Building trust frameworks for Verifiable Health Credentials including digital COVID-19 certificates

Marcos Allende Lopez

IDB Specialist in Blockchain, Digital Assets, and Quantum

CTO of LACChain Blockchain Global Alliance

LACCHAIN

IDB
Inter-American Development Bank

Overview

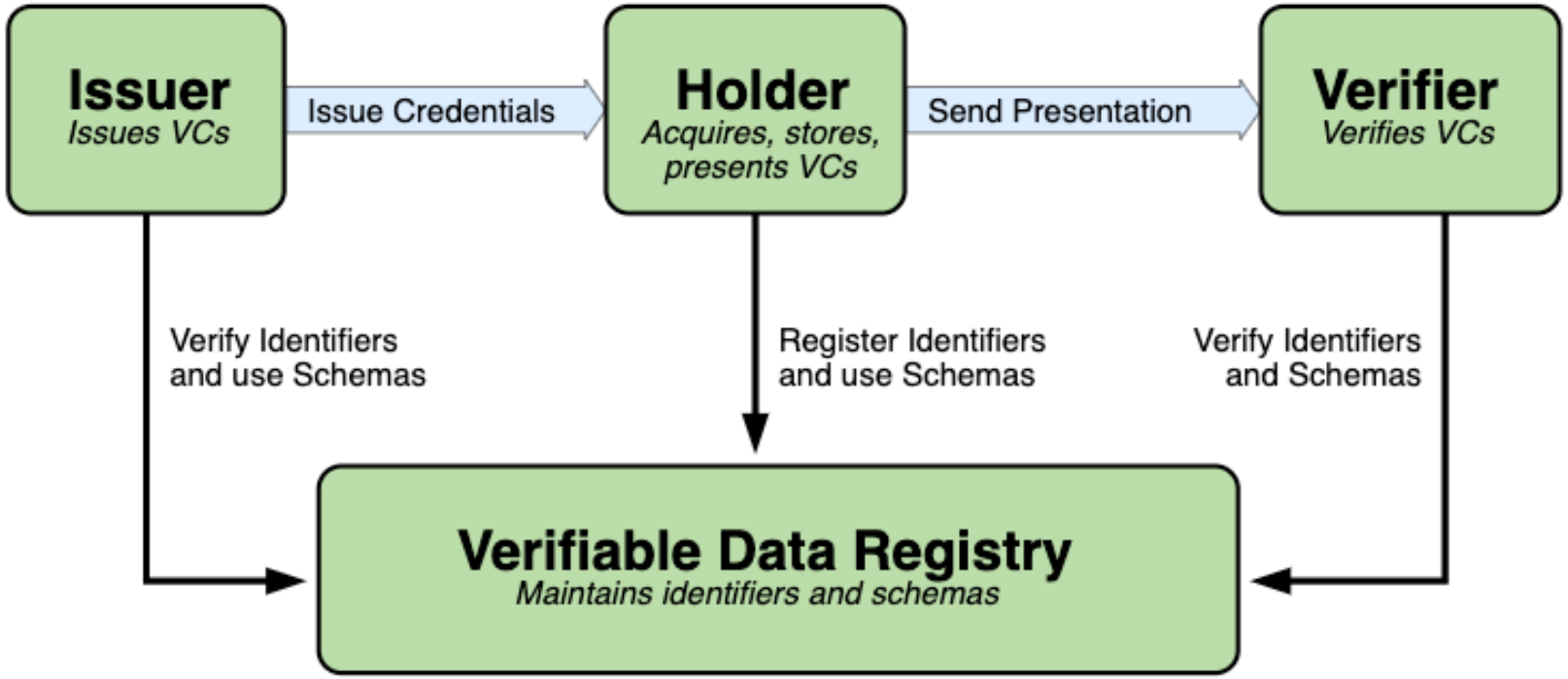
- The importance of digital credentials
- What does it take to verify a credential
- What failed with COVID19 certificates
- Alternatives to address current interoperability issues
- Decentralized Public Key Directories
- Pioneer work of LACChain and LACPass in LATAM
- The new ecosystem of digital credentials and wallets

LACCHAIN IDB Inter-American Development Bank

The importance of digital credentials

- Credentials are data in some sort of structured format
- Credentials have a subject
- Credentials have an issuer (the subject or someone else)
- Credentials are intended to be presentable
- Credentials are intended to be verifiable
- Credentials contain data in the form of claims or attestations about the subject
- An electronic signature in the credential allows to verify integrity
- A timestamp allows to verify issuance data
- A trust registry allows to verify the issuer and the revocation status
- In essence, a credentials allows a subject to prove a third party (a verifier) some claims attested by a trusted issuer

The importance of digital credentials



Bundeskanzleramt

Digital identity

How an ecosystem can promote a self-sovereign and user-friendly approach to digital identity

Contents

The lack of digital credentials is one of the most pressing obstacles facing the digital transformation at the present. This document sheds light on the importance of credentials for the digital world and, with this in mind, outlines the objectives and functioning of self-sovereign identity (SSI). It also sets out the vision for a European identity ecosystem. The establishment of this ecosystem is the objective of the European Digital Identity Initiative project, which the German Federal Government has established together with partners from the business community.

This document consists of the following sections:

LACCHAIN IDB Inter-American Development Bank

EUROPEAN
COMMISSION

Brussels, 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

What is emerging in the market is a new environment where the focus has shifted from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities. There is an increased demand for electronic identity solutions that can deliver these capabilities providing efficiency gains and a high level of trust across the EU, both in the private and the public sector, relying on the need to identify and authenticate users with a high level of assurance.

The evaluation of the eIDAS Regulation[2] revealed that the current Regulation falls short of addressing these new market demands, mostly due to its inherent limitations to the public sector, the limited possibilities and the complexity for online private providers to connect to the system, its insufficient availability of notified eID solutions in all Member States and its lack of flexibility to support a variety of use cases. Furthermore, identity solutions falling outside the scope of eIDAS, such as those offered by social media providers and financial institutions, raise privacy and data protection concerns. They cannot effectively respond to new market demands and lack the cross border outreach to address specific sectoral needs where identification is sensitive and requires a high degree of certainty.

Since the entering into force of the eID part of the Regulation in September 2018, only 14 Member States have notified at least one eID scheme. As a result, only 59 % of EU residents have access to trusted and secure eID schemes across borders. Only 7 schemes are entirely mobile, responding to current user expectations. As not all technical nodes to ensure the connection to the eIDAS interoperability framework are fully operational, cross-border access is limited; very few online public services accessible domestically can be reached cross-border via the eIDAS network.

What does it take to verify a credential

- The format needs to be recognized
- The content needs to be intelligible for the verifier (ideally machine-readable)
- The signature needs to be verified to prove integrity (i.e., data not changed)
- The issuer needs to be checked against a key directory
- The status needs to be verified against a trust registry to check revocation

What failed with COVID19 certificates

- The format needs to be recognized -> Multiple formats including DCC, DIVOC, SHC, ...
- The content needs to be intelligible for the verifier (ideally machine-readable) -> JSON + QR
- The signature needs to be verified to prove integrity (i.e., data not changed) –> Digital Signatures
- The issuer needs to be checked against a key directory –> No public key directories enabled
- The status needs to be verified against a trust registry to check revocation –> No public key directories enabled

LACCHAIN IDB Inter-American Development Bank

Alternatives to address current interoperability issues

- The format needs to be recognized -> Multiple formats including DCC, DIVOC, SHC, ...
  - Universal standard or mutual recognition of different standards, ideally W3C VC
- The content needs to be intelligible for the verifier (ideally machine-readable) -> JSON + QR
  - Continue to use JSON + QR – Enable universal verification apps
- The signature needs to be verified to prove integrity (i.e., data not changed) –> Digital Signatures
  - Improve digital signatures to be quantum-resistant (NIST)
- The issuer needs to be checked against a key directory –> No public key directories enabled
  - Need to enable universal public key directories to verify issuer's signatures
- The status needs to be verified against a trust registry to check revocation –> No public key directories enabled
  - Need to enable universal public key directories to verify credential statuses

LACCHAIN IDB Inter-American Development Bank

Decentralized Public Key Directories

- While in centralized public key directories one entity must maintain the digital infra (databases), in a decentralized one all parties can be at the same hierarchy level
- In a decentralized public key directory, each party can update their own information (their public keys and the statuses of the credentials they have issued)
- If using blockchain technology, smart contracts can be leveraged to set governance rules (e.g., the WHO can verify a country's identity and then each Ministry of Health can update their own information)

Pioneer work of LACChain and LACPass in LATAM

- LACChain is the Global Alliance for the Development of Blockchain in Latin America and the Caribbean, created at the Inter-American Development Bank
- LACChain has built a permissioned public blockchain used by +130 entities and +80 projects
- LACPass is a Regional Public Good project led from the Inter-American Development Bank for digital health certificates

https://lacnet.lacchain.net/documentation/
https://www.racsel.org/bprlacpass/

LACCHAIN IDB Inter-American Development Bank

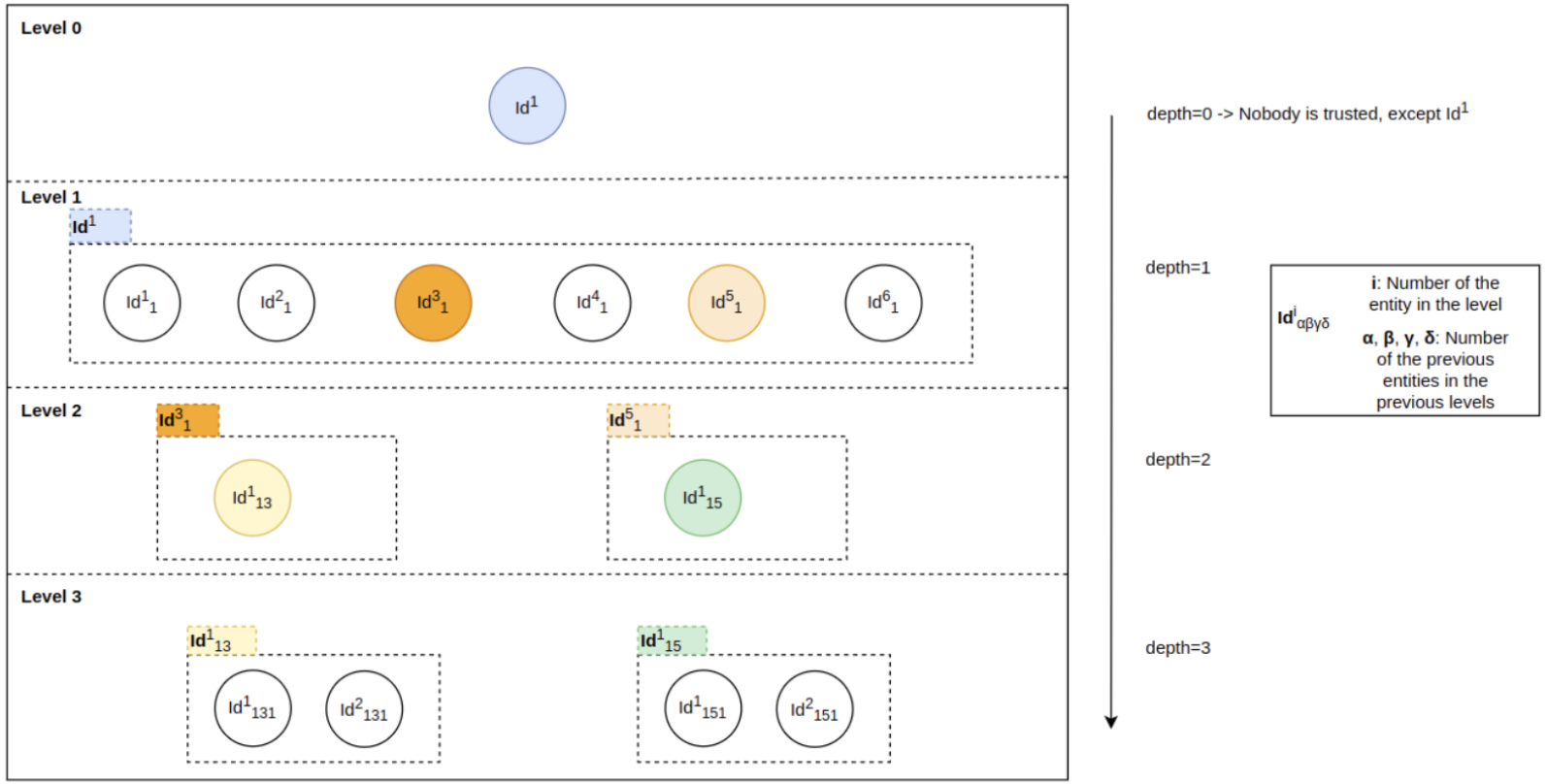
Pioneer work of LACChain and LACPass in LATAM

- We have created a root of trust with three elements, a DID Registry, a PKD, and Trusted Lists
- **DID Registry:** the open registry where every entity can update their public keys and endpoints associated with their DID
- **PKD:** the single directory where the root CA (eg. WHO) lists the DIDs associated to entities they recognize (eg. Ministries of Health)
- **Trusted Lists:** the multiple directories where any entity can become a CA (eg. Ministries of Health) and recognize other entities below their hierarchy

https://lacnet.lacchain.net/documentation/
https://www.racsel.org/bprlacpass/

LACCHAIN IDB Inter-American Development Bank

Pioneer work of LACChain and LACPass in LATAM

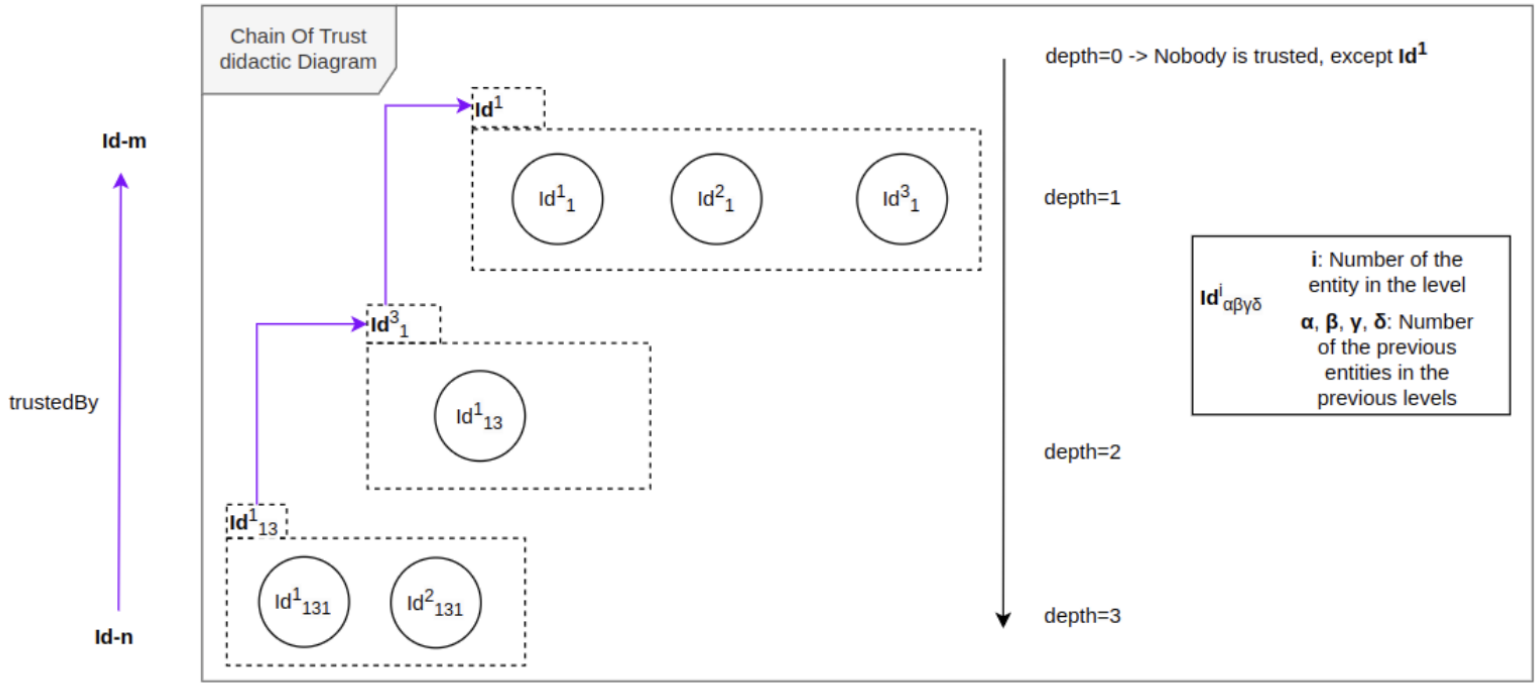


https://github.com/lacchain/LACChain-contracts

LACCHAIN IDB Inter-American Development Bank

Pioneer work of LACChain and LACPass in LATAM

In the following diagram depth=3 is exemplified

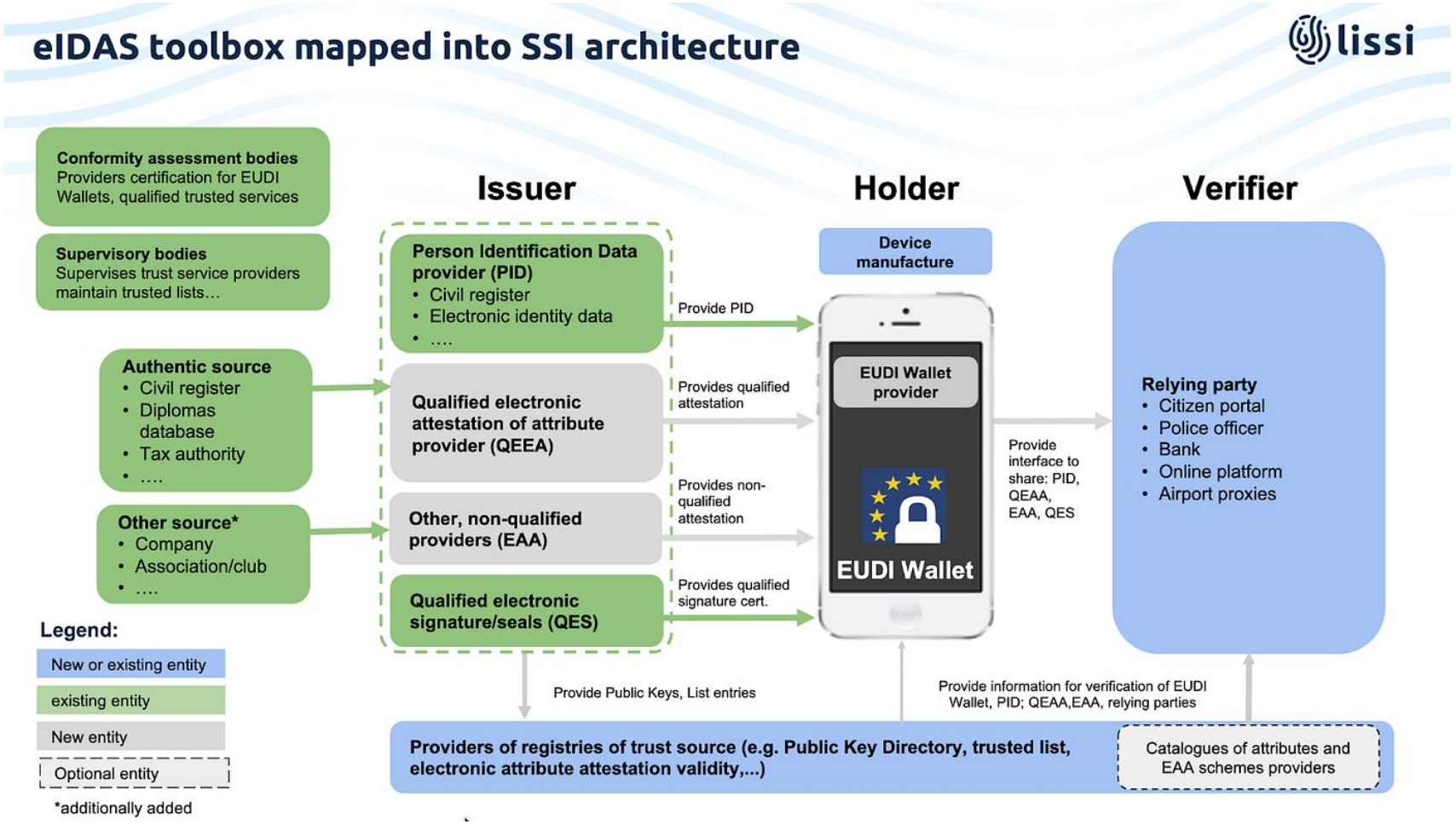


https://github.com/lacchain/LACChain-contracts

The new ecosystem of digital credentials and wallets

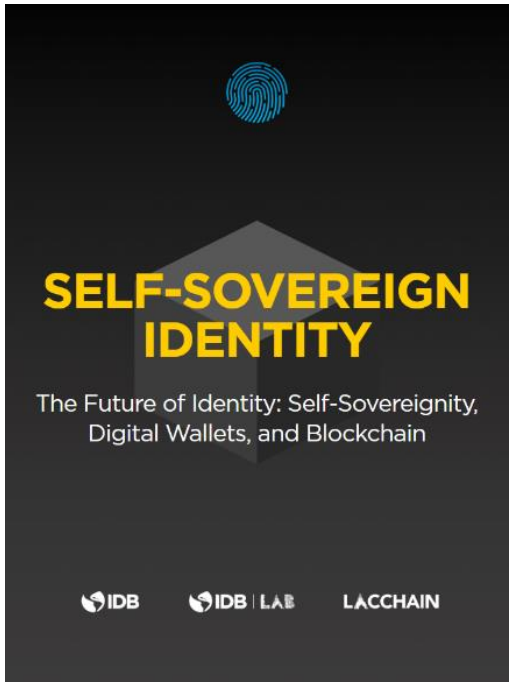
- New standards such as Verifiable Credentials and Decentralized Identifiers are coming from W3C
- Digital Wallets will be essential for users to manage their identity, credentials, and attestations
- EUID Wallet framework and eIDAS2 regulation passing in 2024 are the evidence of EU pioneer work towards this new age
- Selective disclosures, zero-knowledge proofs, revocation status, and decentralized public key directories are the innovations that should happen soon
- Blockchain networks are very useful trust registries to combine the verifiability of data and credentials in full compliance with data protection, and to transfer value in real time

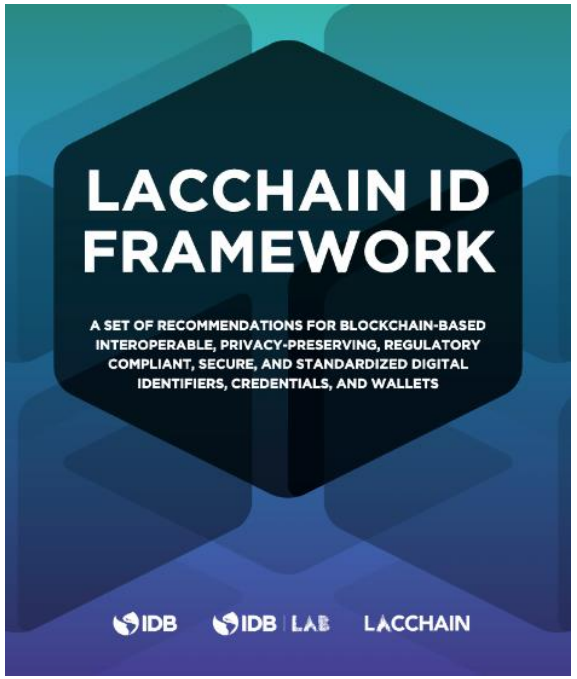
The new ecosystem of digital credentials and wallets

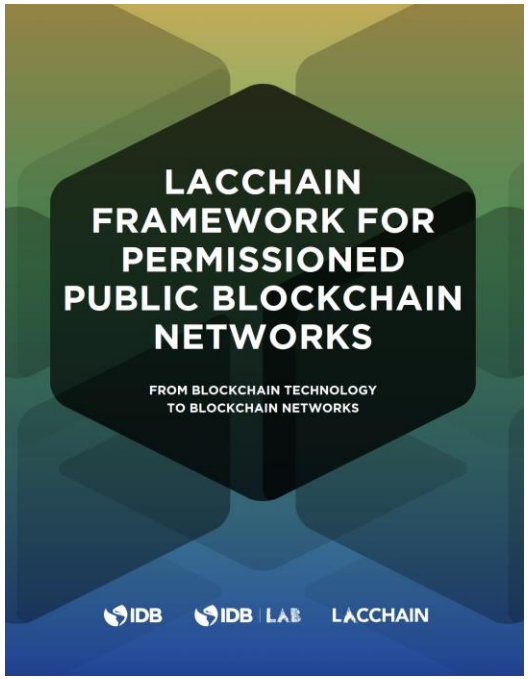


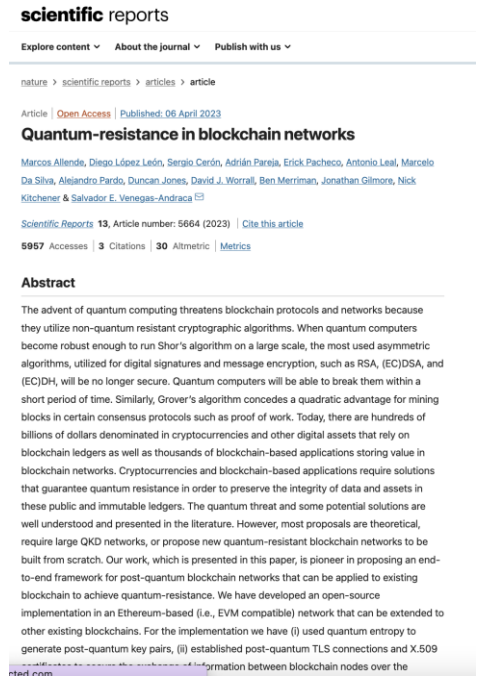
LACCHAIN IDB Inter-American Development Bank

The new ecosystem of digital credentials and wallets









scientific reports

Explore content · About the journal · Publish with us

nature › scientific reports › articles › article

Article | Open Access | Published: 06 April 2023

Quantum-resistance in blockchain networks

Marcos Allende, Diego López León, Sergio Cerón, Adrián Pareja, Erick Pacheco, Antonio Leal, Marcelo Da Silva, Alejandro Pardo, Duncan Jones, David J. Worrall, Ben Merriman, Jonathan Gilmore, Nick Kitchener & Salvador E. Venegas-Andraca

Scientific Reports **13**, Article number: 5664 (2023) | Cite this article

5957 Accesses | **3** Citations | **30** Altmetric | Metrics

Abstract

The advent of quantum computing threatens blockchain protocols and networks because they utilize non-quantum resistant cryptographic algorithms. When quantum computers become robust enough to run Shor's algorithm on a large scale, the most used asymmetric algorithms, utilized for digital signatures and message encryption, such as RSA, (EC)DSA, and (EC)DH, will be no longer secure. Quantum computers will be able to break them within a short period of time. Similarly, Grover's algorithm concedes a quadratic advantage for mining blocks in certain consensus protocols such as proof of work. Today, there are hundreds of billions of dollars denominated in cryptocurrencies and other digital assets that rely on blockchain ledgers as well as thousands of blockchain-based applications storing value in blockchain networks. Cryptocurrencies and blockchain-based applications require solutions that guarantee quantum resistance in order to preserve the integrity of data and assets in these public and immutable ledgers. The quantum threat and some potential solutions are well understood and presented in the literature. However, most proposals are theoretical, require large QKD networks, or propose new quantum-resistant blockchain networks to be built from scratch. Our work, which is presented in this paper, is pioneer in proposing an end-to-end framework for post-quantum blockchain networks that can be applied to existing blockchain to achieve quantum-resistance. We have developed an open-source implementation in an Ethereum-based (i.e., EVM compatible) network that can be extended to other existing blockchains. For the implementation we have (i) used quantum entropy to generate post-quantum key pairs, (ii) established post-quantum TLS connections and X.509

LACCHAIN IDB Inter-American Development Bank

Building trust frameworks for Verifiable Health Credentials including digital COVID-19 certificates

Marcos Allende Lopez

IDB Specialist in Blockchain, Digital Assets, and Quantum

CTO of LACChain Blockchain Global Alliance

LACCHAIN

IDB
Inter-American Development Bank