

LACCHAIN

The use of blockchain and verifiable credentials for vaccination certificates

LACChain Global Alliance led by IDB Lab
Marcos Allende Lopez – IDB Specialist & Technical Leader of LACChain
CONECTATON LACPASS – MAY 30th 2022

IDB | LAB

Agenda

1. Quick recap of blockchain
2. LACChain and LACNet: the largest permissioned-public blockchain in the world
3. Using the LACChain blockchain as Public Key Directory
4. Using Verifiable Credentials for Vaccination Certificates
5. Understanding the demo
6. Demo



LANGCHAIN

1. Quick recap of blockchain



Definition

Blockchain is a registry of information with the following properties:



DECENTRALIZED



CHRONOLOGICAL

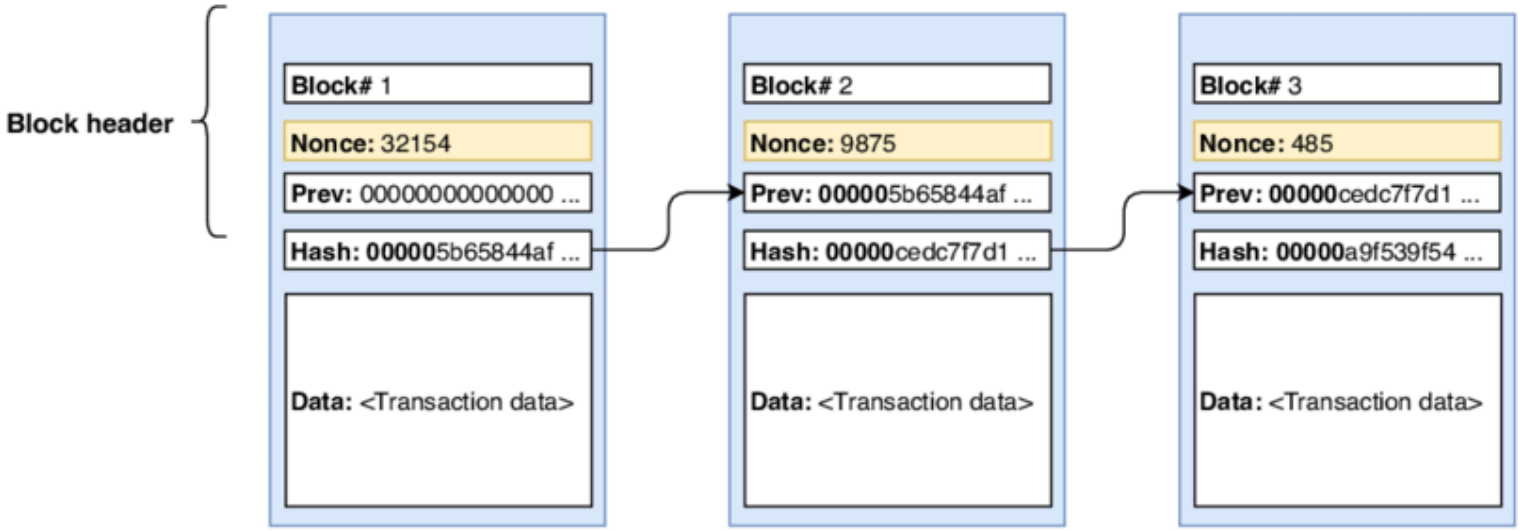


IMMUTABLE



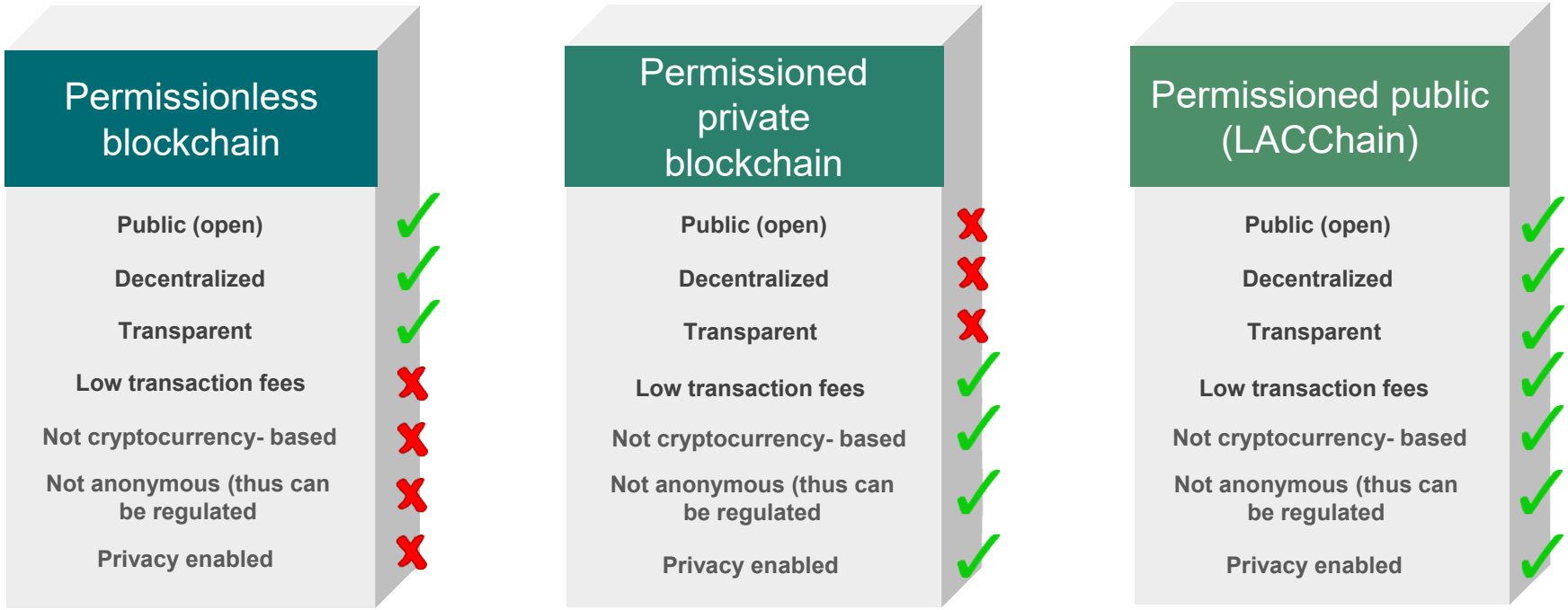
CONSENSUATED

Graphical example



Note: *The fields of* ***Nonce, Prev,*** *and* ***Hash*** *contain arbitrary values*

Types of blockchain networks

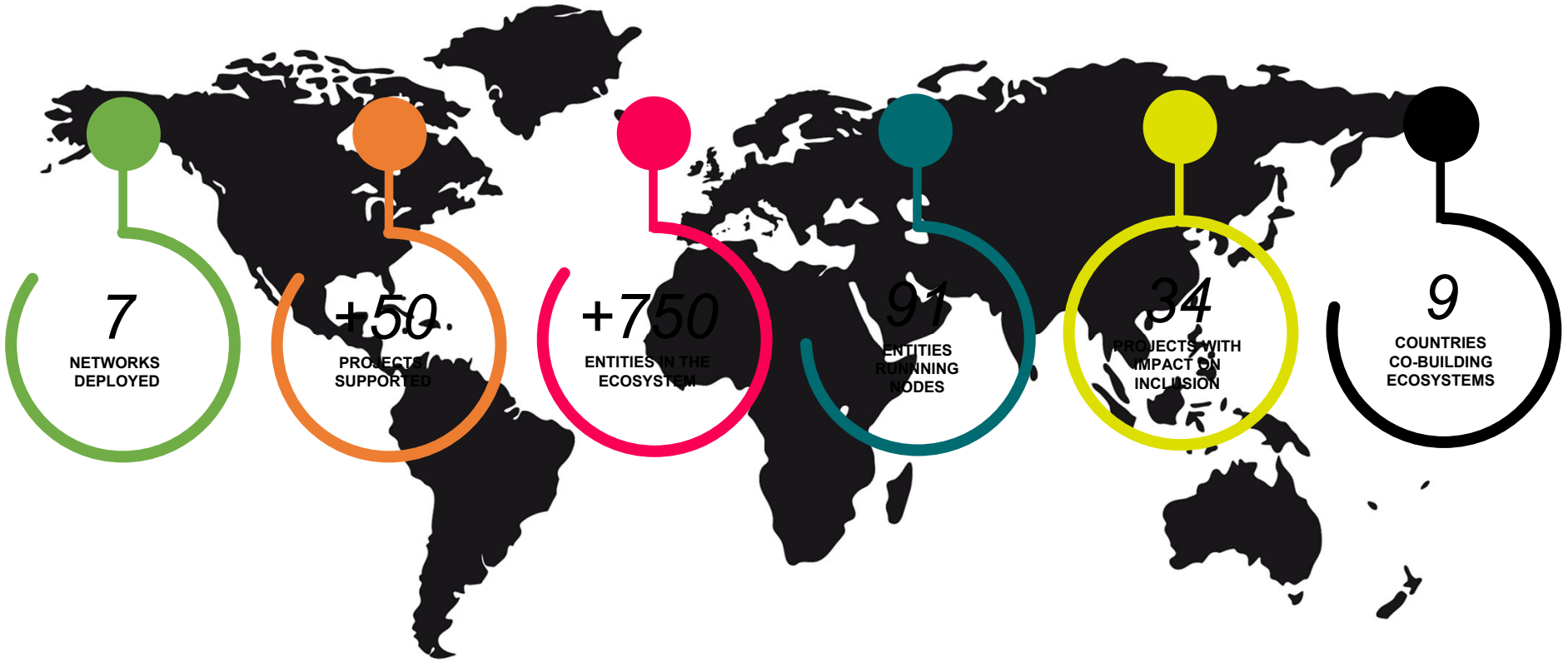


LACCHAIN

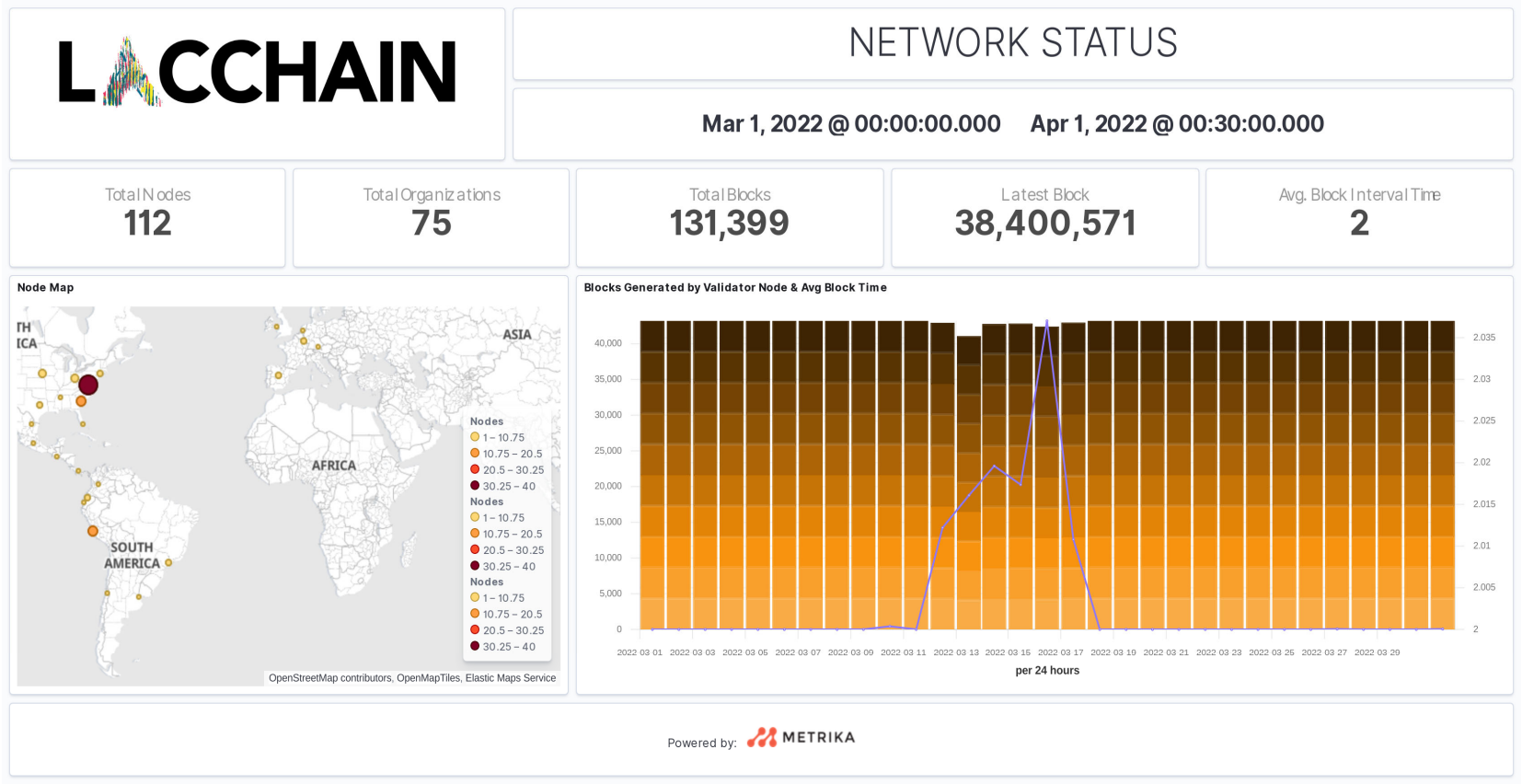
2. LACChain and LACNet: The Largest Permissioned-Public Blockchain in the World



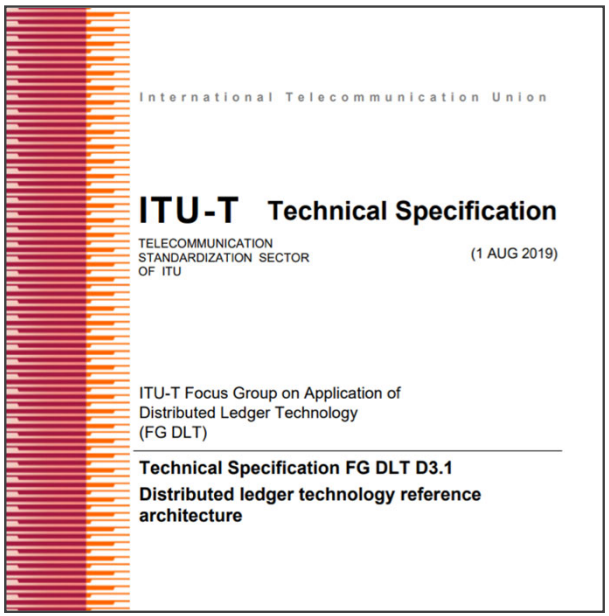
The Largest Permissioned-Public Blockchain in the World



A mainstream regional network



ITU Recognition as a reference worldwide



International Telecommunication Union

ITU-T Technical Specification

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

(1 AUG 2019)

ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT)

Technical Specification FG DLT D3.1

Distributed ledger technology reference architecture

Table A.1: Overview of architecture mapping to existing DLT platforms

Attachment	Platform	Contributor	Organization	Reviewer	Organization
I	**Alastria (Quorum version)**	Jesus Ruiz	Alastria	Paulo Brizola	Multiledgers
II	**Ardor**	Skylar Hurwitz	Jelurida	Xiaofeng Chen	Qulian
III	**Bitcoin**	Robin Renwick	Independent	Lisa Tan	Economics Design
IV	**Corda**	Paulo Brizola	Multiledgers	Ruifeng Hu	Huawei
V	**EOS**	Ning Hu	Ontology	Giovanni Cambronero	ANCE
VI	**Ethereum**	Suzana Maranhão	BNDES	Ning Hu	Ontology
VII	**Fabric**	Ruifeng Hu	Huawei	Paulo Brizola	Multiledgers
VIII	**Hyperchain**	Xiaofang Chen	Qulian	Baixue Yang	CAICT
IX	**LACChain**	Marcos Allende	IADB	Ismael Arribas	Kunfud
X	**Masterchain**	Alexander Chuburkov	Russian Fintech Association	Lisa Tan	Economics Design
XI	**Monero**	Robin Renwick	Independent	Lisa Tan	Economics Design
XII	**Ontology**	Ning Hu	Ontology	Baixue Yang	CAICT
XIII	**Quorum**	Ismael Arribas / Jose Nogueira	Kunfud/BNDES	Paulo Brizola	Multiledgers
XIV	**Sawtooth**	Ruifeng Hu	Huawei	Xiaofeng Chen	Qulian

The ideal features for public sector (I)



✓ **Carbon neutral** - CO2 emissions equivalent to 4 regular households, compensated by negative carbon initiative



✓ **No mining** – Consensus protocol is Proof of Authority



✓ **Neutral and non-profit network:** Orchestrator based in Uruguay and constituted by LACNIC, Red Clara, IDB Lab

The ideal features for public sector (II)



✓ **24/7 monitoring**, technical support based on SLA



✓ Several APIs and **open source resources**



✓ Recognized by ITU, ISO, and ETSI

LACNet, a neutral blockchain infrastructure orchestrator for for Latin America and the Caribbean





In collaboration with:

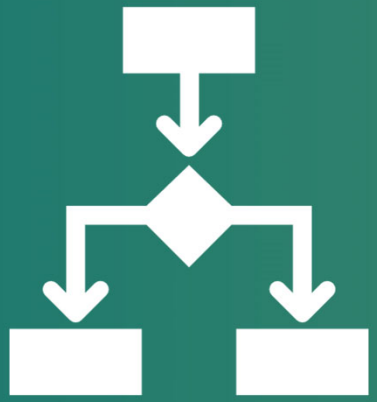


To orchestrate the networks of

LACCHAIN

LACCHAIN

3. Using the LACChain Blockchain as Public Key Directory



Comparing Public Key Directories

European Union

- TLs exposed privately through the EU Gateway. No open access
- For public access, you need to be checking each of the N trusted lists from the N countries
- You can not subscribe to events/updates about the trusted list
- Only the public key of the certificate is stored, not the full certificate (necessary for revocations)
- Impossible to rotate keys

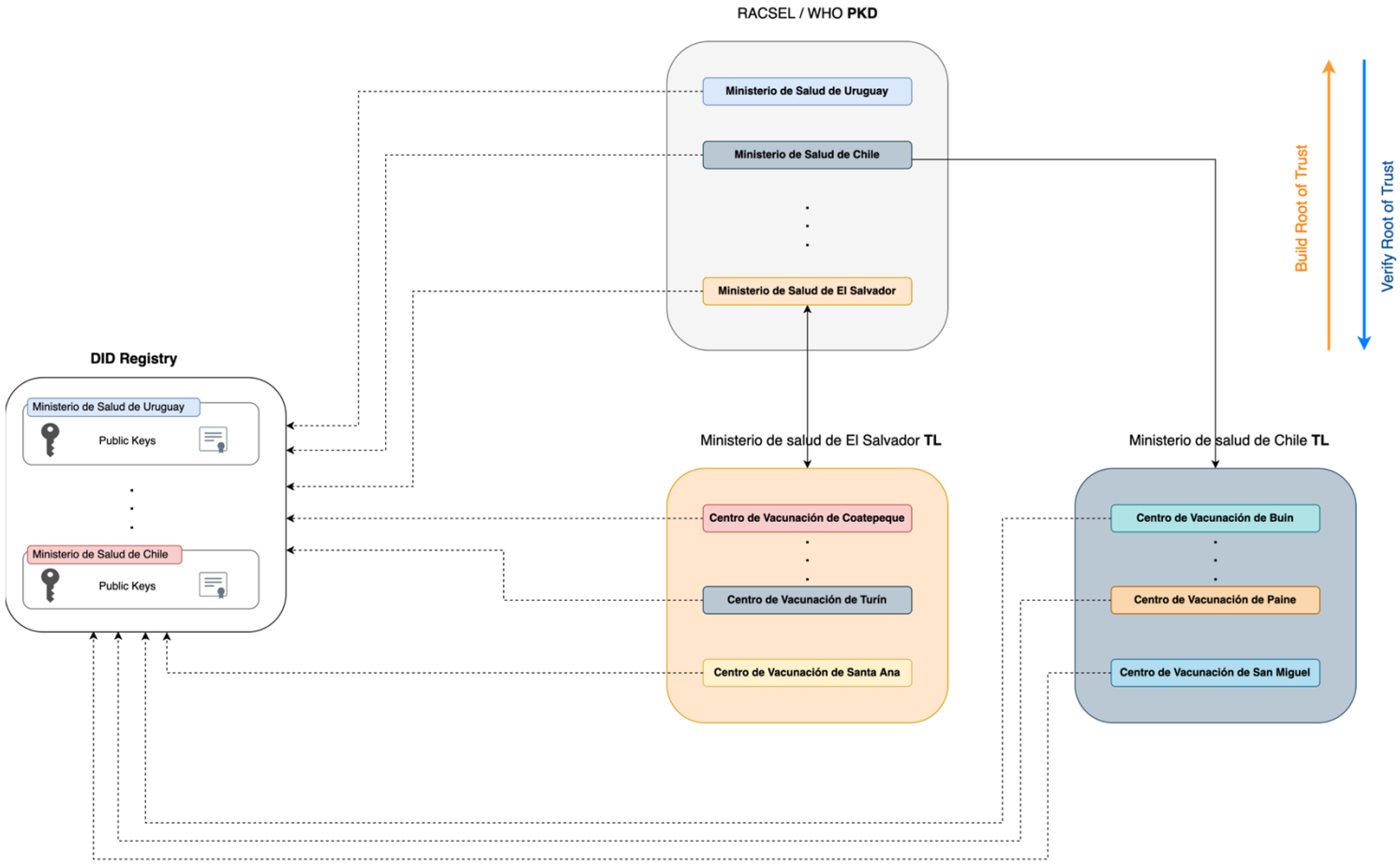
Current LAC situation

- Most countries don't expose any kind of public list
- Most advance countries TLs are being recognized by EU to then recognize each other
- No standard for public TLs
- As in the EU no possibility of subscription to updates
- Impossible to rotate keys

LACChain solution

- Blockchain-based root of trust
- Regional/international health entity maintaining one smart-contract based PKD
- Each Ministry of health can maintain one smart-contract based national TL
- Open access via API
- Possibility to be subscribed to events about any update in the smart contracts
- All smart contracts following common standard (GCCN, ToIP, LACChain)
- Very easy to rotate keys for a DID identifier

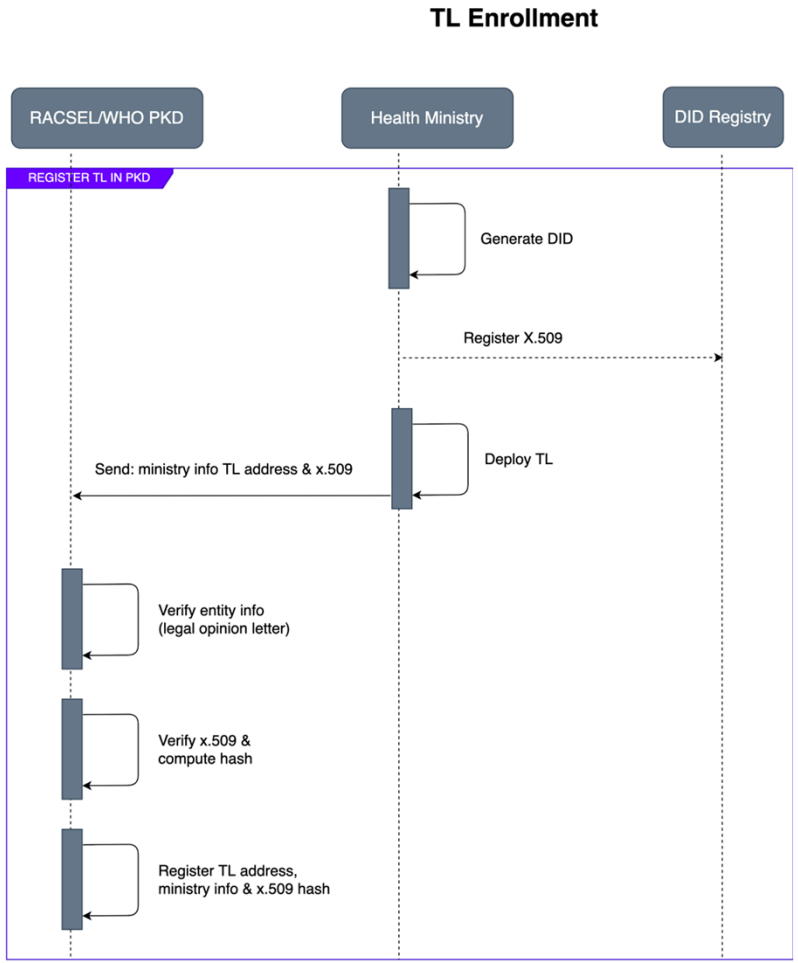
On-chain root of trust using smart contracts



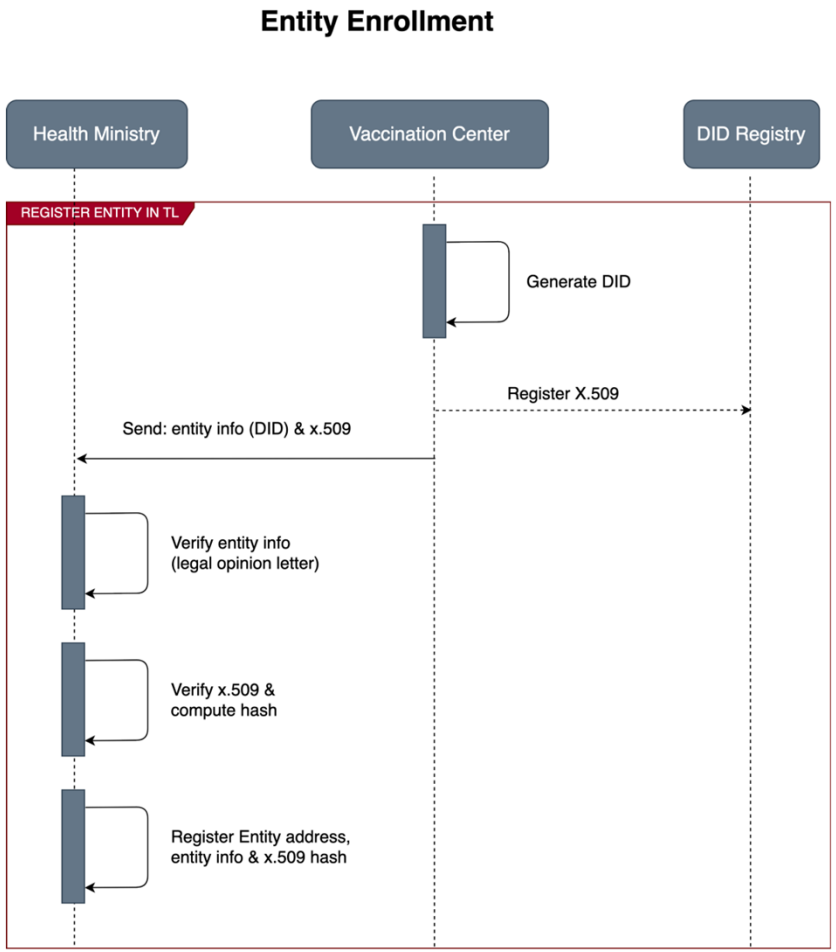
Each entity manages its own private keys and can register its own DIDs that comprise public keys and endpoints

Health authorities (e.g., RACSEL and Ministries of Health) register verified DIDs into the smart contracts representing the PKD and the Trusted List

Creating the Regional Public Key Directory



Creating the National Trusted Lists



TL Smart Contract - Code

```
pragma solidity ^0.8.0;
pragma experimental ABIEncoderV2;
import "@openzeppelin/contracts/access/Ownable.sol";

contract TrustedList is Ownable {
    struct TrustedEntity {
        string did;
        string name;
        uint expires;
        uint8 status;
    }

    string public name;
    address public parent;
    mapping(address => TrustedEntity) public entities;

    event EntityAdded( address indexed entity, string did, uint expires );
    event EntityUpdated( address indexed entity, string did, uint expires );
    event EntityRevoked( address indexed entity );

    constructor( address _parent, string memory _name ) Ownable() public {
        parent = _parent;
        name = _name;
    }

    function register( address _entity, string memory _did, string memory _name, uint _expires )
onlyOwner external {
        TrustedEntity storage entity = entities[_entity];
        entity.status = 1;
        entity.expires = _expires;
        entity.did = _did;
        entity.name = _name;

        emit EntityAdded( _entity, _did, _expires );
    }
    function update( address _entity, string memory _did, string memory _name, uint _expires )
onlyOwner external {
        TrustedEntity storage entity = entities[_entity];
        entity.expires = _expires;
        entity.did = _did;
        entity.name = _name;

        emit EntityUpdated( _entity, _did, _expires );
    }
    function revoke( address _entity ) onlyOwner external {
        TrustedEntity storage entity = entities[_entity];
        entity.status = 2;

        emit EntityRevoked( _entity );
    }
}
```

LACCHAIN

4. Using Verifiable Credentials for Vaccination Certificates



Verifiable Credentials (VCs) for Vaccination Certificates

EU DDCC

- Only integrity (checking digital signature), expiration, and valid issuer (against TL) are verified
- Revocation is unavailable
- Not integrated with digital wallets
- No possibility of Zero Knowledge Proofs
- Required physical ID to verify subject's identity
- Reveal a lot of personal data to every verifier

LACChain Solution

- ✓ You can verify integrity, valid issuer, revocation, expiration, and the subject cryptographically
- ✓ It is possible to revoke issuers and credentials via API – Also possible to subscribe to these events
- ✓ Integrated digital wallets
- ✓ Zero Knowledge proofs
- ✓ No need of physical ID to verify subject's identity
- ✓ No need to reveal any personal data to verifiers

COVID19 Certificate – Turning DDCC into VC


```
{
  "ver": "1.3.0",
  "nam": {
    "fn": "Cerón Figueroa",
    "fnt": "CERON<FIGUEROA",
    "gn": "Sergio",
    "gnt": "SERGIO"
  },
  "dob": "1989-01-25",
  "v": [
    {
      "tg": "840539006",
      "vp": "1119349007",
      "mp": "EU/1/20/1507",
      "ma": "ORG-100031184",
      "dn": 2,
      "sd": 2,
      "dt": "2021-02-15",
      "co": "CL",
      "is": "Dr. Juan Perez",
      "ci": "URN:UVCI:01:CL:DADFCC47C7334E45A906DB12FD859FB7#1"
    }
  ]
}
```



```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vaccination/v1"
  ],
  "type": ["VerifiableCredential", "VaccinationCertificate"],
  "id": "a6de5fff:9275:47be:9599:a5a591dfd895",
  "name": "COVID-19",
  "issuer": "did:lac:main:0xa1cde6e582b19c8c6f94f91d129566a621b25f65",
  "issuanceDate": "2022-05-25T20:45:01.524Z",
  "expirationDate": "2022-05-31T20:44:56.871Z",
  "trustedList": "0xaD9C7D8AAba030E586Ba016735b0b3B5FD650738",
  "credentialSubject": {
    "id": "did:lac:main:0x00085c59f280f531d2ae0357493e911abca0643c",
    "type": "VaccinationEvent",
    "batchNumber": "344",
    "administeringCentre": "Centro de Vacunacion de Coatepeque",
    "healthProfessional": "Centro de Vacunacion de Coatepeque",
    "countryOfVaccination": "El Salvador",
    "order": 1,
    "recipient": {
      "type": "VaccineRecipient",
      "givenName": "Marcos",
      "familyName": "Allende Lopez",
      "gender": "male",
      "birthDate": "02-02-2000"
    },
    "vaccine": {
      "type": "Vaccine",
      "disease": "COVID-19",
      "atcCode": "J07BX03"
    }
  },
  "proof": [...]
}
```

Yellow Fever Certificate – Turning FHIR into VC


```
{
  "fhirVersion": "4.0.1",
  "fhirBundle": {
    "resourceType": "Bundle",
    "type": "collection",
    "entry": [
      {
        "fullUrl": "resource:0",
        "resource": {
          "resourceType": "Patient",
          "name": [
            {
              "family": "Anyperson",
              "given": [
                "Jane",
                "C."
              ]
            }
          ],
          "birthDate": "1961-01-20"
        }
      },
      {
        "fullUrl": "resource:1",
        "resource": {
          "resourceType": "Immunization",
          "status": "completed",
          "vaccineCode": {
            "coding": [
              {
                "system": "http://hl7.org/fhir/sid/cvx",
                "code": "208"
              }
            ]
          },
          "patient": {
            "reference": "resource:0"
          },
          "occurrenceDateTime": "2021-01-01",
          "performer": [
            {
              "actor": {
                "display": "ABC General Hospital"
              }
            }
          ],
          "lotNumber": "0000002"
        }
      },
      {
        "fullUrl": "resource:2",
        "resource": {
          "resourceType": "Immunization",
          "status": "completed",
          "vaccineCode": {
            "coding": [
              {
                "system": "http://hl7.org/fhir/sid/cvx",
                "code": "208"
              }
            ]
          },
          "patient": {
            "reference": "resource:0"
          },
          "occurrenceDateTime": "2021-01-29",
          "performer": [
            {
              "actor": {
                "display": "ABC General Hospital"
              }
            }
          ],
          "lotNumber": "0000008"
        }
      }
    ]
  }
}
```



```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vaccination/v1"
  ],
  "type": ["VerifiableCredential", "VaccinationCertificate"],
  "id": "a6de5fff:9275:47be:9599:a5a591dfd895",
  "name": "COVID-19",
  "issuer": "did:lac:main:0xa1cde6e582b19c8c6f94f91d129566a621b25f65",
  "issuanceDate": "2022-05-25T20:45:01.524Z",
  "expirationDate": "2022-05-31T20:44:56.871Z",
  "trustedList": "0xaD9C7D8AAba030E586Ba016735b0b3B5FD650738",
  "credentialSubject": {
    "id": "did:lac:main:0x00085c59f280f531d2ae0357493e911abca0643c",
    "type": "VaccinationEvent",
    "batchNumber": "344",
    "administeringCentre": "Centro de Vacunacion de Coatepeque",
    "healthProfessional": "Centro de Vacunacion de Coatepeque",
    "countryOfVaccination": "El Salvador",
    "order": 1,
    "recipient": {
      "type": "VaccineRecipient",
      "givenName": "Marcos",
      "familyName": "Allende Lopez",
      "gender": "male",
      "birthDate": "02-02-2000"
    },
    "vaccine": {
      "type": "Vaccine",
      "disease": "Yellow fever",
      "atcCode": "J07BL01"
    }
  },
  "proof": [...]
}
```

LANGCHAIN

5. Understading the DEMO



Creating the Root of Trust (PKD y TLs) – (1/4)

- RACSEL authenticates as the entity running the PKD
- RACSEL registers three Ministries of Health (their blockchain identifiers and their X.509)
- Each Ministry of Health authenticates and creates its own national TL

Disclaimer: In practice all these is via API with each entity authenticating themselves using X.509 and blockchain identities. For the demo we show a web interface.

Issuing Vaccination Certificates - (2/4)

- One of the authorized verifiers (registered in the TL of one country) authenticates and creates a vaccination certificate in Green Pass and Verifiable Credential (VC) format. The VC format is signed with a X.509 key, with a DID key, and with a ZKP key
- The vaccination certificate is registered in the blockchain (hash, revocation information, subject DID)
- The vaccination certificate is sent to the digital wallet of the subject

Disclaimer: In practice all these is via API with each entity authenticating themselves using X.509 and blockchain identities. For the demo we show a web interface.

Presenting and verifying vaccination certificates - (3/4)

- The subject selects which presentation to provide from the digital wallet and generates a QR

- The verifier verifies the QR

  - If verifying the Green Pass, revocation and subject can't be verified properly
  - If verifying the VC, everything can be verified properly using both X.509 and DID signature
  - If verifying the VC with zero knowledge proof, the verifier verifies everything without knowing anything more than what the subject discloses

DZ0

Revoking (4/4)

- The credential is revoked – the VC is revoked but the Green Pass is not
- Any of the entities in the root of trust is revoked – the VC is revoked but the Green Pass is not

Diapositiva 28

DZ0 Creemos que este debería ser el número 4

Daniel Zárate; 2022-05-26T20:12:59.297


LACCHAIN
www.lacchain.net

Main Links

- **Website**: lacnet.lacchain.net
- **LACNet's GitHub: https://github.com/LACNetNetworks**
- LACChain **Academy** www.lacchain.net/academy
- LACChain's **Wiki** https://github.com/lacchain/wiki/wiki
- **Framework DLT** **https://publications.iadb.org/en/lacchain-framework-permissioned-public-blockchain-networks-blockchain-technology-blockchain**
- **Framework ID** **https://publications.iadb.org/en/lacchain-id-framework-set-recommendations-blockchain-based-interoperable-privacy-preserving**

Know more

- Deploy your first **ERC20** https://github.com/LACNetNetworks/gas-management/blob/master/docs/tutorial/Deploy_SmartContract.md
- Deploy and test a **digital credentials verification** https://github.com/LACNetNetworks/gas-management/blob/master/docs/tutorial/VC_en.md
- Deploy and test a **trusted list on-chain** https://github.com/LACNetNetworks/gas-management/blob/master/docs/tutorial/PKD_en.md
- Network **GAS distribution** mechanism https://github.com/LACNetNetworks/gas-management
- Mechanism of **rotation** of validating **nodes** https://github.com/LACNetNetworks/rotation-validator
- **LACChain ID Demo Wallet https://wallet.lacchain.net/register**