

COOV: 블록체인 기반 백신접종증명 시스템 구축 사례 및 전망

GISC 2021

Jaehoon Shim, Nov 10 2021



Jaehoon Shim

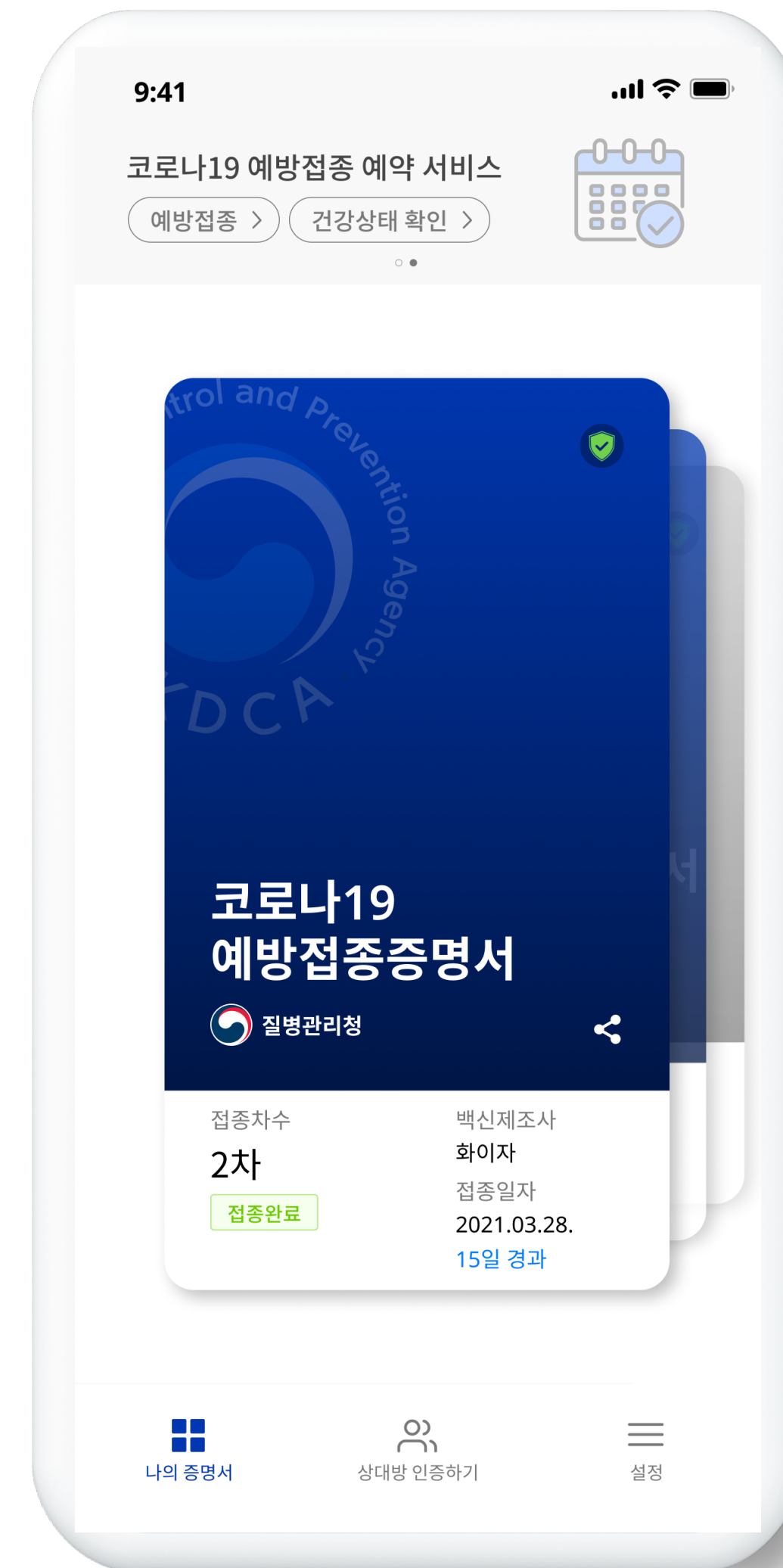
Head of Product @블록체인랩스

- 질병관리청 COOV 총괄 PM
- SSIMeetup Korea Lead Organizer
 - W3C Decentralized Identifiers v1.0 표준,
Verifiable Credentials v1.0 표준 번역 Lead
- TTA ICT 국제표준화 전문가
- (전) LG CNS 블록체인 연구원
- CS @ University of Illinois at Urbana-Champaign

세계 최초 블록체인 기반 코로나 19 디지털 예방접종 증명서

COOV

전자예방접종증명서 발급시스템



Statistics

15.78 M

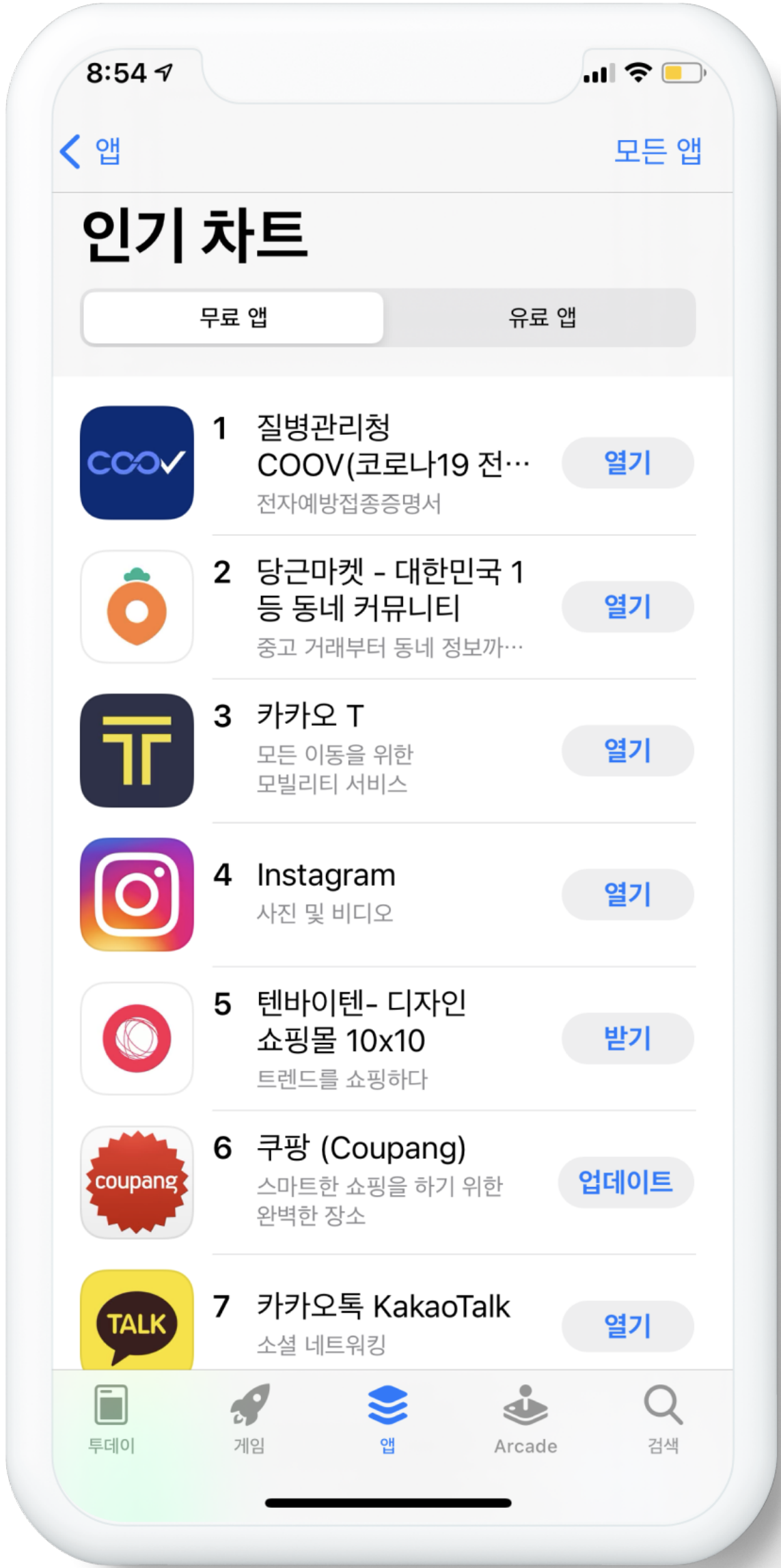
Downloads

141M

Issued Credentials

13.2M

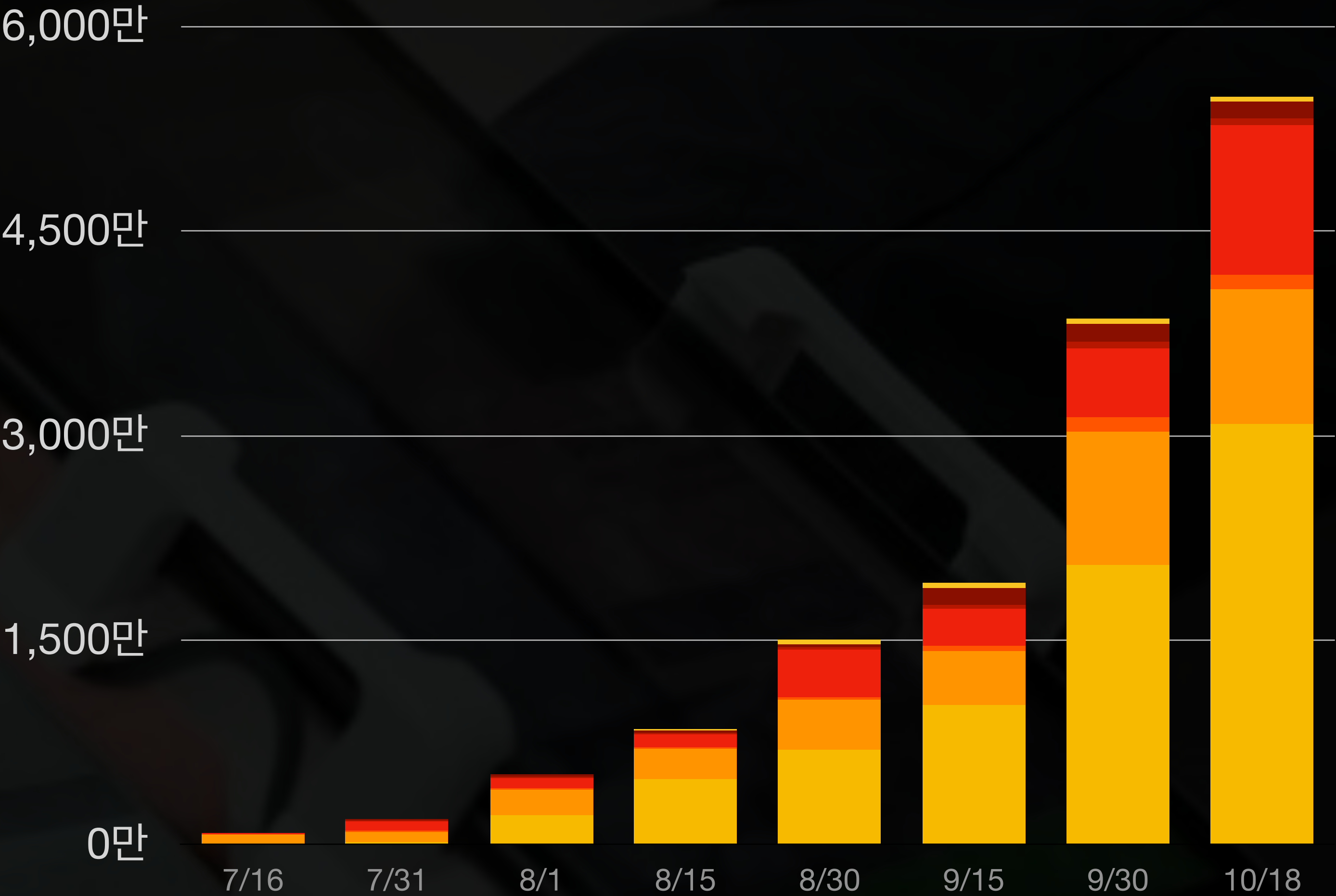
Verifications



Domestic Usage



QR x COOV
전자출입명부 시스템과 통합



전체 발급된 증명서 수
(플랫폼 중복 가능)

Problems

위변조 방지 개인정보 보호

COVID-19 Vaccination Record Card

Please keep this record card, which includes medical information about the vaccines you have received.
Por favor, guarde esta tarjeta de registro, que incluye información médica sobre las vacunas que ha recibido.

Tschacher Last Name *Megan* First Name *MI* State

Date of birth _____ Patient number (medical record or IIS record number) _____

Vaccine	Product Name/Manufacturer Lot Number	Date mm dd yy	Healthcare Professional or Clinic Site
1 st Dose COVID-19	<i>COVID-19 EH 9899 / Pfizer</i>	<i>12 / 14 / 2020</i> mm dd yy	<i>UHealth PVH</i>
2 nd Dose COVID-19		mm dd yy	
3 rd Dose COVID-19		mm dd yy	
Other		mm dd yy	

Problems

위변조 방지 개인정보 보호



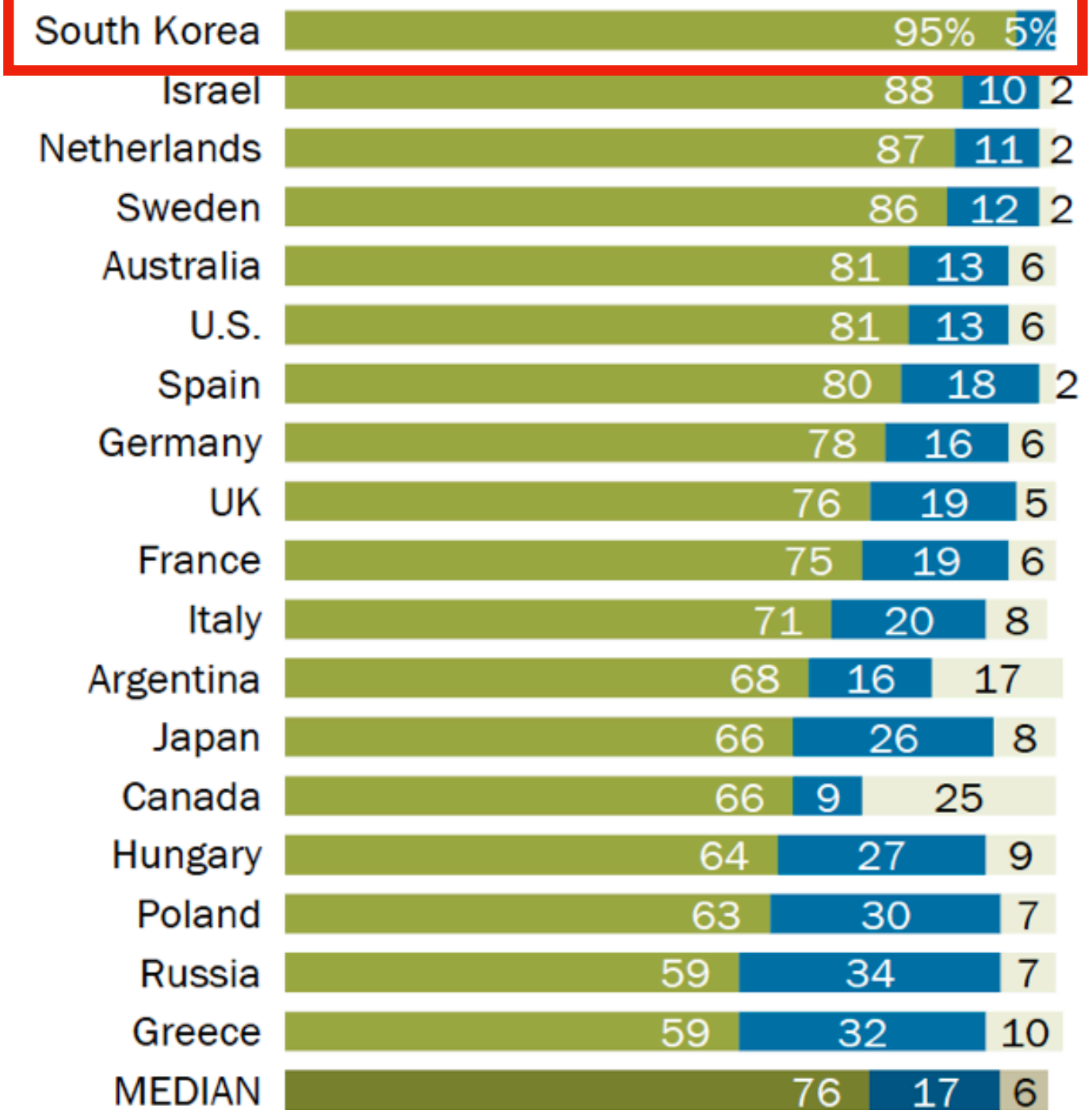
전자적 예방접종증명서 발급 필요

- 코로나19 예방접종을 시작하면서 접종 사실을 증명할 수 있는 예방접종 증명서 시스템이 필요함
- 종이증명서는 해외에서 위변조 사례가 다수 발생함에 따라 위변조 불가능한 전자증명서 시스템이 필요함
- 실시간 접종사실 검증과 편리한 휴대성을 위한 전자적 예방접종증명서 발급 여론 확산
- 개인의 민감한 의료 정보를 담고 있기 때문에 **익명화 기술을 이용한 인증 시스템**을 도입해야 하고 해외 국가와의 연계도 중요함
- 대한민국은 전세계에서 스마트폰 보급률이 가장 높고 국민들의 IT에 대한 기술 이해와 활용능력이 탁월함

% of adults who report owning ...

- A smartphone
- A mobile phone that is not a smartphone
- No mobile phone

Advanced economies



Design Goals

COOV의 설계



Issue

KDCA is the only authorized issuer in Republic of Korea



Wallet

Issued credential is only stored in user's own device



Verify

Anyone can verify other's credential
Integrity is secured by using blockchain and Decentralized Identity technology

개인의 선택에 따른 선택적 정보 제공

9:41

Sharing Settings

Required Information

Vaccine

Brand

Lot Number

Vaccination Series

Vaccination Date

Vaccination Country

Administered Centre

required

required

required

required

required

required

Additional Information

Full Name

Date of Birth

확인

9:41

QR

Time Left 15 seconds

Required Information

Vaccine

Brand

Lot Number

Vaccination Series

Vaccination Date

Country

Administered Center

Additional Information

Name

Date of Birth

Additional Information Settings

Global Certificate



Verified Information

Vaccine Dose / Vaccine Manufacturer

2st / Pfizer

Vaccine

COVID-19

Name

Undisclosed

Lot No.

CTMAV508

Date of Birth

Undisclosed

Date

March 28, 2021

Nationality

U.S.A.

My credentials

Verify Credentials

Settings

disclosing nationality only

Verified Information

Vaccine Dose / Vaccine Manufacturer

2st / Pfizer

Vaccine

COVID-19

Name

Smith, Paul

Lot No.

CTMAV508

Date of Birth

Undisclosed

Date

March 28, 2021

Nationality

U.S.A.

My credentials

Verify Credentials

Settings

disclosing name and nationality

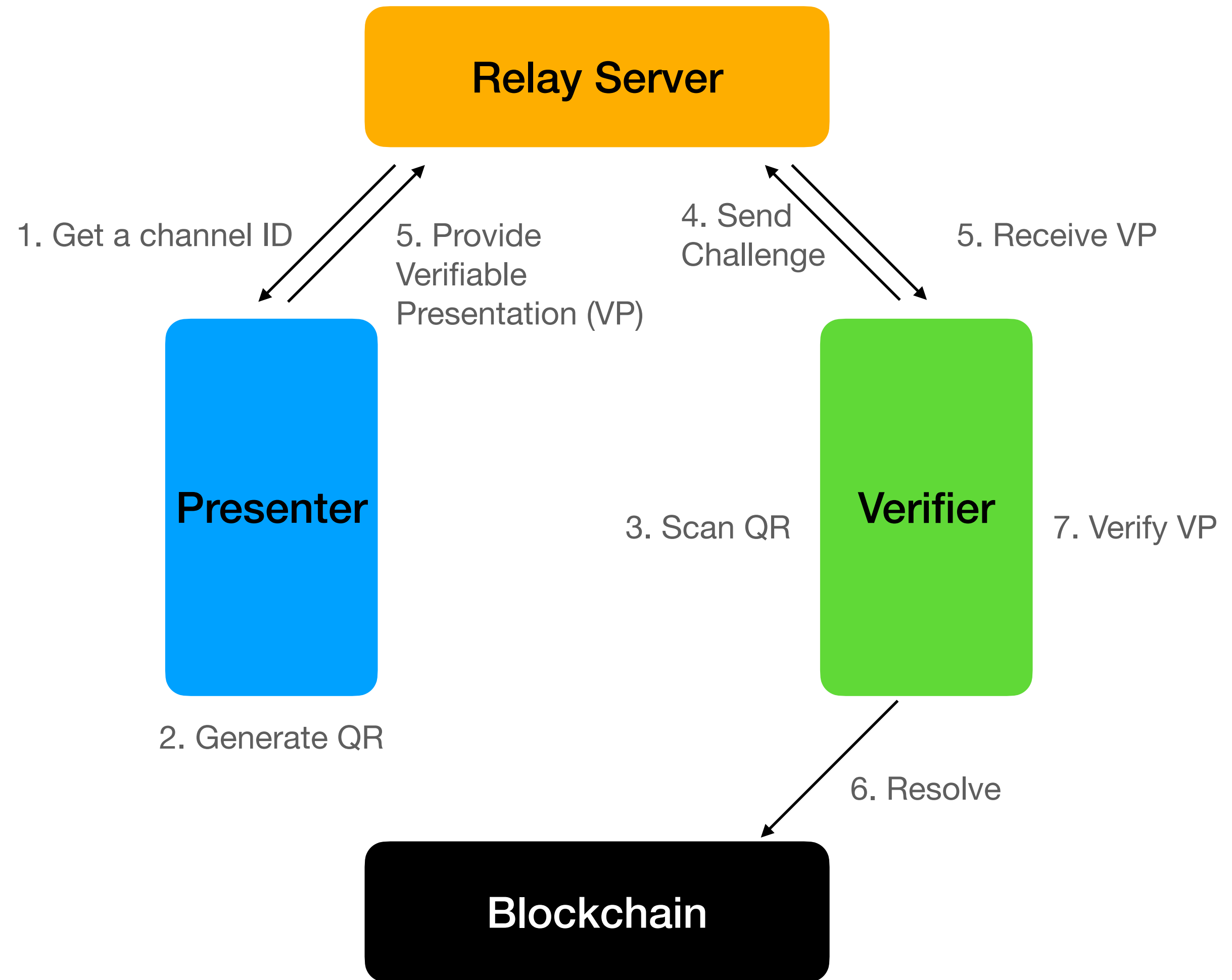
상호운영성을 위한 노력



did:infra:coov:PUB_K1_5LnLPSFL1ioJyA
TiTQ7jUzQJe1PqzEbBWyE8efzyn88TBz4w8N

자기주권신원을 위한 노력

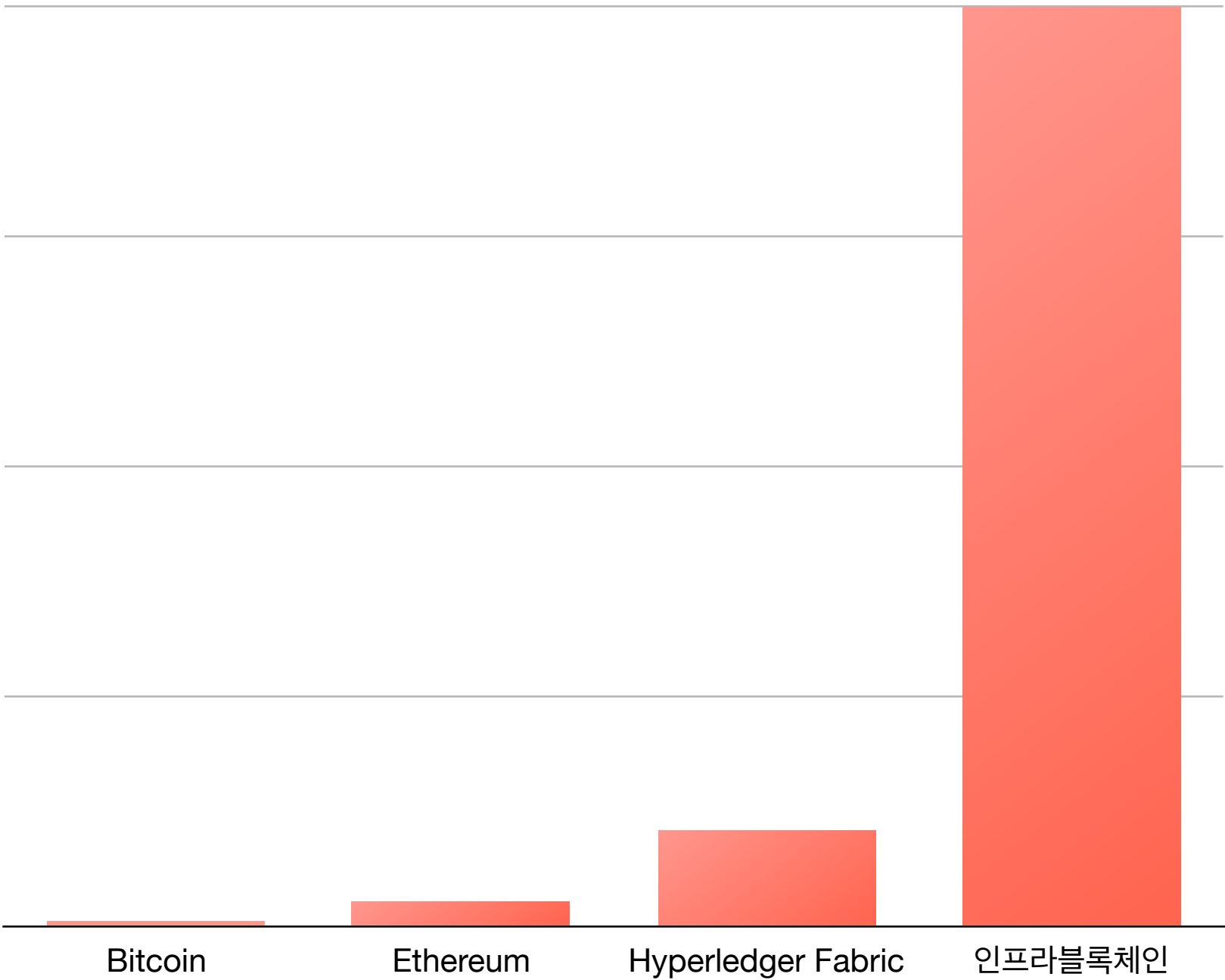
- DID가 사용자의 모바일 기기에서 직접 생성
- 본인인증 후 사용자가 제시한 DID를 시스템에 등록
- 이후 DID 기반 전자서명 시스템 (DID Auth)를 이용하여 서버와 통신
- 증명서(VC) 발급시 발급 서버에는 발급 기록만 남고, 발급된 증명서는 사용자의 기기에만 저장
- 사용자가 검증 받고자 할 때 검증자에게서 받은 Challenge와 Domain을 포함한 VP를 만들어 제출
- 검증자는 블록체인에서 DID Document를 가져와 VP의 전자서명 검증



고성능 블록체인 시스템 도입

2000 TPS

초당 처리 속도



Proof of Transaction

암호화폐 없이 공개형 블록체인을 만들 수 있는
특허받은 합의 알고리즘

VC Sample

```
{
  "vc": {
    "id": "did:infra:01:PUB_K1_5SzUXCYCz5gzrwxHzVxE6jFRnwPYzu9Vtk925q1BTJCGGq3r7Z",
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://coov.io/docs/vc/context/v1"
    ],
    "type": [
      "VerifiableCredential",
      "VaccinationCredential"
    ],
    "credentialSubject": {
      "vaccine": "COVID19",
      "brand": "Moderna",
      // 보안상 문제로 생략
    }
  },
  "sub": "did:infra:01:PUB_K1_6wJNmCJUuErqEXhw8WpEnbTALHtzQTXQFaUtMY3CkxTbB6uafA",
  "ver": "0.9",
  "iss": "did:infra:01:PUB_K1_6WGrvnuG7xFxCFA4dPrefh93HUdG7d1fjUQNsZXQ6JfRC6G3ZC"
}
```

Global Standardization

국제적 우수 사례로 기술 전파

2021년 9월 16일

UN ESCAP - WHO

Workshop on Digital COVID Certificate

2021년 9월 3일

BRICS Digital Health Summit

Smart Digital Vaccination Certification
Delivery Framework

2021년 8월 21일

ITU - WHO

Workshop on Digital Vaccination
Certificate



LF PUBLIC HEALTH

March 31, 2021

Dear KDCA Commissioner Jeong Eun Kyeong and Blockchain Labs CEO Um Jee Yong,

We are delighted to hear that KDCA is the first national public health authority to launch a blockchain-based COVID-19 vaccination verification system using the W3C Verifiable Credential standard. We wish both KDCA and Blockchain Labs every success with its launch. I would also like to explore how we, Linux Foundation Public Health (LFPH), can collaborate with you in this important work at a global level.

LFPH, as part of the Linux Foundation, is an open community that works with leading tech companies and public health authorities like yourselves, harnessing open source software to combat COVID-19 and to assist health authorities and public health globally. One of our vibrant community's focuses is verifiable vaccination credentials, and we are examining further areas where we can support health authorities and their tech partners. Therefore, Linux Foundation Public Health would like to request KDCA and Blockchain Labs join as members and contribute code to the LFPH initiative, in order to establish the technology that will be used as the global standard for verifiable COVID-19 vaccination credentials.

It would be an incredible service for KDCA and Blockchain Labs to contribute code to the LFPH initiative to combat COVID-19 around the world. This would open up opportunities for KDCA to communicate with health authorities in other countries on its use. Contributing code to a Linux Foundation project is very prestigious, as we are selective in choosing only the best codebases.

We would of course ensure there is substantial recognition, promotion and publicity globally on your contribution, your code base, and on the exceptional work you are doing in this area.

Please be aware that when an organization offers to contribute code to LFPH, our Technical Advisory Council takes it through the governance and due diligence process in order to accept the project. From what we have seen and heard of your software, we imagine this would be a straightforward process. We are excited to add that the COVID-19 Credentials Initiative (CCI) has joined LFPH, leading our work in introducing your software as a global standard.

We look forward to making a global impact together with KDCA and Blockchain Labs.

Sincerely,

Brian Behlendorf
Executive Director, Linux Foundation Public Health



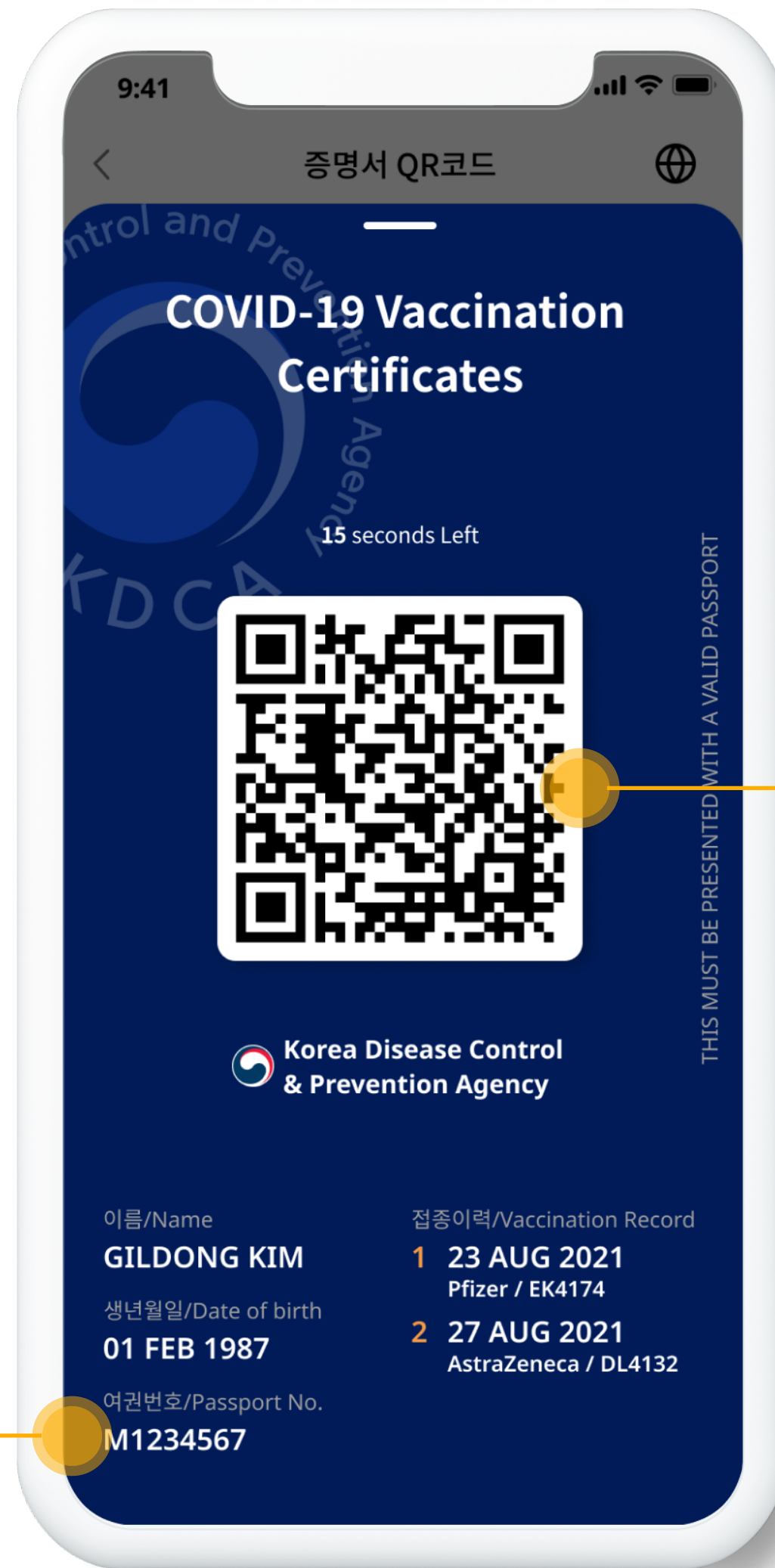
리눅스 재단에서 받은
공식 기술 지원 요청

International Usage

접종증명서 국제화

여권 정보 연동

외교부 여권 정보 시스템과의 연동을 통해 국민들이 해외 여행 시 여권과 함께 제시할 수 있는 영문 이름과 여권 번호 제공



국제 표준 준수

전세계적으로 가장 최신의 국제 표준을 준수하여 여러 나라들과 원활한 연동 가능



Statistics

15.78 M

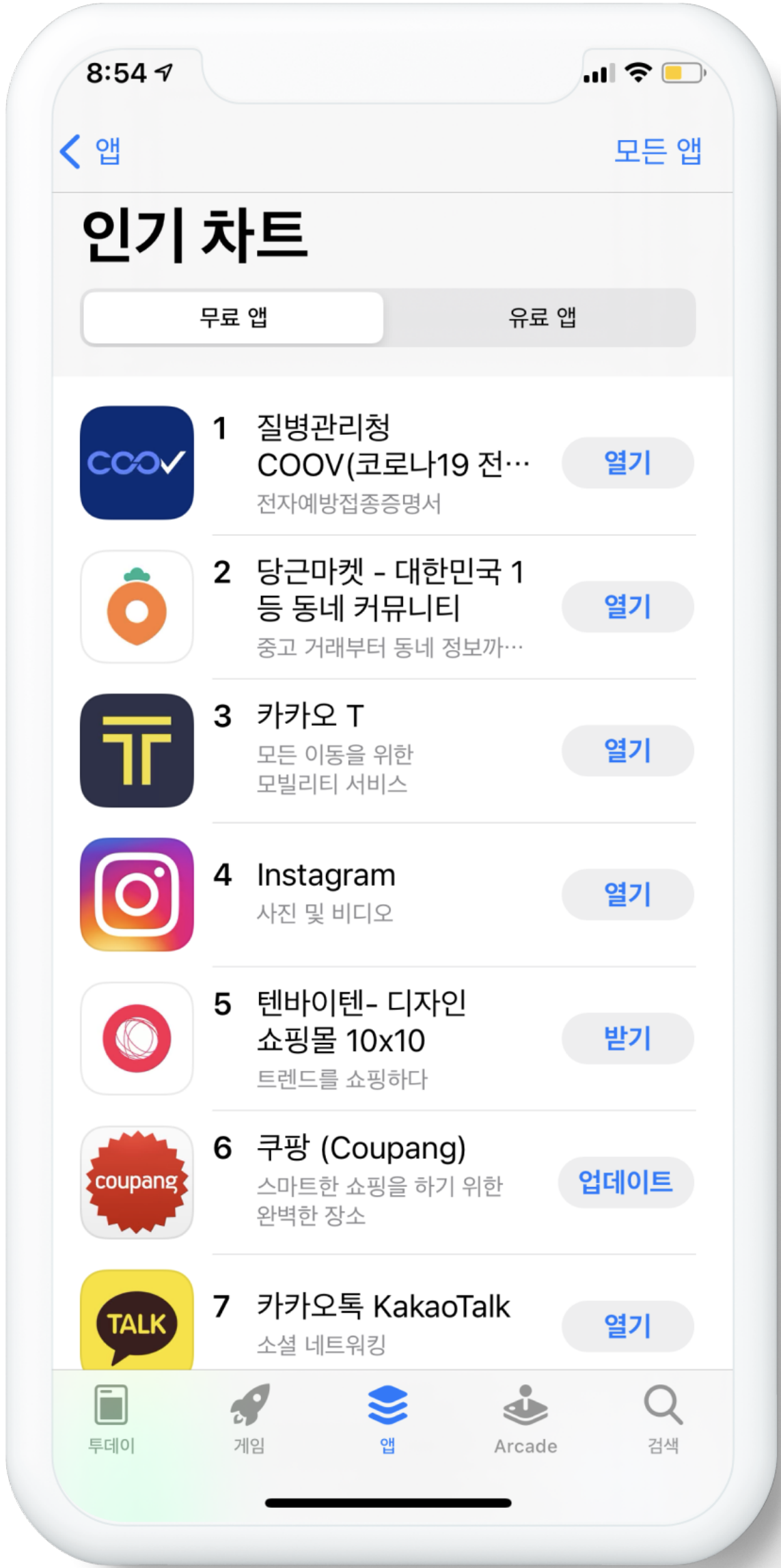
Downloads

141M

Issued Credentials

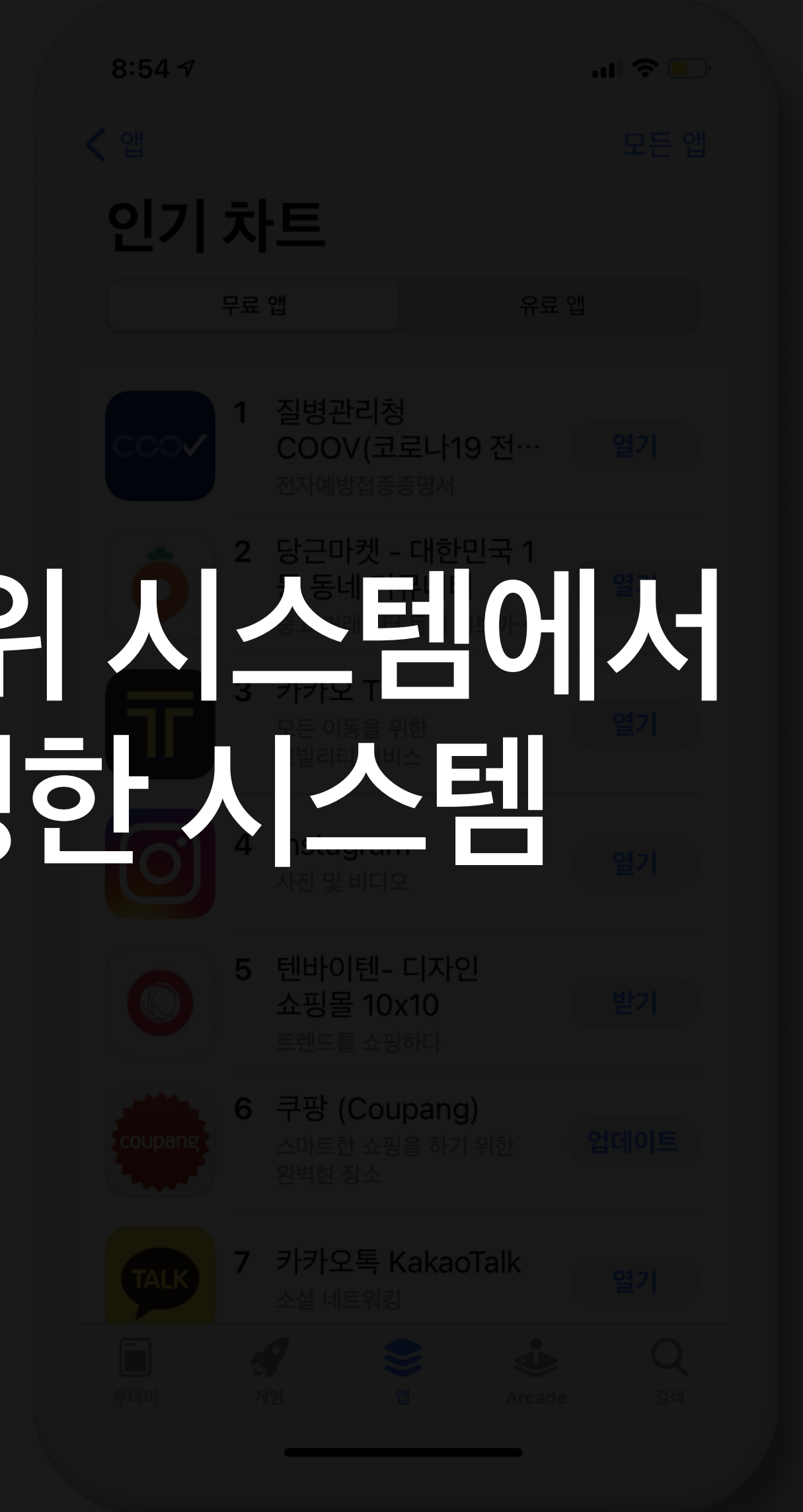
632M

Verifications



사용자가 스스로 신원 정보를 통제하는

자기주권 신원 (SSI) 모델이 국가 단위 시스템에서 가능하다는 것을 세계 최초로 증명한 시스템



Statistics

13.79M 14M 572M

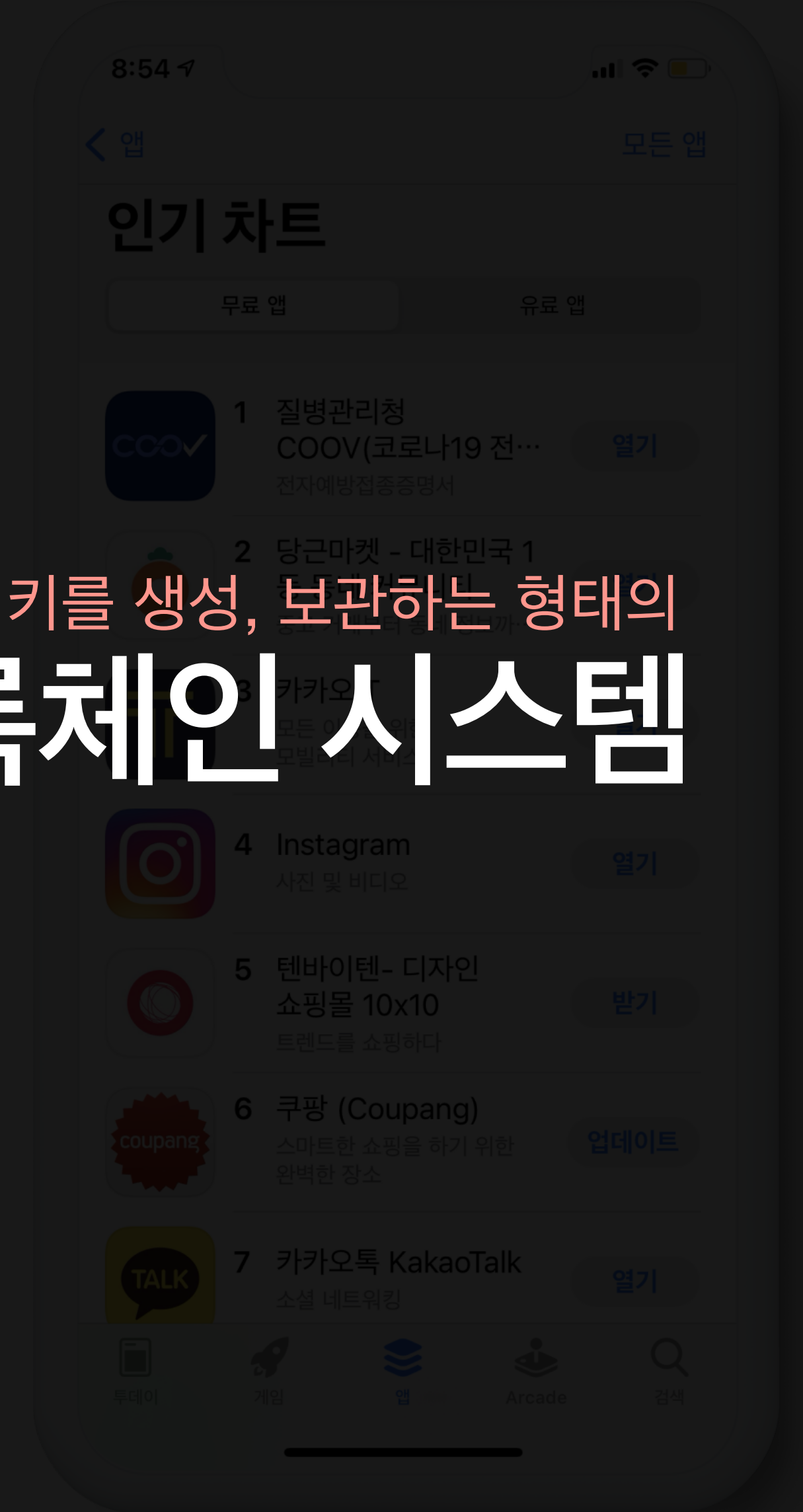
전세계에서 가장 큰 규모의 정부 블록체인 시스템

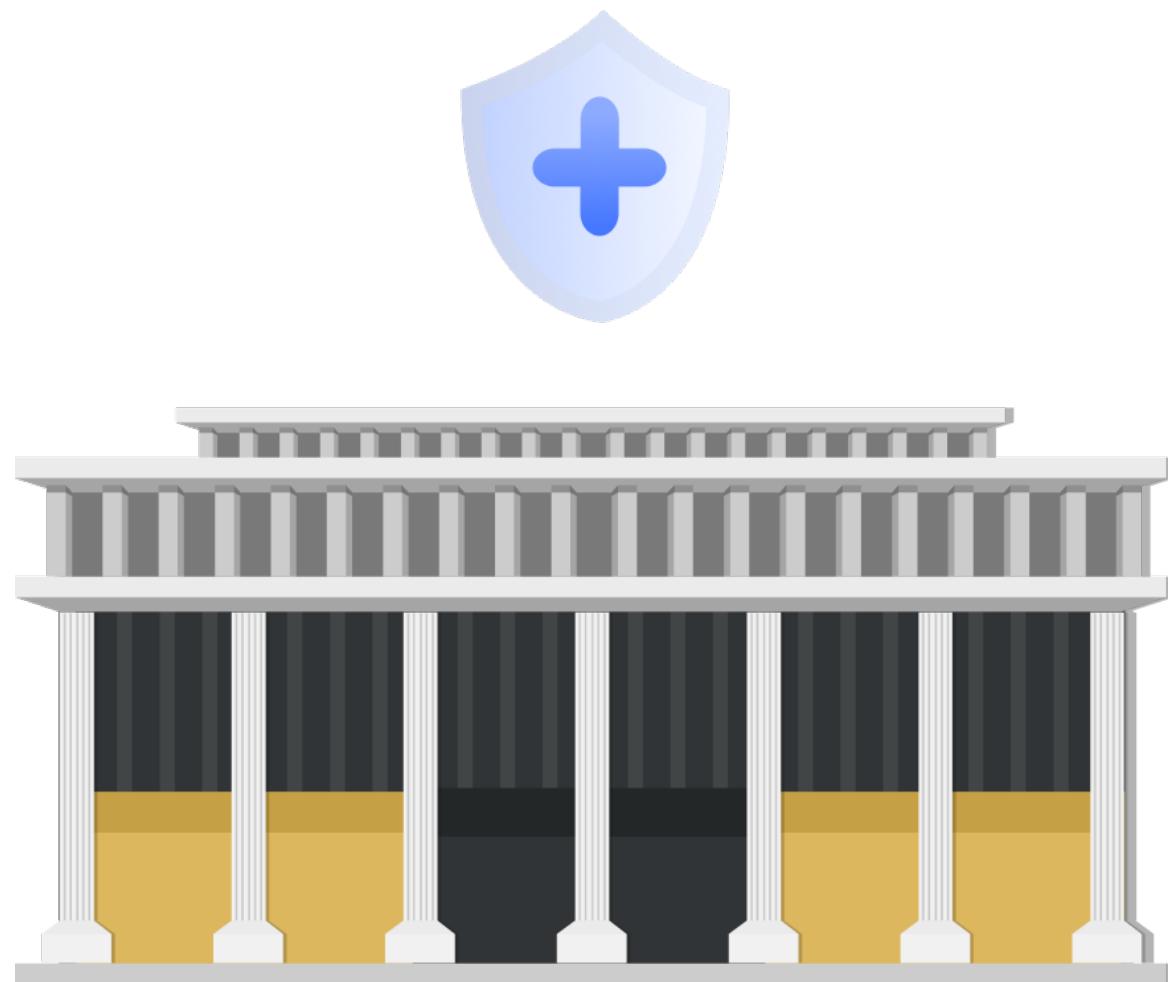
사용자가 직접 키를 생성, 보관하는 형태의

Downloads

Issued Credentials

Verifications





Root of Trust

Government agencies role as a root of trust to provide citizens' convenience and enhance privacy.



Self-Sovereignty

Provide secure system so that users can preserve ownership of personal and medical data

“Users own the data they create”

Thank you

Contact

Jaehoon Shim | Head of Product
Blockchain Labs, Inc.
jshim@infrablockchain.com