RETURN VALUES

Decentralized Identifier

Jan. 2019

RETURN VALUES

Agenda

I. 기존의 신원확인의 문제점

II. DIDs Overview

III. DIDs Model

IV. DIDs Ecosystem

기존의 신원확인의 문제점

신원 확인에서 신원은?

신원의 주체가 되는 사람에 관련된 정보를 뜻한다.

신원에 해당되는 정보는 성명, 나이, 주소, 학력, 직업 등 신원의 주체를 식별할 수 있는 모든 정보가 해당된다.

신원확인 시스템이란?

개개인의 중요한 특성을 기록하는 수단인 식별자와 그 주체가 일치하는지 입증하는 시스템

기존의 신원확인의 문제점

신원 확인의 예시

나는 술을 사기 위해 편의점에 갔고, 편의점에서는 내가 만 18세 미만인지 아닌지 확인하고자 나에게 '신분증' 을 요구하였다. 나는 내 나이가 만 18세 이상임을 증명하고자 도로교통공단에서 발급받은 운전면허증을 제시하였고, 편의점은 이를 확인 한 후에 술을 판매하였다.

KoROAD 도로교통공단

운전면허증의 발급 기관

운전면허증이 증명하는 주체

운전면허증으로 주체를 확인하는 검증 기관

기존의 신원확인의 문제점

디지털상에서 신원확인 시스템은 어느 특정 도메인 내에서 식별자와 그 특성을 관리하기 위해서 만들어 진 시스템이다.

즉 주체와 상관 없이 “조직”에서 필요한 시스템이므로 “조직”에서 소유되어진다.

하지만 “조직”에서 의도치 않게, 혹은 악의적으로 식별자를 노출한다면?

기존의 신원확인의 문제점

개인정보 유출을 통해 누군가 나의 신원을 복제한다면 내 명의로 다양한 범죄를 저지를 수 있다.
이와 같은 문제들로 인해 '자주적 신원증명'의 필요성이 강조되었다.

자주적 신원 (Self - Sovereign Identity)

신원의 주체가 되는 사용자가 스스로 저장하고 관리, 통제할 수 있는 신원

중앙에 의존하지 않는 형태

사용자가 어떤 앱이나 서비스에 접근하려면 자신의 ID를 비롯한 개인정보 수집 및 이용, 보관에 대한 광범위한 동의를 요구받는다. 위와 같은 유출사고로 인한 신원도용 범죄는 점점 빈번해지고 있어 이러한 피해를 막고 보안을 향상시키기 위해서는 새로운 개념의 디지털ID를 통해 개인이 자신의 정보를 직접 저장하고 통제할 수 있어야 한다는 주장이 제기되고 있다.

기존의 신원확인의 문제점

온라인 신원의 문제점

오프라인에서는 카드, 혹은 종이의 형태로 된 신원 증명을 항상 본인이 지니고 있어 '자주적'으로
신원의 관리가 가능하지만 그동안 온라인에서는 이러한 시스템을 구현하기 쉽지 않았다.
온라인 신원 증명을 보증해 줄 수 있는 제 3의 기관이 필요하며,
우리가 술을 살때에 운전면허증, 주민등록증, 대학교 학생증과 같이 나이와 사진이 있는
신분증을 아무거나 제시하지만 온라인에서는 오프라인에서처럼 융통성 있게 이루어 지지 않는다.
또한 늘 해킹의 위험이 있고 온라인상의 신원은 이메일, 전화번호와 같은 정보로 손쉽게
연계되는 범용 식별자에 의해 존재하기 때문에 안전하지 못하다는 단점이 있다.
가장 핵심적인 문제는 검색을 위해서는 결국 중앙화 된 서버로 접속하여 검색해야 한다는 점이다.

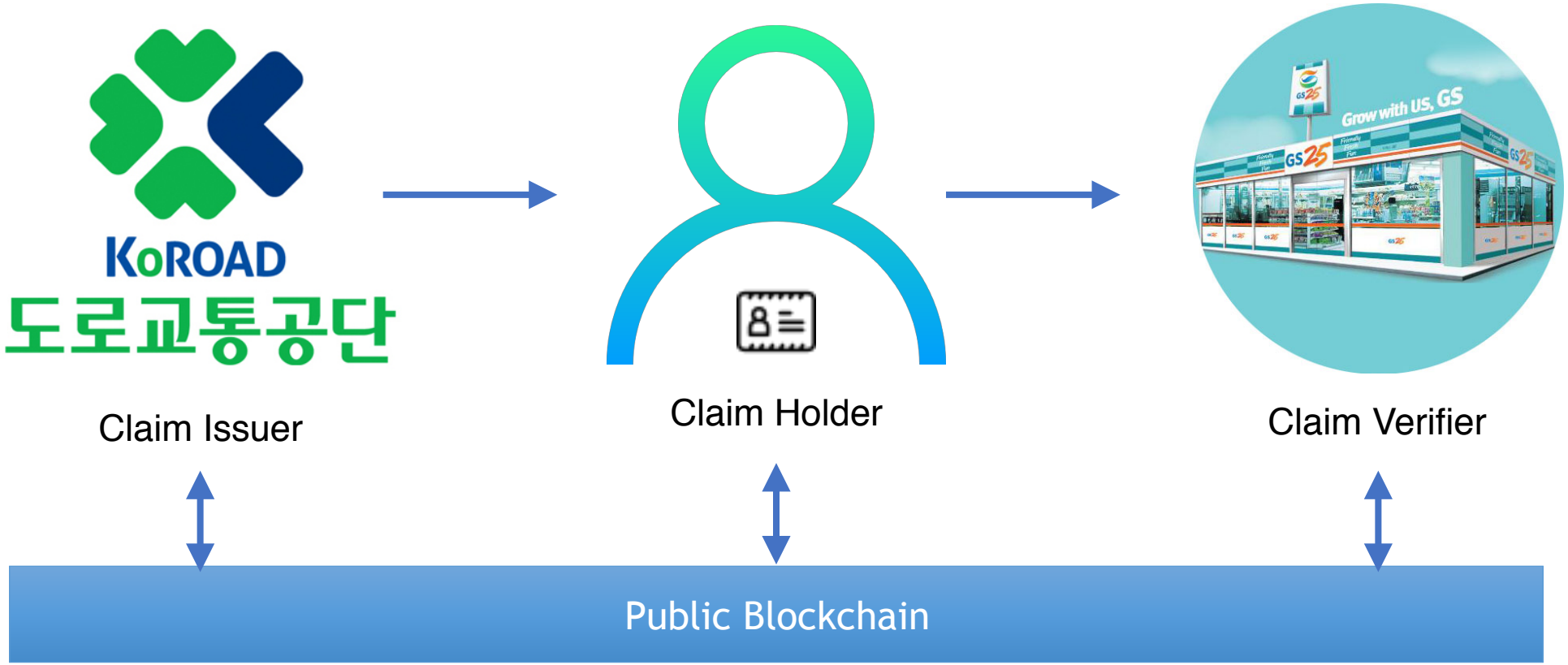
BLOCK CHAIN +DIDs

분산 원장 기술인 블록체인을 이용하면 중앙 서버 없이 분산된 식별자의 조회가 가능하다.

블록체인의 암호화를 통해 중앙 없이도 신뢰 가능한 자격 증명(Claim)을 제시할 수 있다.

온라인에서도 오프라인과 같이 내가 소지하고 관리하는 자격증명을 이용할 수 있다.

DIDs Overview



도로교통공단에서는 소지자에게 면허증의 디지털 표식을 제공한다. 발급처는 블록체인의 분산된 식별자와 연결된 개인키로 서명한다. 이로서 디지털 면허증은 다름아닌 도로교통공단이 발급했음을 증명한다. 소지자는 이를 개인키로 서명하고 월렛에 보관, 법적 성인임을 확인하는 온라인 편의점에서는 공개키를 통해 어디서 발급되었으며 주체와 제시자가 동일인인지 확인할 수 있다.

DID Documents

Credential 커뮤니티 그룹과 W3C 커뮤니티 그룹에서는 DIDs 작성을 위한 표준을 제시하고 있다.

공식 문서의 내용을 통해 DIDs의 구성과 동작원리에 대해 알아보자

DID (Decentralized Idengifier)는 2가지 요소로 이루어져 있다

1. 고유 아이디(did) : DID 문서를 찾는 키

> EXAMPLE 1: A simple example of a Decentralized Identifier (DID)
>
> ```
> did:example:123456789abcdefghi
> ```

DID Documents

2. DID Document : did를 비롯하여 생성시의 Time Stmap, 공개키 리스트, 해당 문서의 유효 증명 및 DID가 사용될 서비스의 리스트 등의 정보가 담겨있는 JSON-LD 오브젝트

EXAMPLE 2: Minimal self-managed DID Document

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    // this key can be used to authenticate as DID ...9938
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

DID Documents

Verifiable Claim

EXAMPLE 3: A simple verifiable claim

```
{
  "@context": "https://w3id.org/security/v1",
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "revocation": {
    "id": "http://example.gov/revocations/738",
    "type": "SimpleRevocationList2017"
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "598c63d6",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/+
    MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
    PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed
    +W3JT24="
  }
}
```

id 항목의 URI를 통해 외부에 있는 공개키를 얻어 올 수 있다. 이를 통해 클레임 유효성을 검증한다.

DID Documents

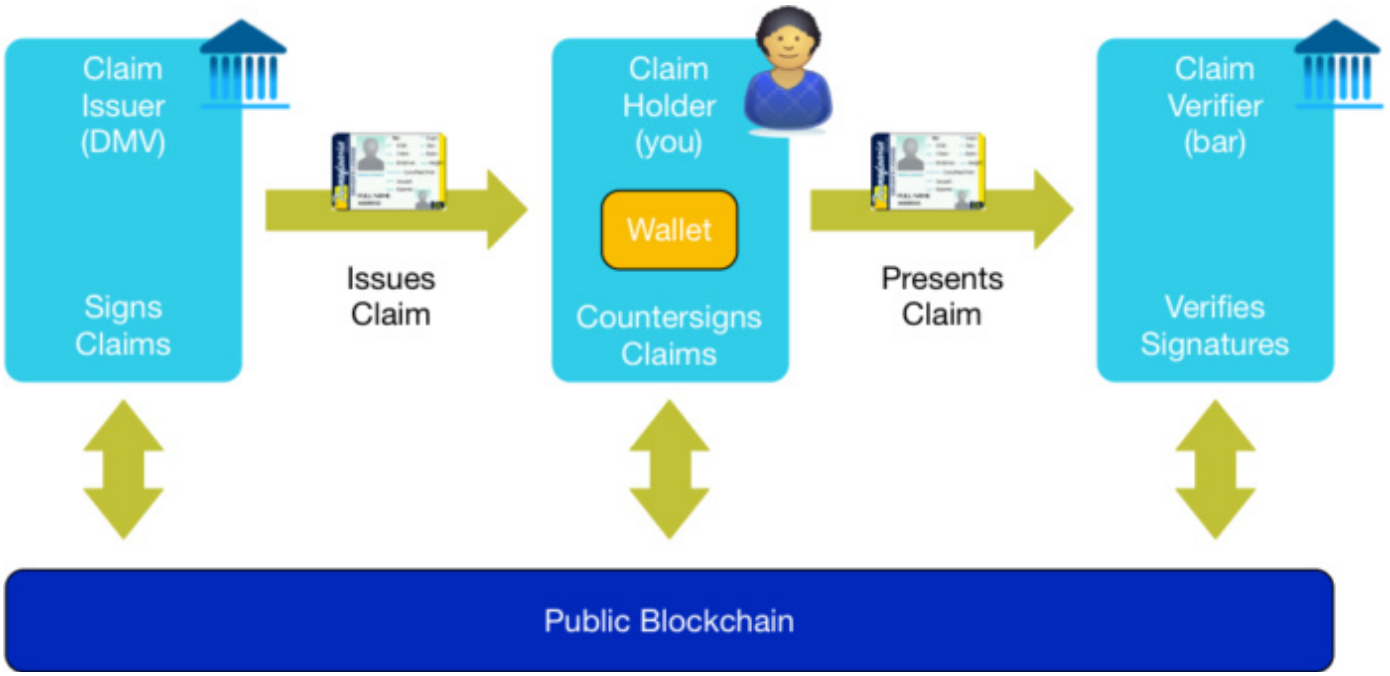
Verifiable Claim

- Subject : 사용자 즉 클레임(확인 가능한 증명)의 주체가 되며 이 항목에는 개인, 회사 애완동물 등

- Issuer : 클레임의 발급자 항목이며 정부, 공공기관, 대학등의 조직

- Claim : 증명을 위한 Subject와 관련된 정보가 서술되는 항목

DIDs Ecosystem



DIDs와 같은 기술로 신원 확인 시스템의 새로운 신원 확인 생태계를 기대할 수 있다.

기존의 신원 확인 시스템에서는 사용자와 서비스 제공자간의 정보교환이 이루어지지만

DIDs에서는 사용자와 서비스 제공자, 발급자의 역할이 뚜렷하기 때문이다.

DIDs Ecosystem

1. 사용자 (Users, Claim Holder)

- 사용자의 개인키가 비공개로 유지되는 한 자기 자신의 신원을 제어할 수 있다.

- 오늘날 많은 사람들은 Google, Facebook과 같은 ID 공급원을 통해 타 웹사이트에 로그인을 한다. 이런점에서 ID공급자들은 사용자의 통제와 감시할 메소드를 쥐게 되는데, DIDs의 이용으로 이러한 제 3자 계정에 의존할 필요가 없어지게 된다.

- 블록체인 기술을 사용함으로써 제 3자는 물론 발급 당국 책임자가 함부로 변경할 수 없어 안전하다.

2.서비스 제공자 (Service Providers, Claim Veryfier)

- 고객의 개인정보를 노출 시킬 위험 부담이 줄어든다. 특히 GDPR과 같이 개인정보 보호 규약이 엄격한 환경에서는 조금의 노출 위험이 있을 경우 막대한 벌금을 부과 받는데 DIDs를 이용하게 된다면 기존과 같이 개인정보를 수집할 필요가 적어지게 된다.

- 서비스 제공자 측에서는 고객의 어떤 claim을 사용자에게서 수용할 것인지와 고객에게서 제공받은 claim과 그 claim의 발급처와 어떻게 법적 관계를 수립할 것인지에 대한 고려가 필요하다.

3.Claim 발급자 (Claim Issuer)

- 사용자가 원하는 형태에 맞는 암호화 된 Claim을 제공할 수 있어야 한다.

- 웹 혹은 모바일 서비스가 다양한 만큼 여러 사용 사례에 맞추어 사용자에게 전송할 수 있어야 한다.

4.DIDs 기술 제공자(Technology Providers)

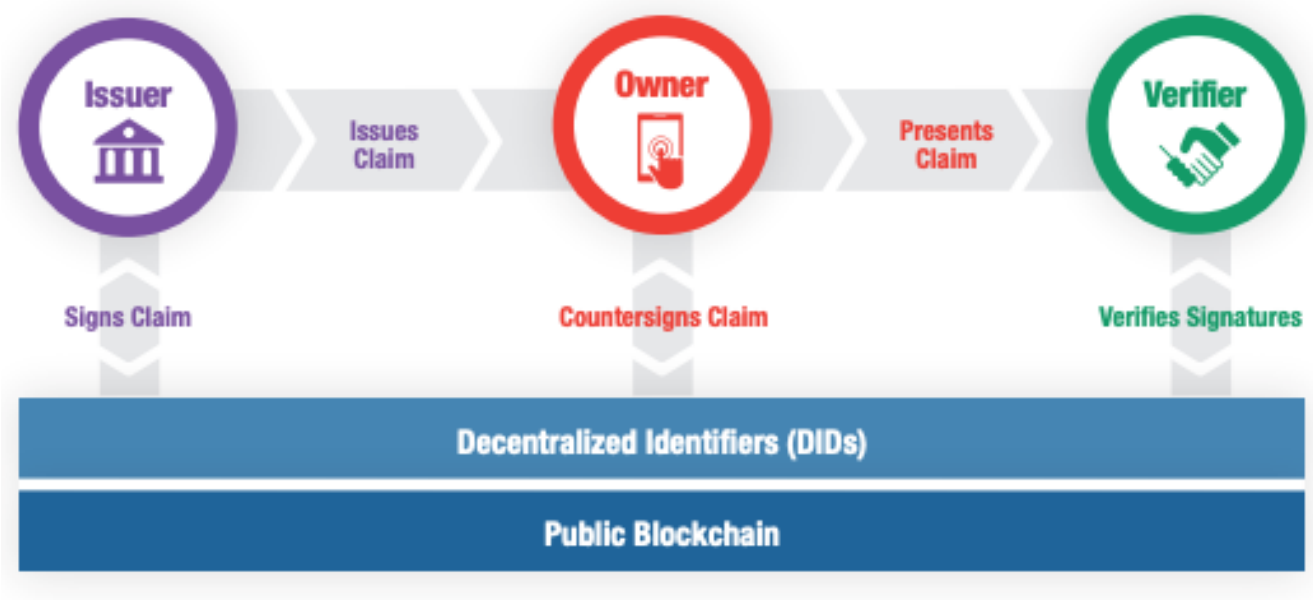
- 기술 제공자는 사용자가 서비스 제공자에게 원활하게 Claim을 제시할 수 있도록 해야 한다.
- 발급자가 사용자에게 적합한 암호화 된 Claim을 발급할 수 있도록 해야 하는 핵심적 역할
- 기존의 정보수집을 통해서 신원을 확인하는 시스템이 아닌 분산원장을 이용한 공개키 암호 인증방식이기 때문에 그에 맞는 기술적, 데이터 모델을 구축해야 한다.

DIDs Ecosystem

DIDs 기술을 활용하는 플랫폼 Sovrin

sovrin
identity for all

- 자주적 신원 증명을 위해 탄생된 블록체인 플랫폼 (Hyperledger Indy 프로젝트)
- 개인정보는 블록체인에 저장하지 않고 DID, Public Key만 블록체인에 저장한다.
- Identity Owner가 정보 노출 범위를 설정할 수 있다(Selective disclosure)
- ZKP(영지식증명)기술을 사용하여 실제 정보 노출 없이 주체에 대한 증명이 가능하다.



DIDs Ecosystem

이더리움 기반 자주적 신원증명 플랫폼 Uport

- 이더리움 어카운트와 동일한 Uport ID를 통하여 자주적 신원증명이 가능한 플랫폼
- 스마트 컨트랙트를 통해 영구적 식별자(Persistent Identifier)를 제공하고 개인키를 분실했을 경우를대비하여 키 복구 및 교체가 가능하도록 설계되었다.
  (Digital Identity + Key Management)
- Schema 협약에 따라 JSON Profile 객체를 생성하고 IPFS에 업로드 하여 레지스트리에 SetAttribute 트랜잭션을 생성, IPFS 해시 공개
- Uport ID로 모든 이더리움의 어플리케이션에 접근이 가능하다.

Reference

•Blog
Understanding Decentralized IDs (DIDs)
https://medium.com/@adam_14796/understanding-decentralized-ids-dids-839798b91809

What is a uPort identity?
https://medium.com/uport/what-is-a-uport-identity-b790b065809c

•Documents
Decentralized Identifiers(DIDS) v0.11
https://w3c-ccg.github.io/did-spec/

Sovrin White Paper
http://www.iotakorea.net/wp-content/uploads/2018/04/Sovrin-Protocol-and-Token-White-Paper.pdf

•Press
블록체인은 어떻게 자주적 신원을 실현하는가?
http://www.itworld.co.kr/news/107849

contact@returnvalues.com