8th Distributed Ledger Technology Workshop (DLT 2026)

Pula – June 5th, 2026

A Post-Quantum Secure Framework for Self-Sovereign Management of Encrypted Personal Data on Blockchain Using ZK-STARK

Alberto Leporati, Andrea Vanini

University of Milano-Bicocca

Department of Informatics, Systems, and Communication

alberto.leporati@unimib.it

The problem: personal data management

Current digital identity challenges and future threats

Centralization

Data is stored and managed by third parties, creating potential **single points of failure**.
Consider, for example, the recent outages of AWS and Azure (cloud computing) and Cloudflare (CDN) in recent months.
There is a high risk of data breaches and loss of control of the data by the citizen.

Quantum threath

«Harvest now, decrypt later» strategy. Malicious actors harvest data today to decrypt it tomorrow using sufficiently powerful quantum computers using the Shor and Grover algorithms.

Weak standards

Microcredentials and Open Badges lack long-term verifiability, robust cryptographic guarantees, poor interoperability, and **a uniform regulatory framework** that guarantees their usability and European recognition.

Regulatory context: The 2024 **eIDAS 2.0** Regulation mandates the adoption of European Digital Identity Wallets (EUDI Wallets) based on the principles of **Self-Sovereign Identity (SSI).**

The goal: A decentralized framework

With post-quantum technology and zero-knowledge proofs

Decentralized

No central authority, eliminating single points of failure (SPoF). Citizens retain control of their data.

Resistant to quantum attacks

Designed to withstand future quantum computers (Shor and Grover algorithms) today.

Zero-Knowledge verifiability

Demonstrates possession of information (for example, having received a vaccination) without revealing the underlying data.

Case study

- **Vaccination management:** Critical domain with stringent integrity and privacy requirements.
- **Historical preservation:** Data that is immutable and verifiable over time.

Generalizability

- **Education:** CFU, Qualifications, State Exams.
- **Work:** Certified professional skills.

Quantum threaths: Shor and Grover algorithms

In the future, classical cryptography will not be enough

Shor algorithm

Compromises asymmetric systems based on integer factorization and discrete logarithm.

- RSA (factorization problem)
- Diffie-Hellman, ElGamal and DSA (discrete logarithm problem)
- Elliptic curve cryptography (ECC)

Grover algorithm

Quadratically reduces the complexity of brute-force attacks on symmetric ciphers and, similarly, that of finding collisions in hash functions.

- AES, and other symmetric cryptosystems
- SHA and other hash functions

Some cryptographic tools

PBKDF2

Password-Based Key Derivation Function 2

Makes each password guess computationally expensive. Designed to thwart brute-force and dictionary attacks. (HMAC-SHA3 512).

HKDF

HMAC-based Key Derivation Function

A derivation function designed to extract and expand key material from an initial source. (SHA3 512).

2SKD

Two-Secret Key Derivation

A cryptographic derivation strategy that combines two independent secrets (pin + password) to obtain a final key.

SPHINCS+

A stateless **digital signature scheme** based on hash functions.

Chosen for its quantum resistance.

Other tools

Blockchain

Distributed ledger

Eliminate the single point of failure by replicating data over a peer-to-peer network.

Smart contracts and SBT

Using SoulBound Tokens (SBT) on Algorand to bind our digital identity permanently and non-transferably.

Immutability

Guaranteed by distributed consensus and cryptographic block chaining.

ZK-SNARKs vs. ZK-STARKs

Feature	ZK-SNARK	ZK-STARK
Trusted setup	Required	**Not required**
Quantum resistance	No (based on ECC)	**Yes (hash-based)**
Proof size	**Small (~200 B)**	Large (~45KB)

Design choice

Despite the larger size of the test, **ZK-STARKs were chosen** for their quantum hardness and lack of a (computationally expensive) trusted setup. The **RISC Zero** system was chosen.

Technological infrastructure

Algorand

Permissionless, immutable blockchain, smart contracts with SoulBound Tokens.

IPFS cluster

Decentralized and distributed storage for storing encrypted certificates.

Backend and Frontend

Django + FastAPI + Flask with React + Vine.

Docker

Containerization for environmental isolation and portability.

SBT and derivation of the owner field

Non-transferable identity and post-quantum security

SoulBound Token (SBT)

Based on ERC-5484 on Algorand.

Non-transferable tokens, permanently linked to the citizen's identity.

The **owner** field contains the address derived from the SPHINCS+ public key.

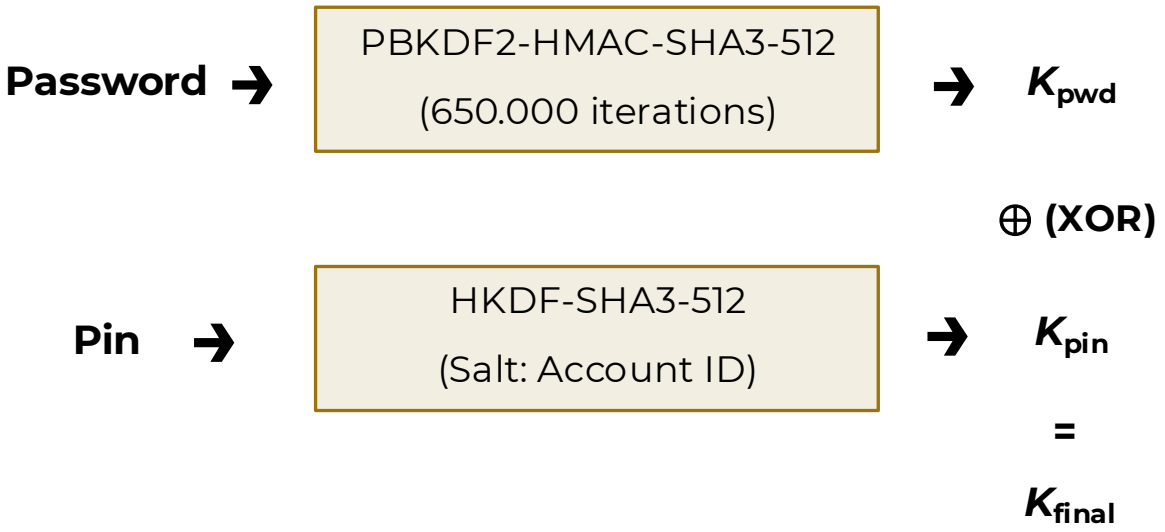
Security

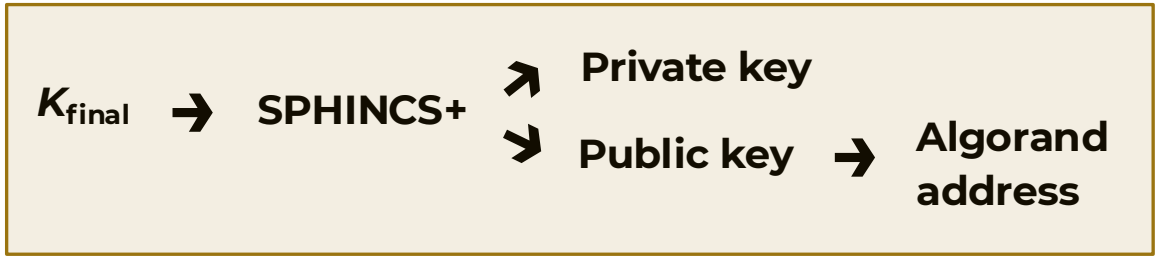
The private key is **never stored persistently**.

Compromise is only possible if:

- **both secrets** (password + PIN) are known;
- the **security** of the SPHINCS+ algorithm is **breached**.

Two-secret key derivation (2SKD)





Functionality: issue an SBT

Healthcare worker area

1. Registration and public key derivation

Deterministic post-quantum public key derivation from user password and PIN.

2SKD and SPHINCS+

2. Deploy SoulBound token

Smart contract creation on the Algorand blockchain. Identity is permanently tied to the owner field.

Algorand smart contract

3. Association of tax code and SBT

The association between the tax code and the SBT is saved within a database.

Database

Functionality: revoke an SBT

Healthcare worker area

Atomicity of the transaction

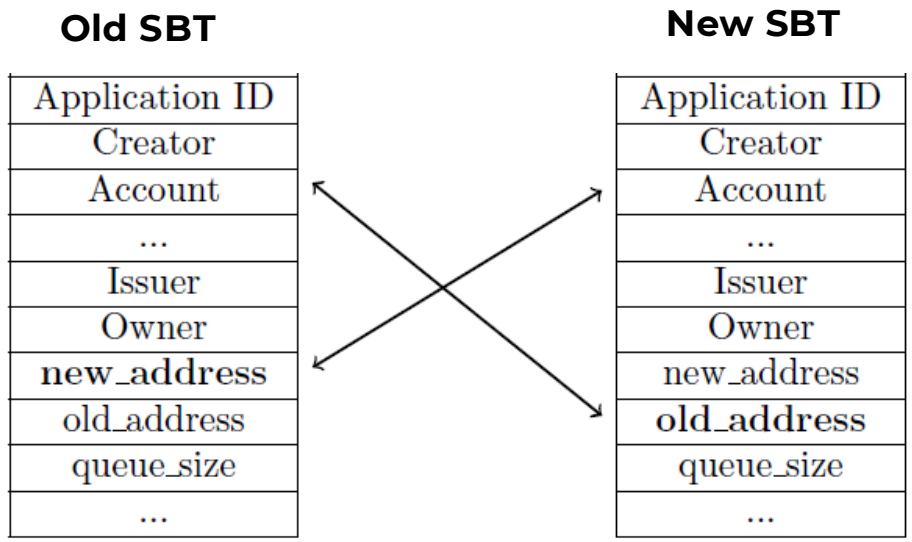
The revocation operation is atomic: either it completes entirely on both SBTs or it fails without leaving any intermediate states.

Access control

Only the issuing authority has the cryptographic permissions to invoke the revocation method on the SBT smart contract.

Immutability of the event

Once revoked, the old SBT is not deleted. A series of pointers allows you to keep track of the history of SBTs, ensuring their integrity and future verifiability.



Note: Revoking does not delete data on IPFS.

Functionality: vaccination registration

Healthcare worker area

1. Verify data

The operator enters the vaccinated person's data.

The system checks the match with the existing SBT.

Input validation

2. Post-quantum encryption

Vaccination registration, issuance of encrypted JSON certificate by the user.

AES-256

3. Upload to IPFS cluster

The encrypted file is uploaded to the IPFS Cluster. A unique CID is generated to ensure the integrity of the content.

Upload IPFS

4. Update SBT

The CID is stored on the Algorand blockchain and recorded within the SBT.

Algorand transaction

Guaranteed Integrity: Any change to the certificate on IPFS would change the CID, making it immediately possible to detect tampering with the value recorded on-chain.

ZK-STARKs with RISC Zero

Citizen area

1. Read SBT data

Retrieve the latest CID from the smart contract.

Algorand

2. Decrypt

Download the certificate from IPFS and decrypt it locally using the user's credentials.

IPFS cluster and AES-256

3. Generate ZK proof

Creation of cryptographic proof (receipt.bin) that certifies the validity of the vaccine without revealing the data.

RISC Zero ZKVM

4. Public verification

Anyone can check the validity of the proof in **about 3 seconds**.

Verifier

Functionality: vaccination registration

Verify without revealing: from private data to public evidence

Private input (ZKVM)

- Vaccination certificate (JSON).
- List of requested vaccines.
- Current timestamp.

ZKVM processing

- Execution of verification logic.
- Proof generation.
- No sensitive data is revealed.

Output

- Receipt.bin (the proof).
- Outcome (ex: vaccine OK).
- SHA-512 fingerprint, to guarantee integrity.

Real-world performance: Testing takes only ~3 seconds on native Ubuntu. Ideal for quick checks.

Correctness

Automatic implementation test results

Backend (Django)

47 tests — **0 Errors**

Frontend (React)

41 tests — **0 Errors**

Test coverage (CI/CD GitLab)

- Cryptographic integrity
- Input validation
- Error handling
- Mock blockchain/IPFS
- Navigation flows
- Build Docker

Conclusions and directions for future work

A decentralized, quantum-resistant infrastructure can be realized today

OBTAINED RESULTS

- **Decentralized framework:** Management of health data without central authority, eliminating SPoF.
- **Post-Quantum by design:** SPHINCS+, SHA3-512, AES-256 and ZK-STARK.
- **Zero-Knowledge verifiability:** Mathematical proof of data possession without access to content.
- **Paradigm shift:** the user returns to the center, actively demonstrating their attributes.

FUTURE APPLICATIONS

Education

Certification of CFUs, Degrees and State Exams.

Work

Professional skills and certifications.

Dedicated hardware (FPGA / ASIC)

To make proof verification even faster.

Thank you for your attention !

GitLab repository of the project: