를 막는다는 점에서 보안성이 높지만, 개인키를 다른 사람이 활용하거나 해킹될 경우 대해 보안이 약하다. 이에 대한 해결책으로 개인키에 사용자의 생체 정보를 활용하거나 HSM(?)의 보안성을 높이는 방법. HSM은 하드웨어 보안 모듈로 디지털 키를 안전하게 보호하고 관리하는 기능. HSM은 개인키를 암호화하고 안전하고 분리된 곳에 저장하며, 키의 사용이력을 추적하는 기능을 제공.

마치며

1. 댜디는 인증 절차를 간소화해 UX를 개선하고. 블록체인을 활용해 정보의 위변조를 막으며, 데이터 주권을 보호하는 시스템으로 각광받고 있다. 또한 활용가능성과 잠재력이 많아 정부를 비롯해 우리은행, 신한은행, skt, kt,.

하지만 표준화 개발, 서비스를 이용할 기업의 효용, 개인키의 사용성 및 보안성 등 극복해야할 문제도 많습니다.