2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

Session 2-4

Healthcare Blockchain

이은솔 공동대표 (메디블록)

[요약문]

비트코인으로 대표되고 있는 블록체인 기술은 P2P 분산 네트워크에 일종의 거래 장부라고 할 수 있는 분산원장을 공유하는, 암호화 네트워크 기술이라고 할 수 있다. 일반적으로 블록체인은 운영주체가 없는 탈분산 시스템으로서 탈중앙성, 투명성, 비가역성, 그리고 이를 바탕으로 하는 신뢰성 등을 특징으로 한다.

헬스케어와 관련하여 블록체인은 DID를 활용한 인증, 그리고 데이터에 대한 신뢰를 바탕으로 하는 PHR 등에 활용할 수 있다. 이상적인 PHR을 위해서는 필수적으로 특정 병원에 종속되지 않는 시스템을 구현을 해야하며 이를 개인이 관리할 수 있어야만 한다. 그럼에도 불구하고 보안, 프라이버시의 문제가 지켜져야한다는 과제가 있다. 블록체인 기술은 여기에 가장 적합한 이상적인 기술이다. 누구에게도 종속되지 않고 거래가 이루어지고 증명이 되고 있는 비트코인처럼, PHR에 블록체인 기술을 접목하게 되면 독립적이면서도 완전하게 개인에 의해 관리 가능한 PHR의 구현이 가능하다.

[발표자 약력]

2003-2009	한양대학교 의과대학 의학과 학사 졸업
2012-2014	울산대학교 의과대학 의학과 석사 졸업 (지도교수: 서준범)
2017-	울산대학교 의과대학 의공학과 박사 (지도교수: 서준범)
2009-2010	서울아산병원 인턴
2010-2014	서울아산병원 영상의학과 전공의
2014-2017	공중보건의
2016-2017	정보의학인증의
2019	바이오산업IP 특별전문위원회 위원
2019	NIPA 블록체인 규제개선 연구반 위원
2017-	주식회사 메디블록 공동대표
2019-	대통령직속 4차산업혁명위원회 혁신위원
2019-	대통령직속 4차산업혁명위원회 디지털 헬스케어 특별위원회 위원
2020-	개인정보보호위 제도혁신단 자문위원
2020-	한양대학교 의과대학 IAB 자문교수
2020-	성균관대학교 삼성융합의과학원 겸임교수

블록체인과 의료정보 플랫폼

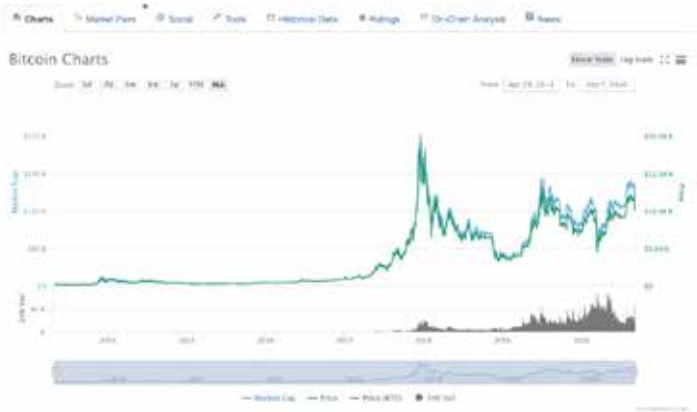
나는 누구?

- 메디블록 공동대표, 창업자 (2017년 4월 ~)
- 디지털헬스케어특별위원회 특별위원 (2019~)
- 성균관대학교 삼성융합의과학원 겸임교수, 한양대학교 의과대학 IAB 자문교수
- 공중보건의 (2014~2017)
- 서울아산병원 인턴, 영상의학과 전공의 (2009~2014)
- 한양대학교 의과대학 (2003~2009)

- 2001 한국정보올림피아드 금상
- 2003 넥슨, 2004 도전하는사람들, 2006 나인티시스템, 2007 모 교수님 플젝, 2008 서울아산병원 MIL
- 2017 MS-AMC 의료 빅데이터 분석 콘테스트 LOL 팀으로 수상

medibloc

블록체인
의료 분야에서의 활용
DID (Decentralized Identity)



[기자수첩] 3년 묵은 가상자산 정책, 손볼 때 됐다

가상자산 투기현상을 막겠다며 정부가 다급히 내놓은 고강도 가상자산 규제정책이 3년째 이어지고 있다. 블록체인 기술은 육성하되 가상자산은 사업으로 인정하지 않겠다는 이분법적 정책이 우리 정부의 정책 기조다.

블록체인이란?

- 블록체인: (하나의 컴퓨터가 아닌) 여러 컴퓨터들이 공통으로 데이터를 관리할 수 있도록 하는 기술, 또는 저장소
- 가상자산: 블록체인의 가장 대표적인 use case
    - 장부에 어느 계정 소유주가 얼마만큼의 BTC, ETH 등을 들고 있는지, 또 어느 계정 소유주가 다른 계정에게 얼마만큼의 BTC, ETH 등을 보냈는지를 모두 기록
    - 계정의 소유주만 전자 서명 형태로 블록체인에 기록을 할 수 있으며, 한번 기록, 다른 컴퓨터에 전파되면 되돌릴 수 없음
    - 컴퓨터에서 블록체인 프로그램 운영을 하는 운영자(노드)는 해당 네트워크에서 거래되는 가상자산을 보상으로 받음

Centralized Model

구글, 네이버, …

Decentralized Model

비트코인, 이더리움, 리플, …

medibloc

법정화폐 vs. 가상자산

- 법정화폐 (법정통화)
    - 원(KRW), 달러(USD) 등 국가가 정한 법률에 의해 그 가치가 보장되는 화폐
    - 원화의 경우 한국은행법에 의해 한국은행이 발행, 관리
    - 국력, 신용도 등에 의해 그 가치 및 신용도가 따라감
    - 국가의 흥망성쇠와 함께 함
- (블록체인 기반) 가상자산
    - 비가역적인 공유 데이터 저장소인 블록체인에 의해 기록, 관리가 이루어지는 전자 화폐
    - 누구나 읽을 수 있지만, 계정 소유주만 비밀키를 가지고 있고 이를 이용하여 전자서명을 할 수 있으므로 소유권 행사 - 쓰기 권한 - 가능
    - 컴퓨터 프로토콜에 의해 자동으로 관리
    - 얼마나 많은 곳에 의해 사용이 이루어지냐, 또 의미있는 참여자들에 의해 운영되냐 등에 따라 그 가치 및 신용도 등이 따라감
    - 프로토콜에 문제가 있거나 유의미한 해킹이 있을 시 문제

medibloc

블록체인에 가상자산 말고 다른 것?

- 자산 거래 장부
  - 가상 자산 (BTC, ETH, …)
  - 부동산 거래 장부
  - 미술품 거래 장부
  - …
- 데이터 기록
  - 영원히 박제되는 데이터 저장소
- 인증
  - DID 등 public key 저장소
  - Hash 값 저장소

medibloc

블록체인의 특징

- 탈중앙성
    - 중앙화된 시스템 (서버나 데이터베이스 등) 없이 모두가 공유 가능한 데이터를 만들어내고 관리할 수 있음
- 투명성
    - 누구나 데이터에 접근, 모니터링 가능함
- 무결성
    - 한번 작성되면 기록을 되돌릴 수 없어 저장된 기록에 대해 신뢰 가능
- 비싼 가격
    - 컴퓨터, 네트워크 리소스를 많이 소모함

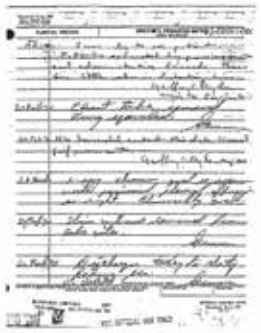
medibloc

블록체인의 활용

- 기존 시스템 + 블록체인
- 블록체인의 가격이 비싼 만큼 꼭 필요한 곳에 블록체인을 활용하는 것이 중요
    - 동등한 지위의 시스템 끼리의 데이터 공유, 거래 등, ...

medibloc

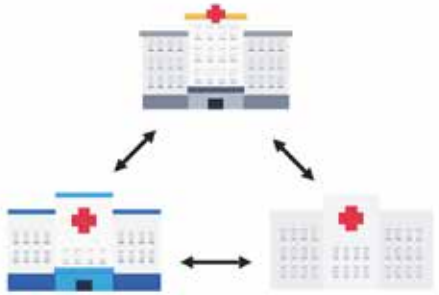
의료기록



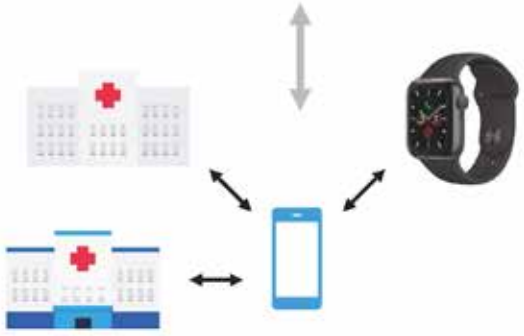
그냥 진료 기록.. ?
(in 의료기관, in 개인)

EMR

Life log



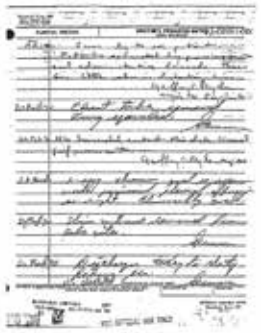
EHR



PHR

medibloc

의료기록



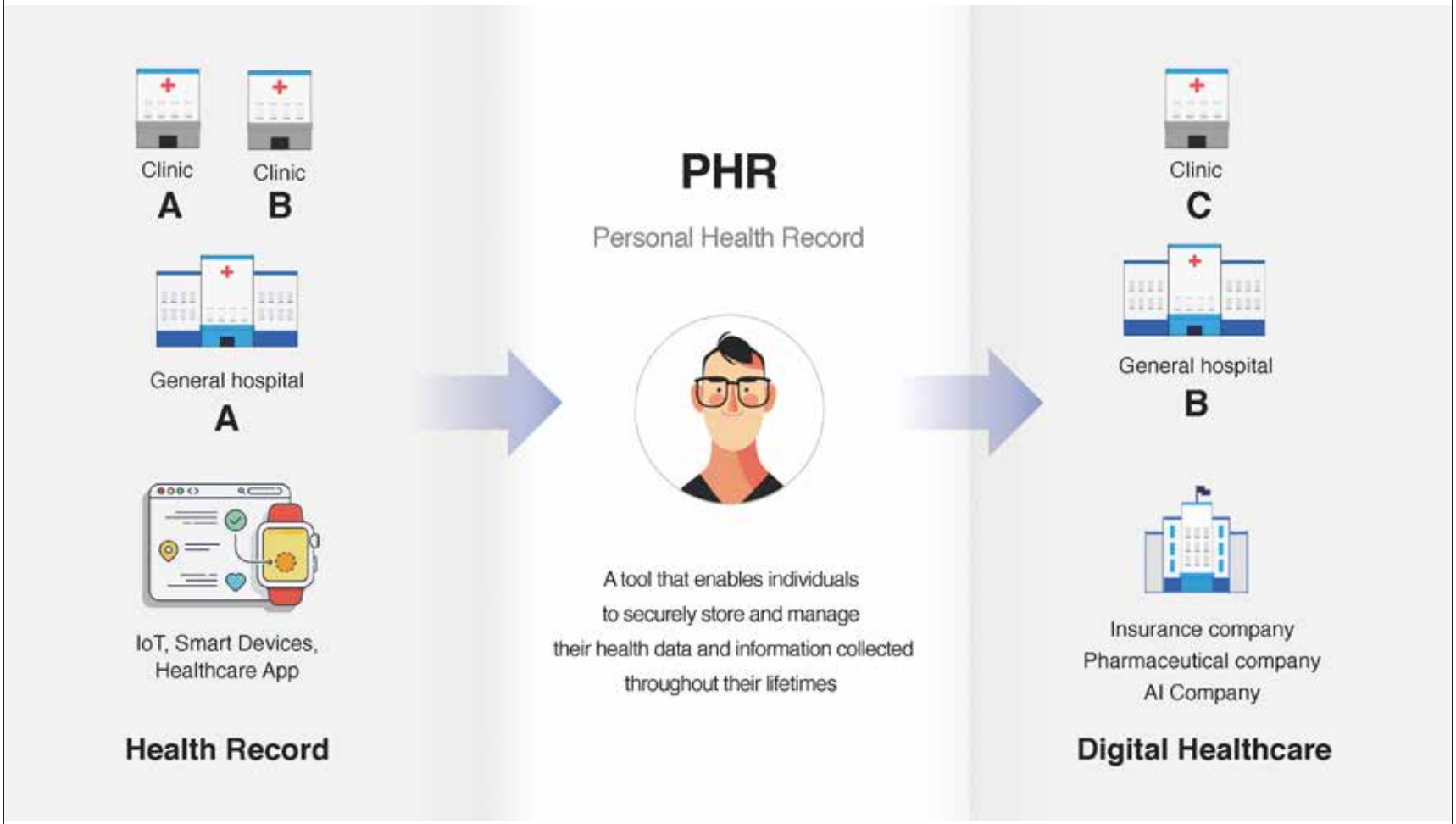
그냥 진료 기록.. ?
(in 의료기관, in 개인)

EMR

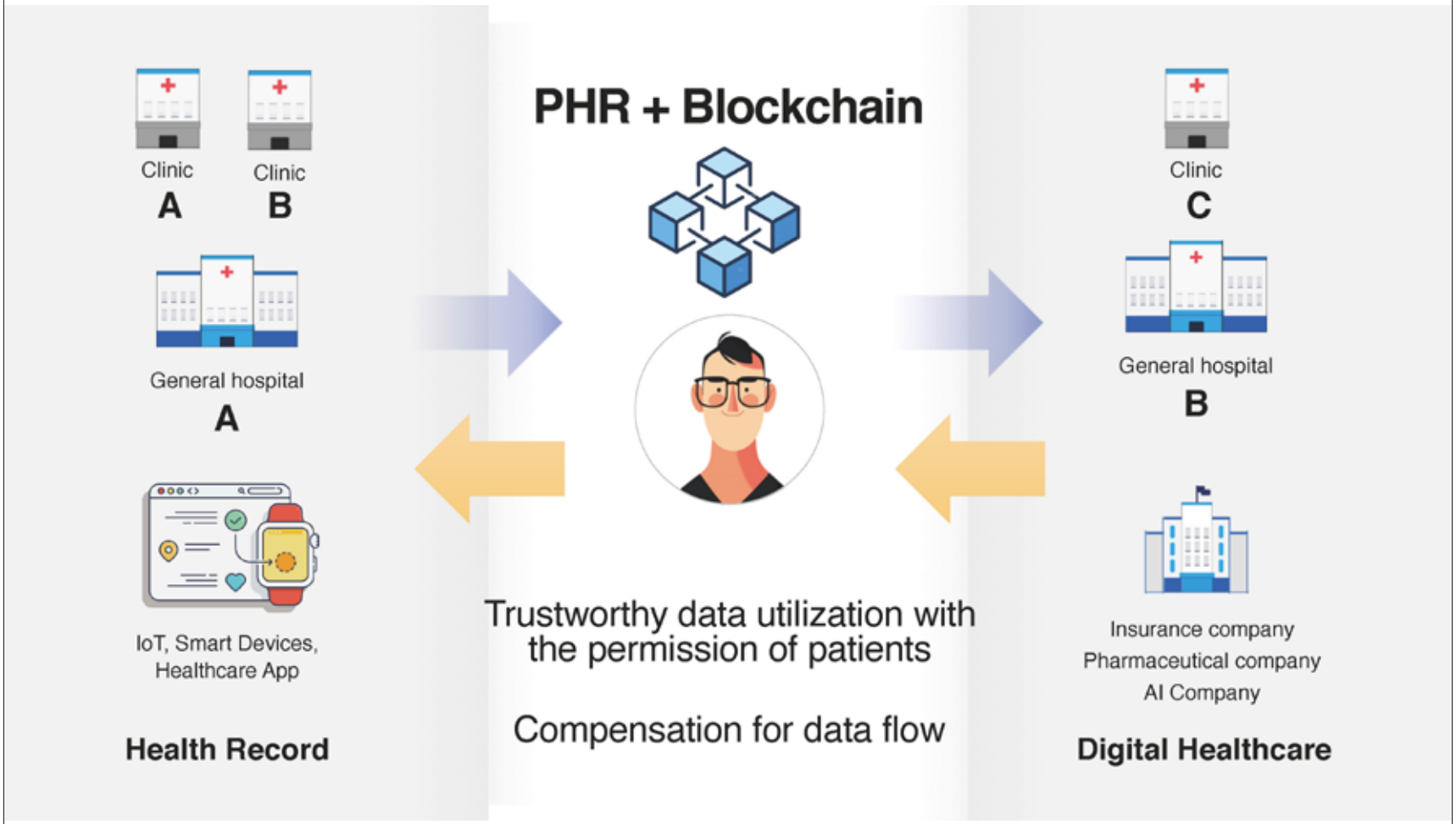
Life log

EHR

PHR


Clinic
A
Clinic
B
General hospital
A
IoT, Smart Devices,
Healthcare App
Health Record
PHR
Personal Health Record
A tool that enables individuals
to securely store and manage
their health data and information collected
throughout their lifetimes
Clinic
C
General hospital
B
Insurance company
Pharmaceutical company
AI Company
Digital Healthcare

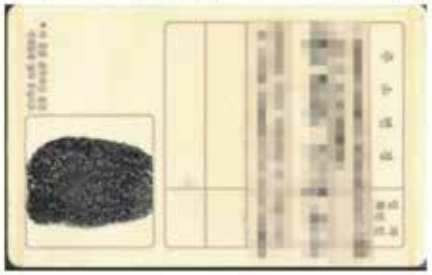

Clinic
A
Clinic
B
General hospital
A
IoT, Smart Devices
Healthcare App
Health Record
PHR
Personal Health Record
Data Forgery
Reliability Issue
Insufficient Incentive
to securely store and manage
their health data and information collected
throughout their lifetimes
Clinic
C
General hospital
B
Insurance company
Pharmaceutical company
AI Company
Digital Healthcare


PHR + Blockchain
Clinic
A
Clinic
B
General hospital
A
IoT, Smart Devices,
Healthcare App
Health Record
Trustworthy data utilization with
the permission of patients
Compensation for data flow
Clinic
C
General hospital
B
Insurance company
Pharmaceutical company
AI Company
Digital Healthcare

Data Flow

DID 란?

- 가상 세계에서의 ID 카드, 신원 인증 수단 필요
- 현실 세계에서의 ID 카드: 주민등록증 -> 지자체 (정부) 에 의해 이 사람은 이런 번호를 가진 이런 사람이라는 것을 증명하는 ID 카드



- 현실 세계에서의 신원 인증 수단: 지문, 얼굴 인식, … -> 지문, 얼굴을 이용해 시스템에 등록된 패턴과 대조

medibloc

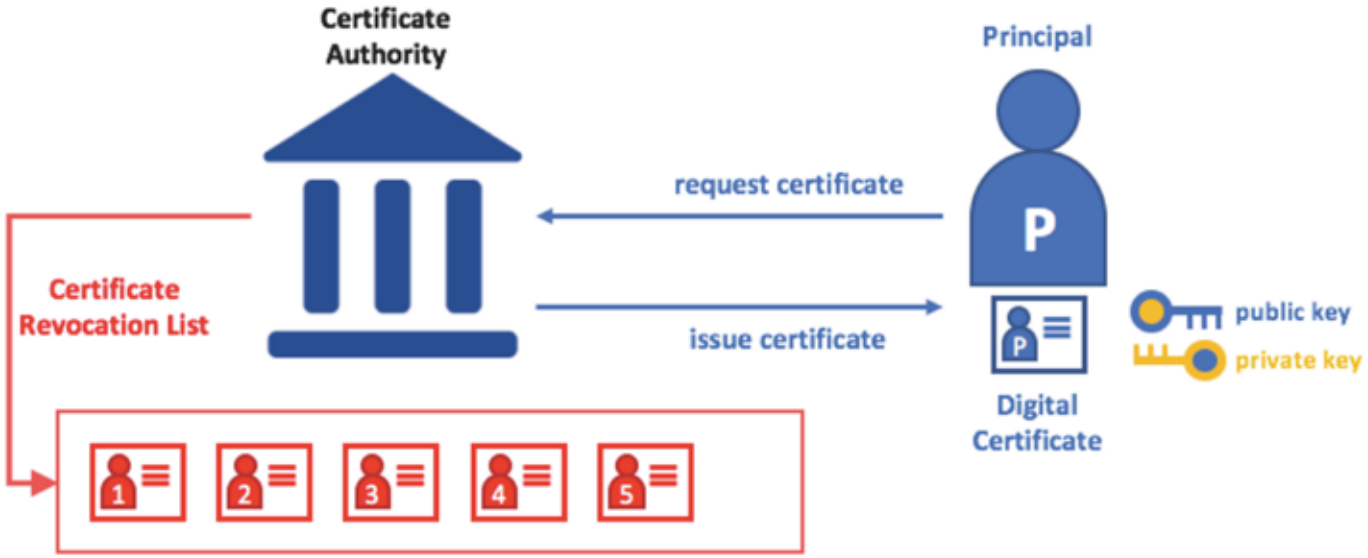
Why DID in Healthcare?

- 의료기관, 의료인, 환자, 보호자, 보험사, PHR 업체 등 다양한 주체에 대한 인증 필요
- 국내 뿐만 아니라 해외 기관에 대한 인증 필요
- 신원 인증 뿐만 아니라, 데이터, 동의서 등 다양한 형식에 대한 인증 필요

- 의료기관 DID, 의료인 DID, 환자 DID, 보호자 DID, …
- 의료기관 -> 해당 의료기관을 다니는 환자임을 증명하는 VC
- 의료기관 -> 해당 의료기관에서 검사한 기록임을 증명하는 VC
- 환자 -> 의료기관에서 수술 받는 거에 동의했다는 것을 증명하는 VC
- …

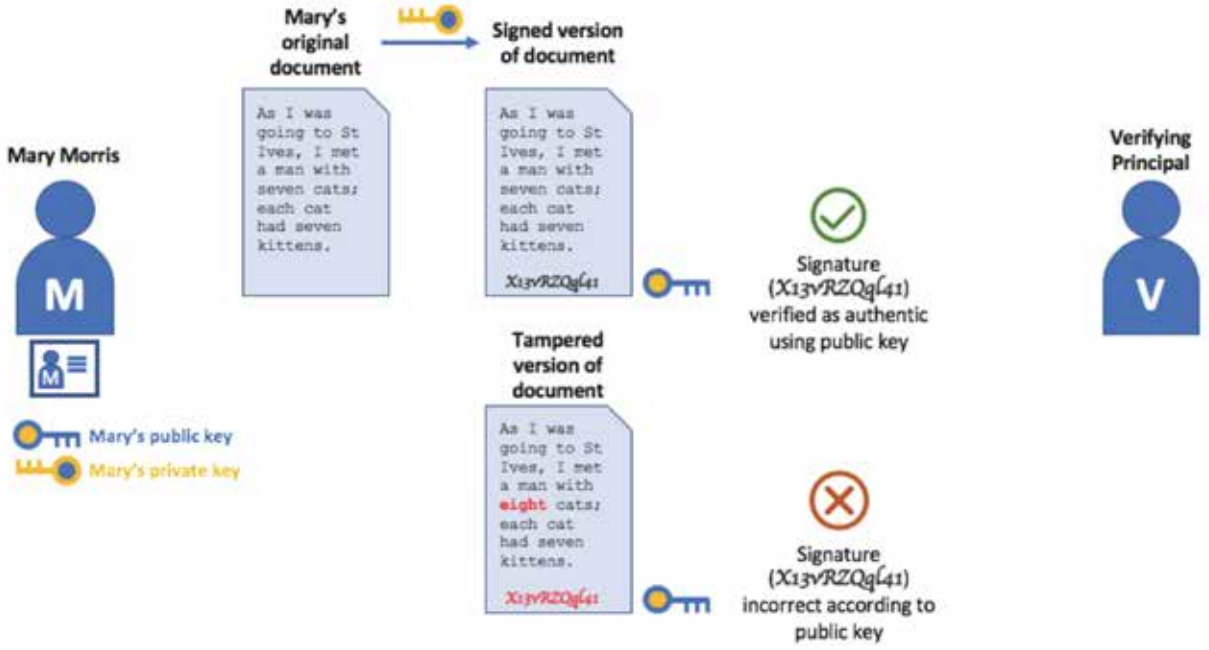
medibloc

디지털 세상에서의 ID 카드: Digital Certificate

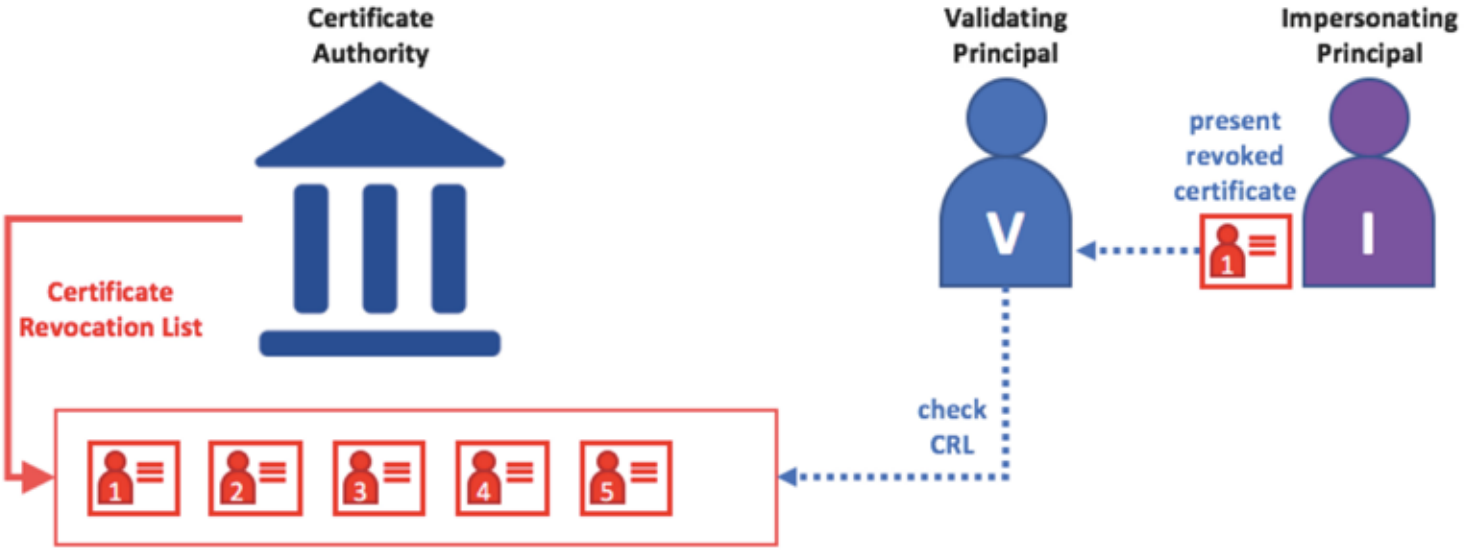


디지털 세상에서의 ID 카드: Digital Certificate

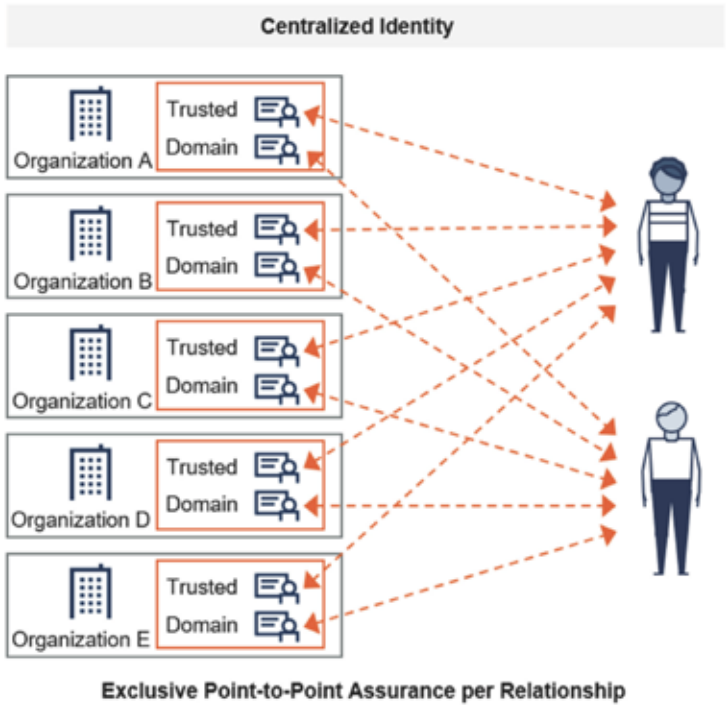
디지털 세상에서의 서명(signature) 검증



디지털 세상에서의 서명(signature) 검증

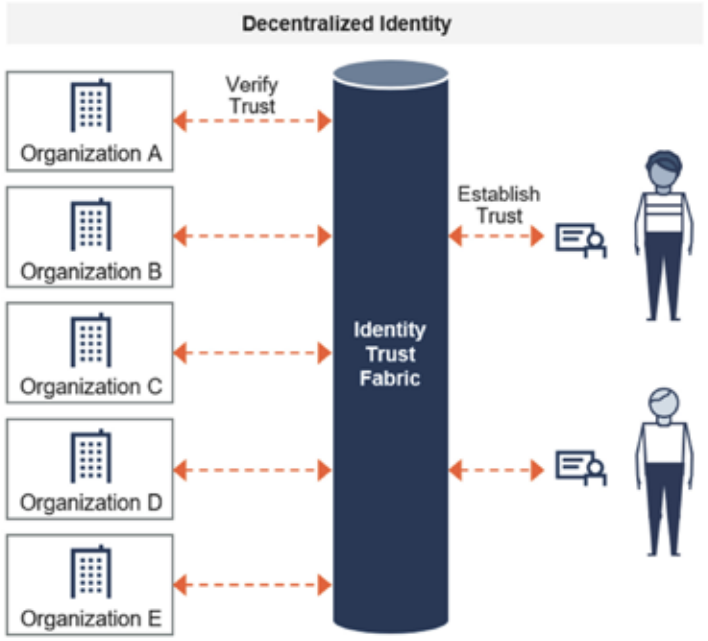


ID 발급자가 엄청 많다면?



- 각 발급자에게 어떻게 access 할 것인가?
- 발급자들을 신뢰할 수 있는가?
- 발급자들의 보안은 안전한가?
- 각기 다른 Certificates를 어떻게 활용할 것인가?
- Certificates을 활용하는 Apps는 대체 얼마나 많은 Certificates을 지원해야하는가?

표준이 필요하다. 하지만 안전하고 공개적으로



The Common Shared Assurance on Identity Trust Fabric

- 모든 발급자들은 '표준'에 따라 ID 발급
- ID card는 안전한 공개 저장소에 보관
  - 악의적인 자가 데이터를 변조/삭제할 수 없는
  - 모두가 서로의 ID card를 조회할 수 있는
  - 세계 어디서든 접근 가능한

표준: DID (Decentralized Identifier)

did:panacea:mainnet:DnreD8QqXAQaEW9DwC16Wh

- 주민등록번호 같은 것. 하지만 세계적 표준 format을 따름 https://www.w3.org/TR/did-core/
- unique
- immutable
- 1인당 n개 가질 수 있다. use-case에 따라 여러개 가질수도잇고, 재발급 등의 수요도 있다

표준: DID Document

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:panacea:mainnet:DnreD8QqXAQaEW9DwC16Wh",
  "authentication": [
    "key1"
  ],
  "publicKey": [
    {
      "id": "key1",
      "type": "Secp256k1VerificationKey2018",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    }
  ],
  "service": [
    {
      "id": "svc1",
      "type": "VerifiableCredentialService",
      "serviceEndpoint": "https://example.com/vc/"
    }
  ]
}
```

- ID card(주민등록증) 같은 것. 하지만 공통 포맷
- public key (지문)가 기재되어 있음
- 안전한 공개 저장소에 보관되어야 함
  - 모두가 read 할 수 있도록
- 오직 ID owner에 의해서만 변경/삭제 가능

- 단, 세부 포맷은 플랫폼(DID method)에 따라 다를 수 있음.
  - 예) 플랫폼 = panacea, bitcoin, ethereum, …

https://github.com/medibloc/panacea-core/blob/master/docs/did.md

안전한 공개 저장소: Blockchain

did:panacea:mainnet:DnreD8QqXAQaEW9DwC16Wh

+

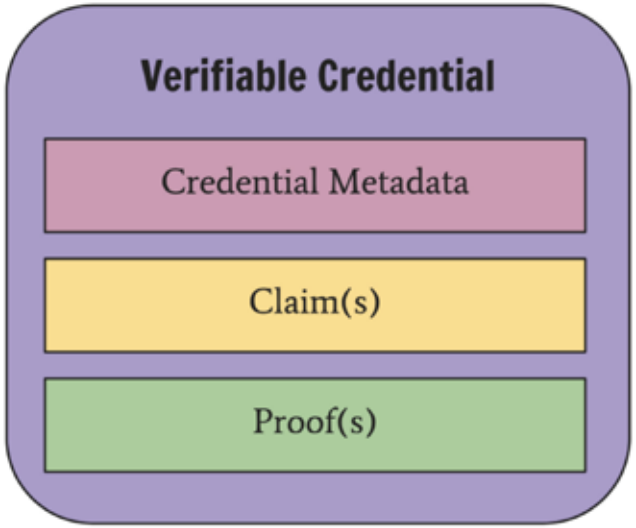
DID Doc

Stored

Panacea

- Blockchain은
  - 데이터가 수정/삭제될 수 없다.
  - 모두가 read 할 수 있다.
  - 세계 어디서건 일관된(consistent) data를 read 할 수 있다.

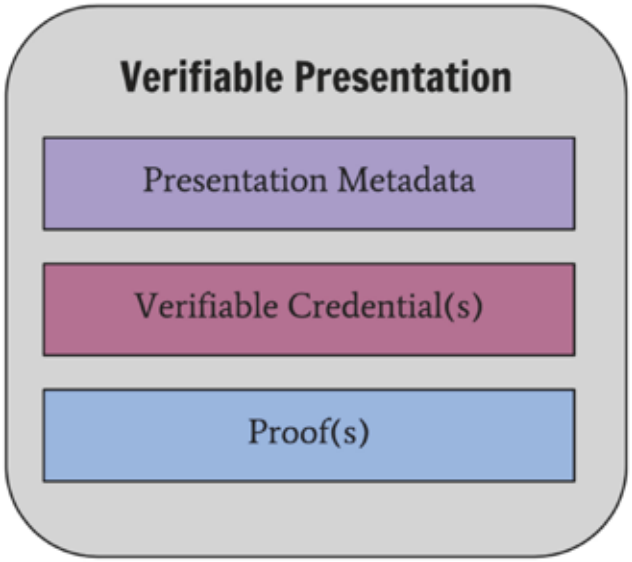
표준 VerifiableCredential: Signature(proof)를 포함한 Data card

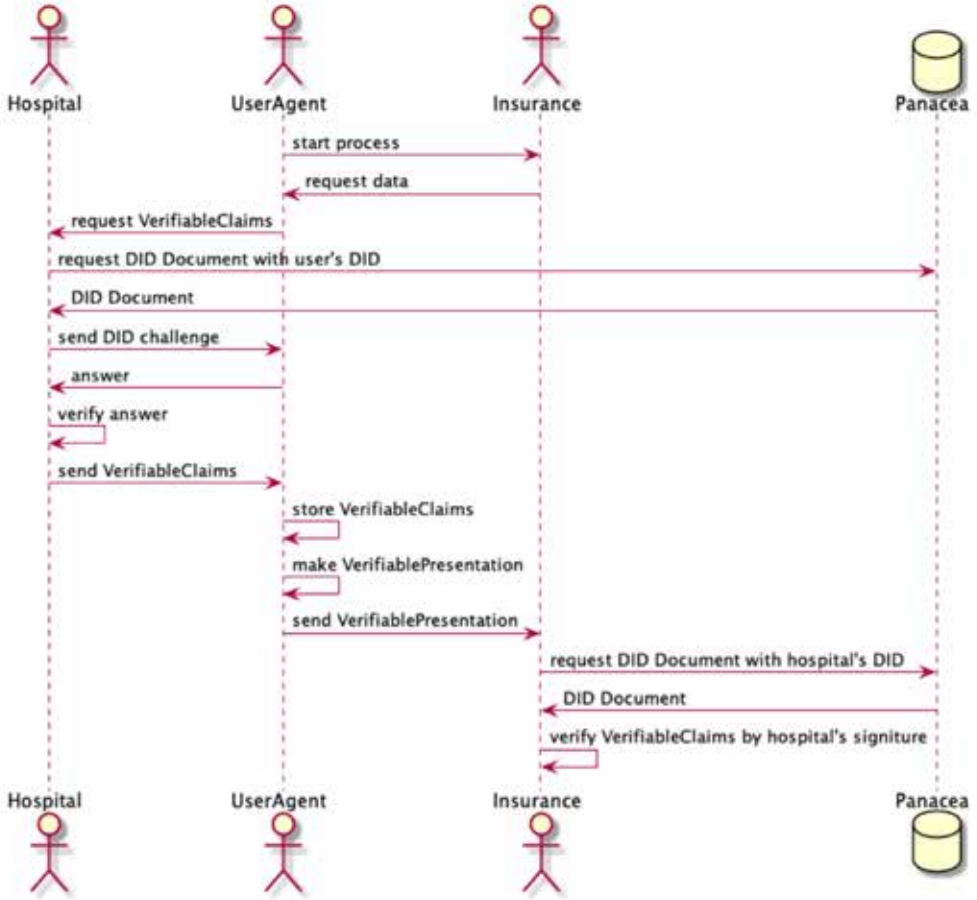


표준 VerifiableCredential: Signature(proof)를 포함한 Data card

```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential"],
  "issuer": {
    "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
    "name": "Example University"
  },
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "jws": "eyJhbGciOiJSUzI....UdBBPM"
  }
}
```

VerifiablePresentation




Hospital
UserAgent
Insurance
Panacea
start process
request data
request VerifiableClaims
request DID Document with user's DID
DID Document
send DID challenge
answer
verify answer
send VerifiableClaims
store VerifiableClaims
make VerifiablePresentation
send VerifiablePresentation
request DID Document with hospital's DID
DID Document
verify VerifiableClaims by hospital's signiture
Hospital
UserAgent
Insurance
Panacea


Our Solution
환자향
My palette
병원향
Dr.palette
환자향
medipass
마이팔레트 Q2 2020. 개발 완료 예정
• 진료 예약/접수
• 진료기록 및 건강검진 기록 관리
• 모바일 전자처방전
• 복약지도 및 건강 관리
닥터팔레트 Q4 2019. 청구 S/W 승인, Q1 2020 출시 예정
• 진료기록 작성 및 관리
• 환자 건강 관리
• 임상의사결정지원시스템(CDSS) 지원
메디패스 Q4 2019. 출시
• 진료기록 조회
• 보험금 간편 청구
• 맞춤형 보험상품 추천
• 건강증진형 보험 관리

End