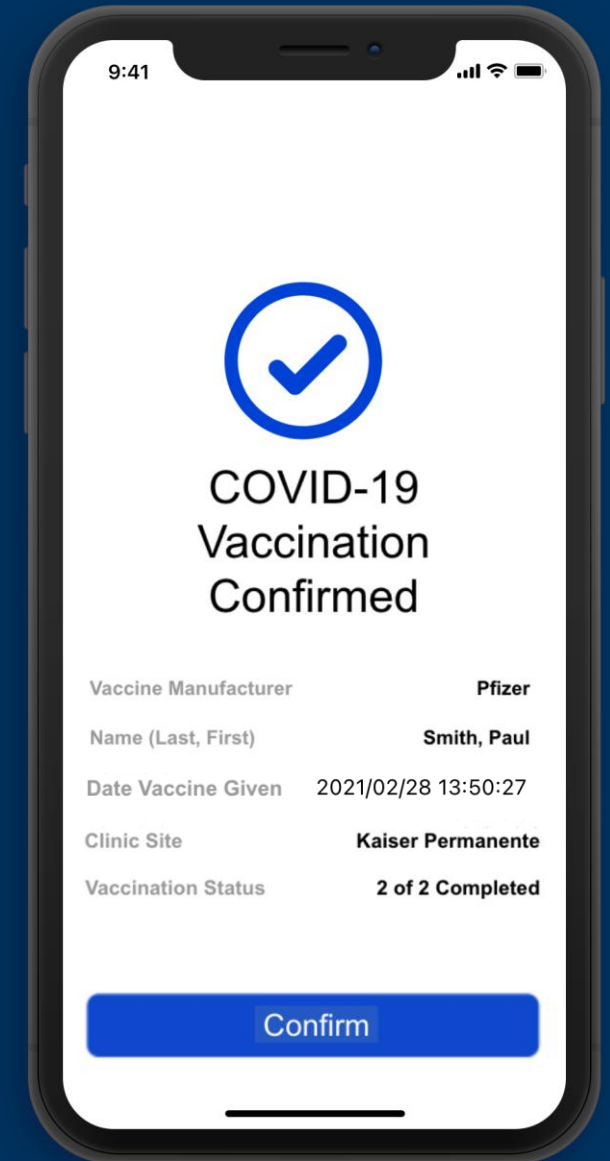


PASS INFRA: Blockchain-based COVID-19 Vaccination Verification & Management System



A Need for the Vaccination Verification System

- With COVID-19 vaccination efforts underway, a system to verify individual's COVID-19 vaccination records is needed at all levels of society
 - Ensure the safe return to the normalcy
 - Resume international travels
 - Return to workplaces
- Because of the sensitive nature of personal information included in the vaccination records, the verification system must be able to provide selective disclosure option on which data is shared

A Need for the Vaccination Management System

- Vaccinated individuals should be able to report any adverse events from the vaccines they have taken
- A management system should enable follow-up measures to be carried out quickly, in the case of a vaccine's reported manufacturing and/or distribution problem
- Individuals should be able to receive administrative and other emergency alerts, including a reminder for any subsequent shots

Blockchain Labs's Blockchain-based Digital COVID-19 Vaccination Verification System (PASS INFRA)

- Allows the government to effectively manage vaccinated individuals, and promptly respond to emergency situations
- Ensures the safe protection of personal information through the enhanced data security using the blockchain and DID technology
- Can also store and manage other identification credentials, **potentially functioning as a global ID verification system**

Product Concept

PASS INFRA for Individuals

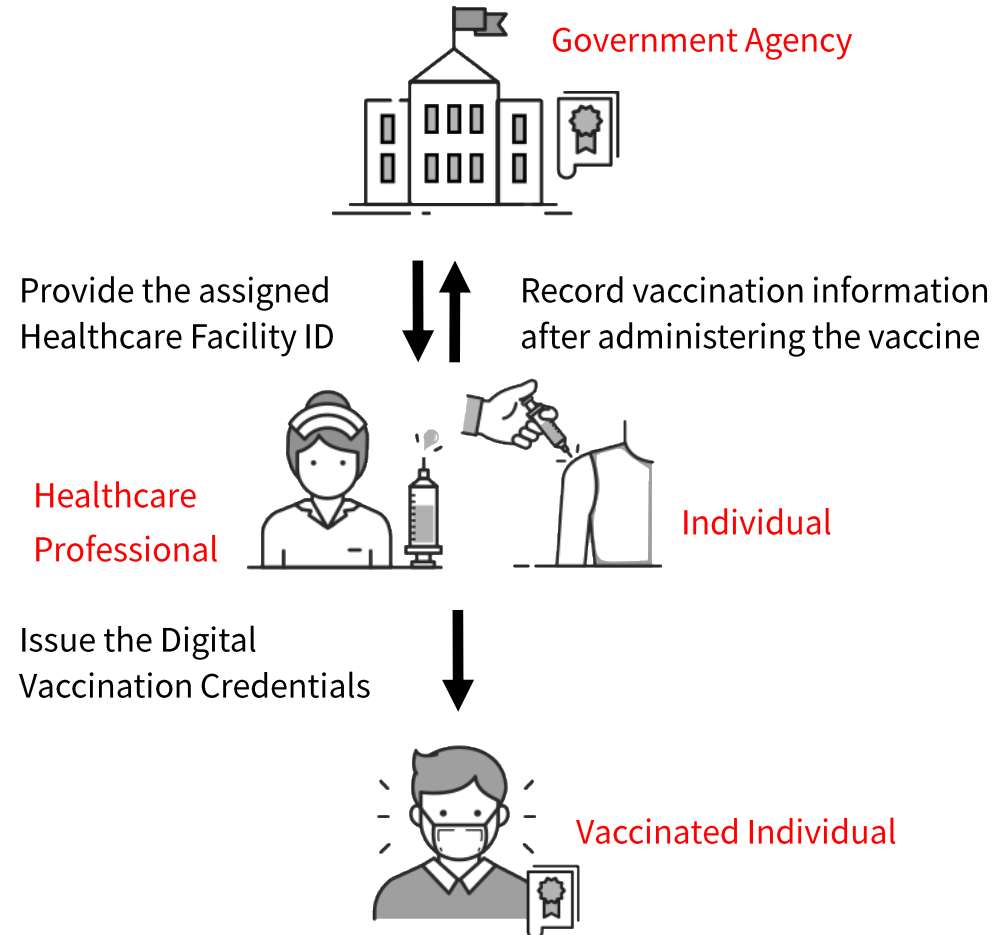
- Download & Install PASS INFRA from Google Play or App Store
- Verify Identity
- Submit the digital vaccination credentials
- Verify each others' digital vaccination credentials
- Report abnormalities, if any
- Receive emergency alerts and contact the responsible government agency

PASS INFRA for Healthcare

- Download & Install PASS INFRA from Google Play or App Store
- Verify authorized vaccination clinic credentials
- Identify the vaccine information by scanning its QR code
- Send the digital vaccination credentials to the vaccinated individual by scanning his QR code
- Send the vaccination information (who got which vaccine) to the responsible government agency

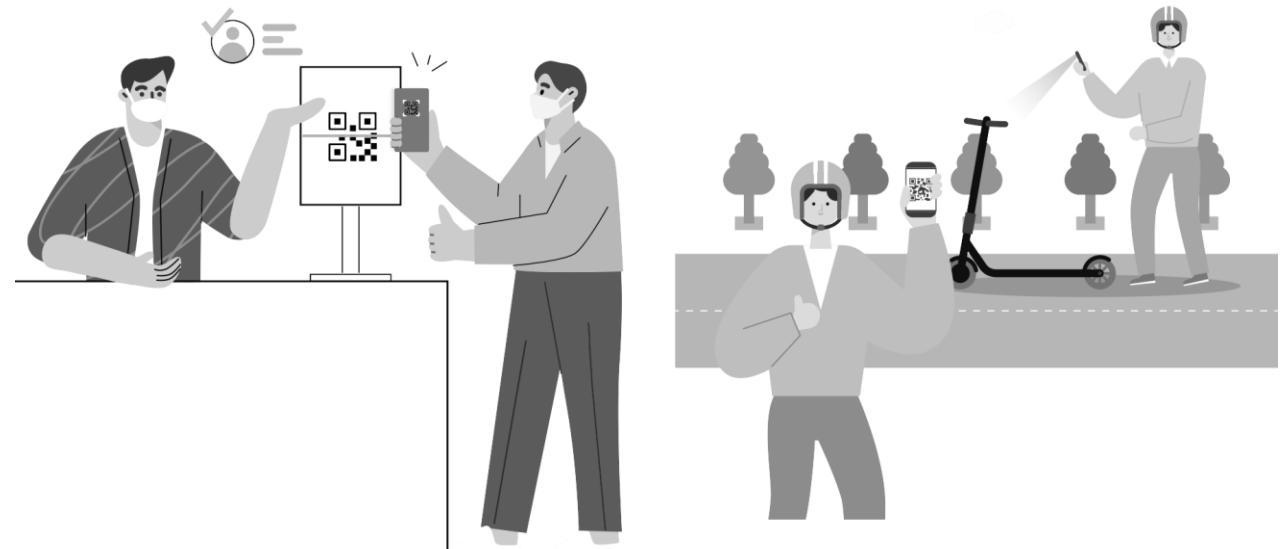
Issuing & Using the Digital Vaccination Credentials

Issuing the Digital Credentials



Using the Digital Credentials

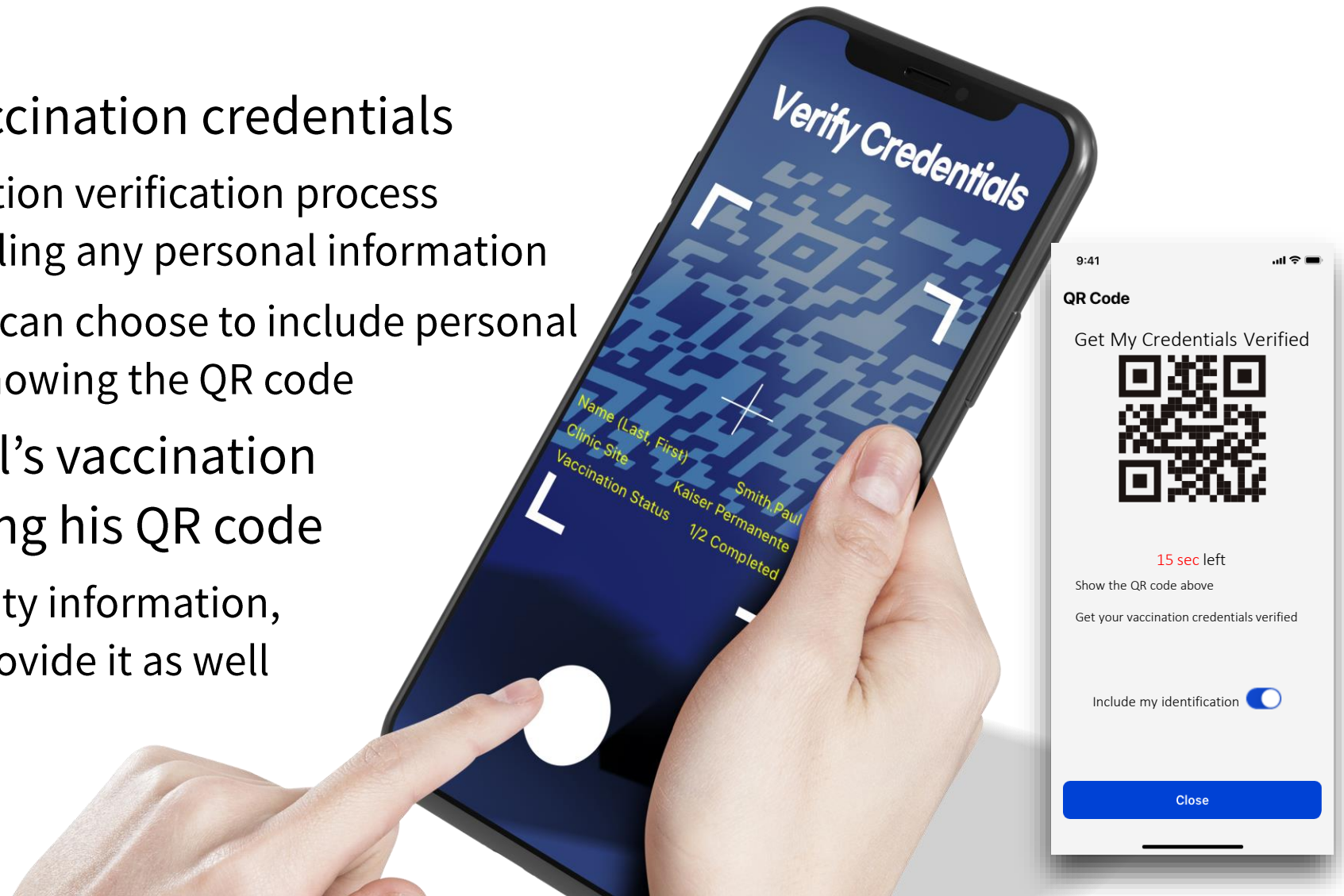
Get the digital vaccination credentials verified by scanning each other's QR code



*The proof of vaccination can be verified without exposing any personal information

PASS INFRA for Individuals - Vaccination Verification

- Submit the digital vaccination credentials
 - Complete the vaccination verification process without directly revealing any personal information
 - If needed, individuals can choose to include personal identification when showing the QR code
- Verify other individual's vaccination credentials by scanning his QR code
 - Cannot view his identity information, unless he agrees to provide it as well



PASS INFRA for Individuals - Vaccination Verification

- Review the information of the vaccine taken
- Personalized post-vaccination management
 - Alert future vaccination schedule
 - Report abnormalities, if any
- Contact the vaccination clinic and/or the responsible government agency

9:41

Review My Vaccination Record

Vaccine Information

Batch Number	NDC59267-1000-1
Manufacturer	Pfizer
Clinic Site	Kaiser Permanente
Clinic ID	SNI029-1192
Administrator ID	IN129SLMA910-2
Vaccination Status	1 of 2 Completed
Follow-up Note	2nd Vaccination Needed by Feb 04, 2021

9:41

Alerts

Emergency Alert

Problem detected from your vaccine batch
1 hour ago

Read Alerts

10 Days left until your 2nd Vaccination
2021/03/01

Please complete the Vaccine Allergy Assessment before your 2nd Vaccination
2021/02/27

You need to get vaccinated!
2021/02/23

Post-Vaccination Care Instructions

- Contact the government agency
- Contact the Vaccine Clinic

9:41

Self-Assessment Report

Do you have a fever, over 37.5°C (100.4°F)?

Yes No

Do you have any cough symptoms?

Yes No

Are you suffering from shortness of breath?

Yes No

Do you have excessive mucus?

Yes No

Are you experiencing sore throat?

Yes No

Close

PASS INFRA for Healthcare Facilities - Creating Vaccination Credentials

- Verify the institution's authorized vaccination clinic credentials
- Manage clinic's health professionals registry
 - Register on-site professionals who are responsible for administering a vaccine
- Identify the vaccine information before administering the vaccine
 - Scan its Barcode
- Issue vaccination credentials to the recipient once the vaccine is administered
 - Scan his QR code
- Submit the vaccination information to the government agency



+

9:41

Vaccine Information

Batch Number	NDC59267-1000-1
Clinic Site	Kaiser Permanente
Vaccine Type	AZD1222

Patient Information

Name (Last, First)	Smith, Paul
Date of Birth	1984/05/27
Clinic Site	Kaiser Permanente

[Record on the Government Database](#)

Record on the
→ Government
Database

PASS INFRA Adoption

- Blockchain Labs is working with government agencies and international organizations to develop the global standards for the credentials verification system, and deploy an interoperable solution
- South Korea's Disease Control and Prevention Agency has modified PASS INFRA system to launch the version that suits their needs, named COOV
- PASS INFRA has been recognized and is currently being reviewed by the technical advisory committee of the Linux Foundation
 - PASS INFRA will continue to be modified to fit the local government's needs and ultimately become the underlying technology for a **globally interoperable credentials verification system**



KDCA



Linux Foundation
Public Health

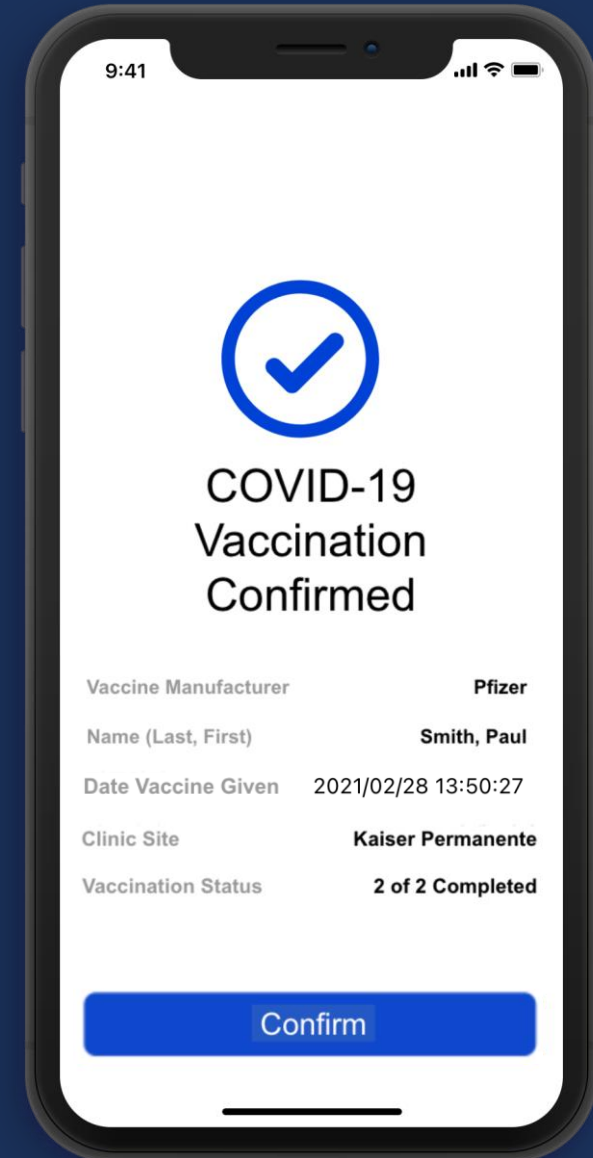
About Blockchain Labs Inc.

-
- A vertical timeline with a central blue line and four dark blue circular markers. The years 2013, 2017, 2020, and 2021 are listed on the left side of the line. To the right of each marker is a text description of an event. The text for 2017 is highlighted in yellow.
- 2013 ● Founded
 - 2017 ● Patented PoT (Proof of Transaction) consensus mechanism
Public blockchain without cryptocurrency
 - 2020 ● Blockchain-based Medical Hemp Production and Distribution tracking system
 - 2021 ● PASS INFRA: Blockchain-based COVID-19 Vaccination Verification & Management System

Notable Shareholders

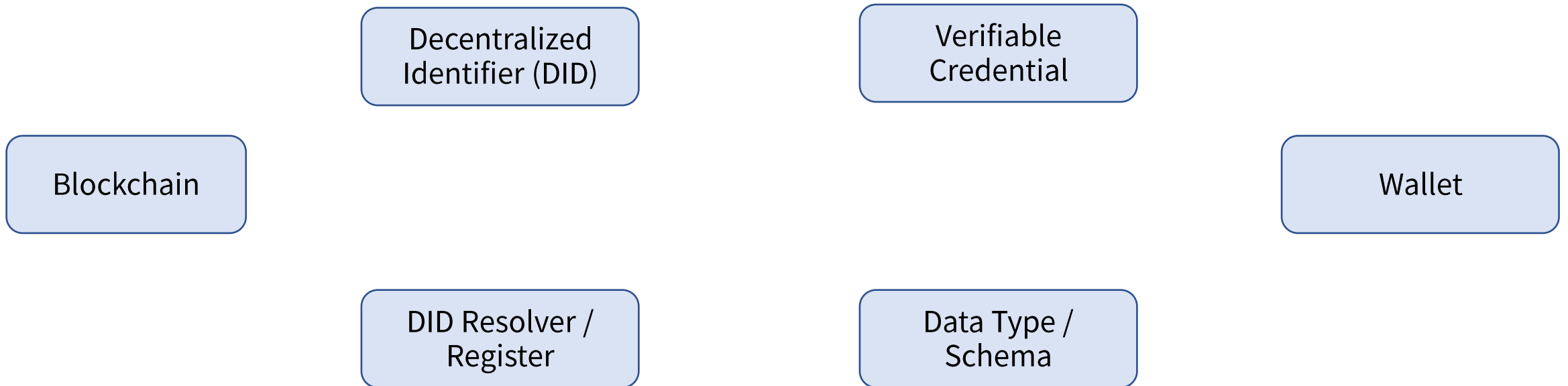
Kiseok Park – Chairman of Sigong Tech, the leader of specialized exhibition, cultural and interior industry in Korea
Soonbaek Kwon – Chairman of Tera Science, a publicly traded advanced-biotech company in Korea

PASS INFRA Technical Pack

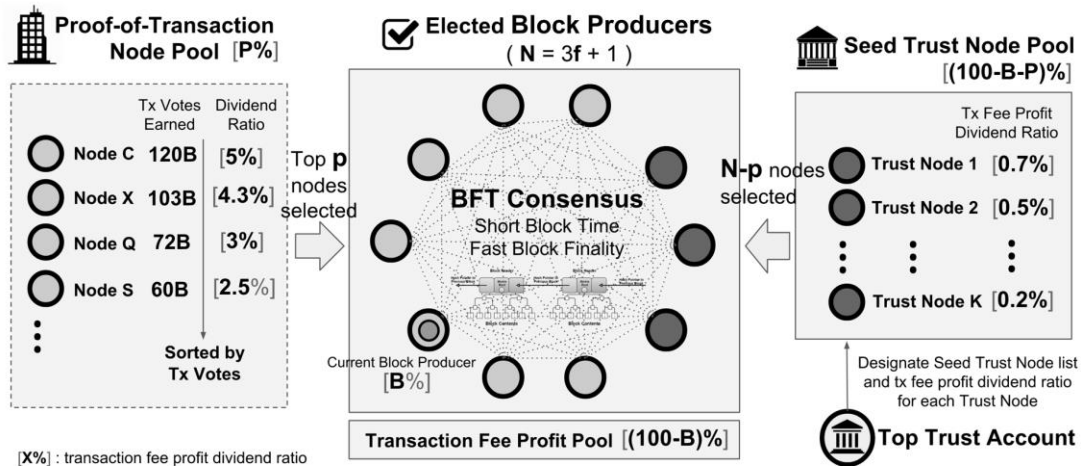


Overview

Technology Components



The blockchain designed for government usage



1. Blockchain without native cryptocurrency
2. Globally scalable design
 1. Public blockchain
 2. Permissioned block producers
3. Flexible Blockchain Governance
4. Proof-of-Transaction (PoT) consensus mechanism
5. High-performance blockchain transaction processing
6. Easy to install
 - ✓ Only need to have the latest update from Github

Overview of Proof of Transaction
<https://infrablockchain.com/en/technology/#proof-of-transaction>

For more information, please visit
<https://infrablockchain.com/en/technology>

Blockchain

Public, upgradable blockchain

	Public Blockchain	Private Blockchain	Infra Blockchain	Note
Representative Protocols	Bitcoin, Ethereum	Hyperledger Fabric, Corda	InfraBlockchain	<ul style="list-style-type: none"> Designed to admit the role of trusted entities to build up trust, but not compromise essential values provided by blockchain technology
Working Mechanism	Mining, Staking	Single Authority, Consortium	Trusted Entities (Government, Enterprise)	
Consensus Algorithm	PoW, PoS	RAFT (Fabric), BFT-SMaRt (Corda)	PoT-aBFT (Proof-of-Transaction asynchronous BFT)	<ul style="list-style-type: none"> Hard to say Consensus Algorithm which doesn't guarantee BFT satisfies the requirements of Blockchain technology
Byzantine Fault Tolerance	○	× (Fabric), △ (Corda; Applied to Notary)	○ (At least 4 nodes, but extensible)	
Network Type	Permissionless	Permissioned	Flexible	<ul style="list-style-type: none"> Designed to work by trust entities' participation unlike cryptocurrency (public) or off-chain regulations (private) Support flexible network construction including permissioned · semi-permissioned · permissionless Specialized in Local currency service by Fiat-based scheme
Self-issued Cryptocurrency	○ (Essentially Required)	×	×	
Cryptocurrency Volatility	Severely Volatile due to no backed assets	- (Not required)	Stable backed by Fiat Reserve of Trust Entities	
Transaction Throughput	7 TPS (Bitcoin) 20 TPS (Ethereum)	3500 TPS (Fabric v2.x)	4000+ TPS	<ul style="list-style-type: none"> Higher performance in semi-permissioned or permissionless setup compared to permissioned
Transaction Anonymity	△	△	○	<ul style="list-style-type: none"> Provides selective anonymity so as to use in vote or micropayment with transparency
Key Messages	<ul style="list-style-type: none"> Limited possibilities to adopt in enterprise due to low speed, uncontrollability and volatile cryptocurrency 	<ul style="list-style-type: none"> Incomplete implementation of blockchain technology Not extensible in long-term development 	<ul style="list-style-type: none"> Stable token backed by trust entities' reserve Utilize the benefits of public blockchain as well as overcome the limitations in enterprise environment 	

W3C Compliant DID / VC

Sample DID Document (did:infra)

Sample VC

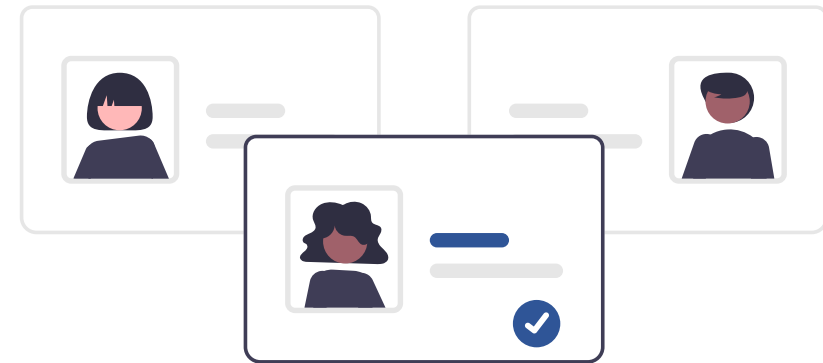
```
Object {  
  "didDocument": Object {  
    "@context": "https://www.w3.org/ns/did/v1",  
    "authentication": Array [  
      "did:infra:vapptest1  
      :PUB_K1_7nxEa8qHEiy34dpuYH4yE2zRWaAoeT1gsdTnh8n5ikapZZ  
      rzjx#controller",  
    ],  
    "id": "did:infra:vapptest1  
    :PUB_K1_7nxEa8qHEiy34dpuYH4yE2zRWaAoeT1gsdTnh8n5ikapZZrz  
    jx",  
    "service": Array [  
      Object {  
        "id": "did:infra:vapptest1  
        :PUB_K1_7nxEa8qHEiy34dpuYH4yE2zRWaAoeT1gsdTnh8n5ikap  
        ZZrzjx#service-1",  
        "serviceEndpoint": "https://infradid.com/pk/3/mysvcr4",  
        "type": "MessagingService",  
      },  
    ],  
    "verificationMethod": Array [  
      Object {  
        "controller": "did:infra:vapptest1  
        :PUB_K1_7nxEa8qHEiy34dpuYH4yE2zRWaAoeT1gsdTnh8n5ikap  
        ZZrzjx",  
        "id": "did:infra:vapptest1  
        :PUB_K1_7nxEa8qHEiy34dpuYH4yE2zRWaAoeT1gsdTnh8n5ikap  
        ZZrzjx#controller",  
        "publicKeyHex":  
        "037e84547231650e816a32eb5b79028e71ac7459bbcd8e81e66  
        97ac9022e64a407",  
        "type": "EcdsaSecp256k1VerificationKey2019",  
      },  
    ],  
  },  
  "didDocumentMetadata": Object {},  
  "didResolutionMetadata": Object {  
    "contentType": "application/did+ld+json",  
  },  
}
```

```
{  
  "vc": {  
    "@context": [  
      "https://www.w3.org/2018/credentials/v1"  
    ],  
    "type": [  
      "VerifiableCredential",  
      "Vaccination"  
    ],  
    "credentialSubject": {  
      "vaccine": "아스트라제네카",  
      "vaccineTime": "1",  
      "vaccineYmd": "20210323",  
      "vaccineOrg": "강남구 보건소",  
      "lotNum":  
    },  
  },  
  "sub": "did:infra:01  
  :PUB_K1_6XpzKXC8amUN1AQccYcVpRMBajq8b3HHhYJVZ4uJQ7pW9TJvnr  
  ",  
  "nbg": 1616762884,  
  "iss": "did:infra:01  
  :PUB_K1_5LnLPSFL1ioJyATiTQ7jUzQJe1PqzEbBWyE8efzyn88TBz4w8N  
  ",  
  "id": "did:infra:01  
  :PUB_K1_5LJ248TiQjd98078zxcvjwenf5ji2Wd9kfkWldfzyn8j89UQJ  
  "  
}
```


Verifiable Credentials - Verification

Verification Checklist

- Authenticity of Issuer (by resolving Issuer's DID)
- Authenticity of Holder (by resolving Holder's DID)
- Compliance to Schema (by using JSON-formatter)
- Integrity of Credentials (by verifying JWT proof)
- Audience of Presentation (by verifying *aud* property of JWT)





Universal Resolver - Interoperability

- Protocol for interoperability
- To discover and retrieve DID Document from multiple verifiable data registry
- COOV includes Universal Resolver module within mobile application which lets mobile agent can directly access blockchain and retrieve did documentation and derive the current status.
- COOV also can resolve 40+ other DID methods registered, including Sovrin. (<https://github.com/decentralized-identity/universal-resolver>)

Messaging

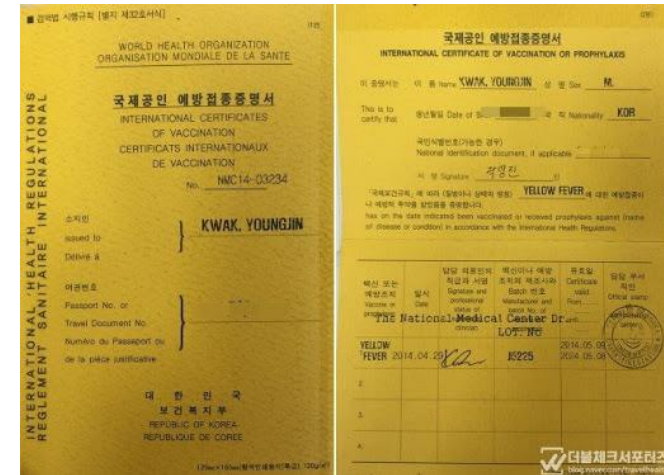
Peer-to-peer messaging using One-Time QR.

- Holder receives a channel id to relay server and display as QR.
- Verifier scans the QR to join the relay server.
- Once someone joins the relay server, the server no longer lets anyone to join.
 - To ensure only executing a one-time transfer to verifiers once authorized by Holder.
- Then the holder and the verifier will process the verification steps.
(Challenge-response for Verifiable Presentation)
- When the process is finished, result of the verification will appear on both screens.

WHO / HL7 FHIR compliant

The data schema used in Verifiable Credentials is initially designed to be HL7 FHIR compatible for global interoperability.

We also reference global movements such as WHO's Interim guidance for developing a Smart Vaccination Certificate



11.7.3 Resource Content

Name	Flags	Card.	Type	Description & Constraints
Immunization	TU		DomainResource	Immunization event information Elements defined in Ancestors: id, meta, im, modifierExtension
identifier		0..*	Identifier	Business Identifier
status	1	1..1	code	completed entered-in-error not-done Immunization Status Codes (Required)
statusReason		0..1	CodableConcept	Reason not done
vaccineCode		1..1	CodableConcept	Immunization Status Reason Codes (Examp Vaccine product administered
patient		1..1	Reference(Patient)	Vaccine Administered Value Set (Example) Who was immunized
encounter		0..1	Reference(Encounter)	Encounter immunization was part of Vaccine administration date
occurrence		1..1		
occurrenceDateTime			dateTime	
occurrenceString			string	
recorded		0..1	dateTime	When the immunization was first captured i
primarySource		0..1	boolean	Indicates context the data was recorded in
reportOrigin		1	CodableConcept	Indicates the source of a secondary reports Immunization Origin Codes (Example)
location		0..1	Reference(Location)	Where immunization occurred
manufacturer		0..1	Reference(Organization)	Vaccine manufacturer
lotNumber		0..1	string	Vaccine lot number
expirationDate		0..1	date	Vaccine expiration date
site		0..1	CodableConcept	Body site vaccine was administered Codes for Immunization Site of Administrat
route		0..1	CodableConcept	How vaccine entered body Immunization Route Codes (Example)
doseQuantity		0..1	SimpleQuantity	Amount of vaccine administered
performer		1	0..*	BackboneElement Who performed event
function		1	0..1	CodableConcept What type of performance was done Immunization Function Codes (Example)
actor		1	1..1	Reference(Practitioner PractitionerRole Organization) Individual or organization who was perform
note		1	0..*	Annotation Additional immunization notes

Interoperability

Interoperability



As a member of LFPH and CCI, we will continue to put effort on making globally interoperable schema and once the standard is set, we can adopt without any effort.



As a member of DIF, we keep the W3C standards and utilize libraries such as universal resolver which allows us to interoperate with 50+ other members.



We plan to join ToIP anytime soon so that we can follow the governance and schema that is discussed in global SSI community.