Ledger Origin

Minting a sanitary pass for fun and privacy

ETHCC 4
July 2021

Nicolas Bacca
@btchip

Whoami / whatisdis

Ledger

Co-founder at Ledger, CTO at Ledger Origin (IoT division)

Interested in open Trusted Computing, privacy

Week end hack turned into an emergency talk

(yes, you’re in the right room)

The sanitary pass

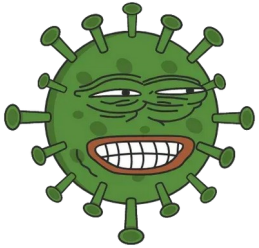
QR code format defined by an European standard (Digital Green Certificate)
https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v1_en.pdf

Useful to get into Ethereum conferences and cafés

In France :

Incorporated into TousAntiCovid app

Verified by TousAntiCovid Verif



Security issues

Signed QR code for authentication ?!?

Everybody can copy it

Sometimes verified using naked eyes

Privacy issues

Trust the validation application not to keep your data when reading it

Which data are we talking about exactly ?

The obvious : Name

The less obvious : Age, Type of vaccine, Vaccination country, Issuance and Expiration date

The correlated : List of venues, time of visit, who is attending together ...

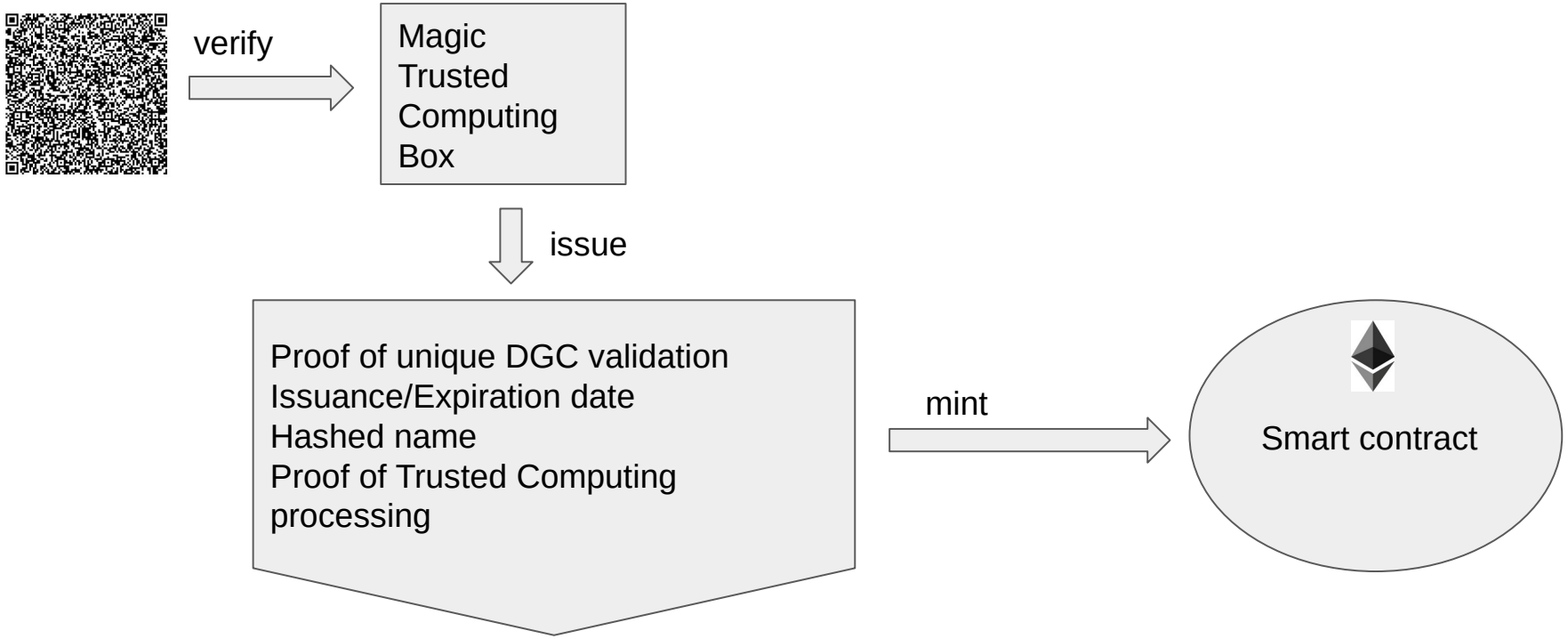
What if ...

We could provide a proof of owning a Digital Green Certificate (locally or remotely)

We could optionally link it to our name, on demand, not by default

This wouldn’t involve sending the DGC to a centralized party at any point

Trusted Computing and Ethereum to the rescue



The challenges

Ledger

Can we verify the DGC on a Trusted Computing platform ?

Is the Trusted Computing Platform open enough to let us check what is it doing ?

Can we verify the Trusted Computing proof in a smart contract ?

Reading the DGC QR code

Ledger

Scanning

Decoding with base45 (https://datatracker.ietf.org/doc/draft-faltstrom-base45/)

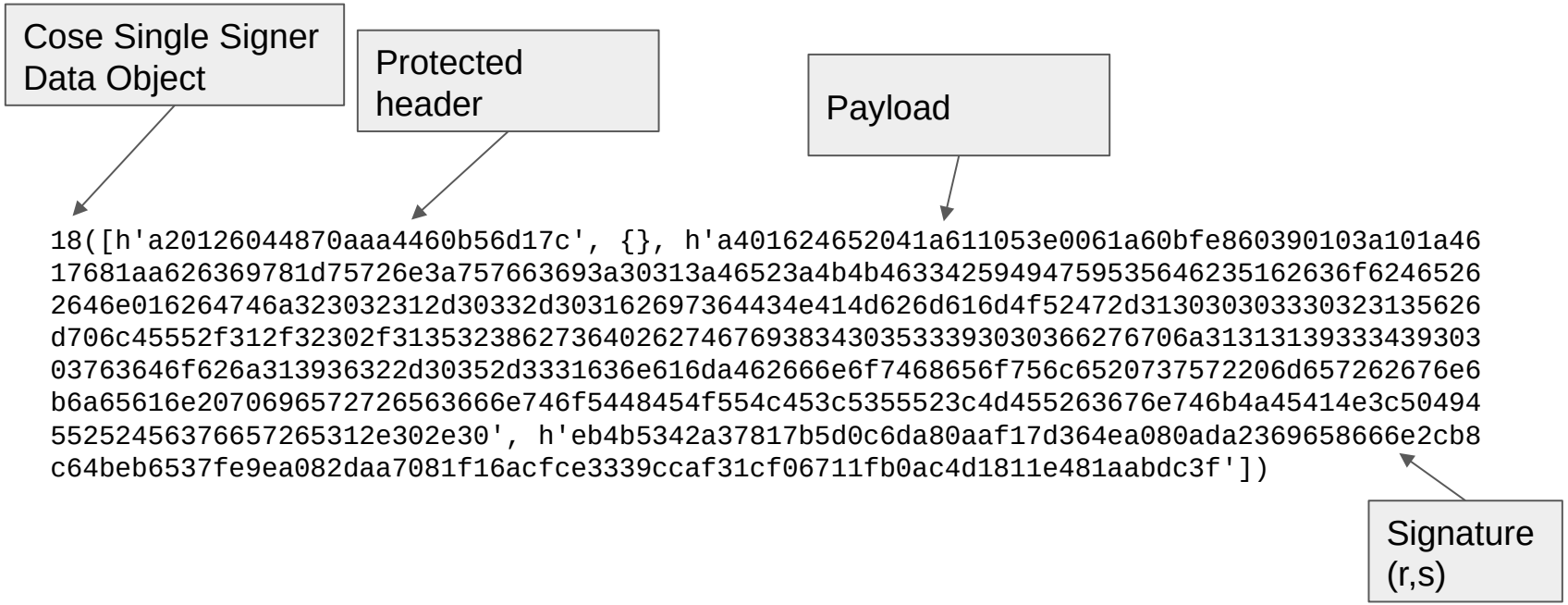
Decompressing with zlib (http://www.zlib.net/)

Result is binary JSON - CBOR (https://cbor.io/)

Start reading with cbordump for example (https://github.com/intel/tinycbor)

Digging into the envelope

COSE encoded envelope : RFC 8152 (https://datatracker.ietf.org/doc/html/rfc8152)



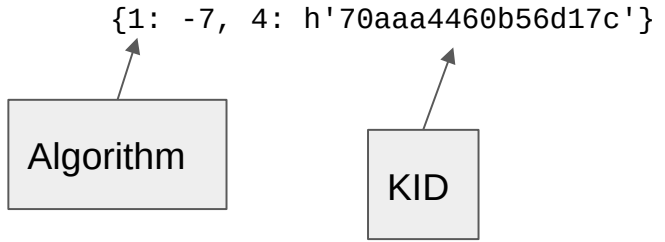
Reading the header

Validating the algorithm (signing with secp256r1 if you're not in Lithuania)

Identifying the key related to the KID

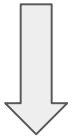
Public trust lists
https://github.com/section42/hcert-trustlist-mirror/blob/main/trustlist_fr.json

(key of each entry is the base64 encoded kid)



Interlude : reading the public key when you're in a hurry

```
"publicKeyPem":
"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEImIFaugzwB5f/VyfQ3KTfTSoukwAPVSg
HZWrtrc2j4FuAUpw/ObRnA9pBjN/HdUc1zcl9SO/vsCEnHkXhxjz4Q=="
```

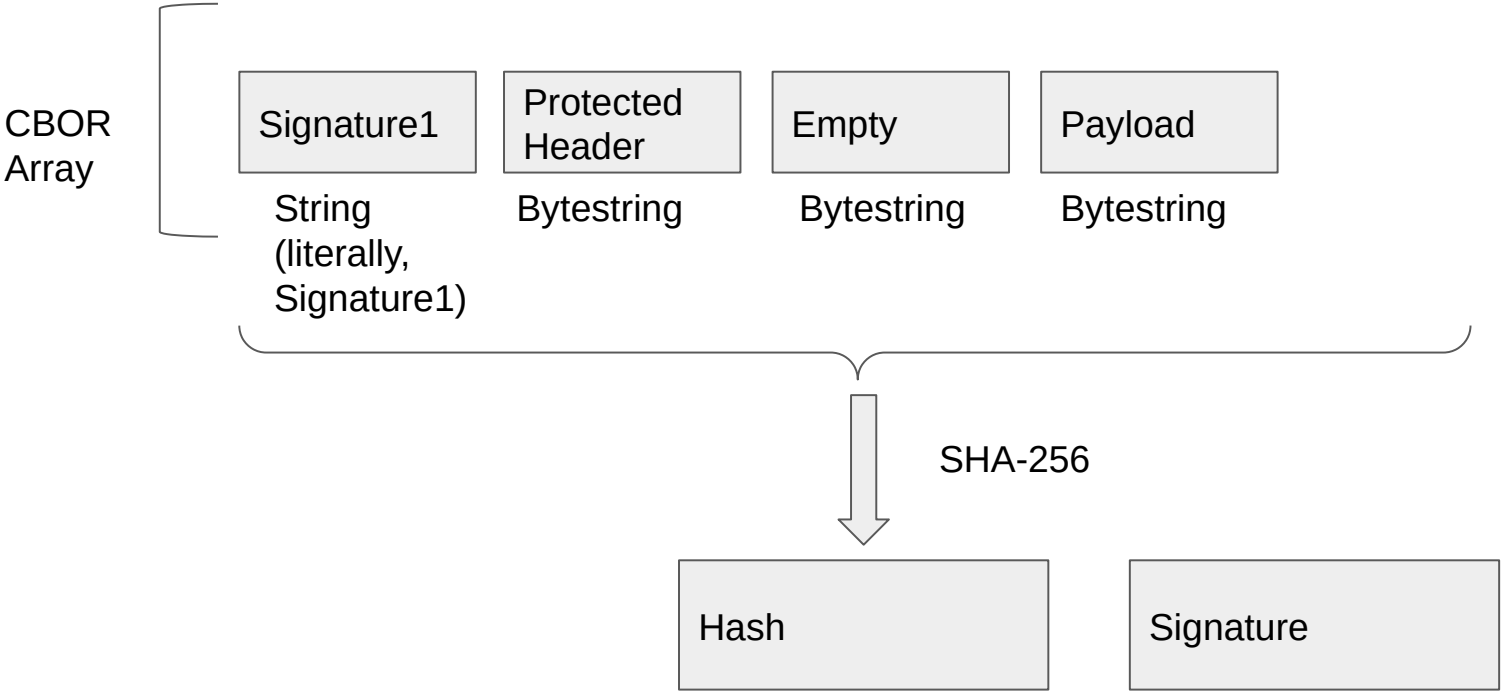


base64 decoding

```
3059301306072a8648ce3d020106082a8648ce3d03010703420004
2262056ae833c01e5ffd5c9f4372937d34a8ba4c003d54a01d95ab
b6b7368f816e014a70fce6d19c0f6906337f1dd51cd73725f523bf
bec0849c79178718f3e1
```

[:-65]

Verifying the DGC signature



Reading the payload

Ledger

Expiration date

Issuance date

Vaccine information

```
{1: "FR", 4: 1628460000, 6: 1623189600, -260: {1: {"v": [{"ci": "urn:uvci:01:FR:KKF3BYIG
YSVF#Q", "co": "FR", "dn": 1, "dt": "2021-03-01", "is": "CNAM", "ma": "ORG-100030215", "
mp": "EU/1/20/1528", "sd": 2, "tg": "840539006", "vp": "1119349007"}], "dob": "1962-05-3
1", "nam": {"fn": "theoule sur mer", "gn": "jean pierre", "fnt": "THEOULE<SUR<MER", "gnt
": "JEAN<PIERRE"}, "ver": "1.0.0"}}}
```

Current doses

Doses needed

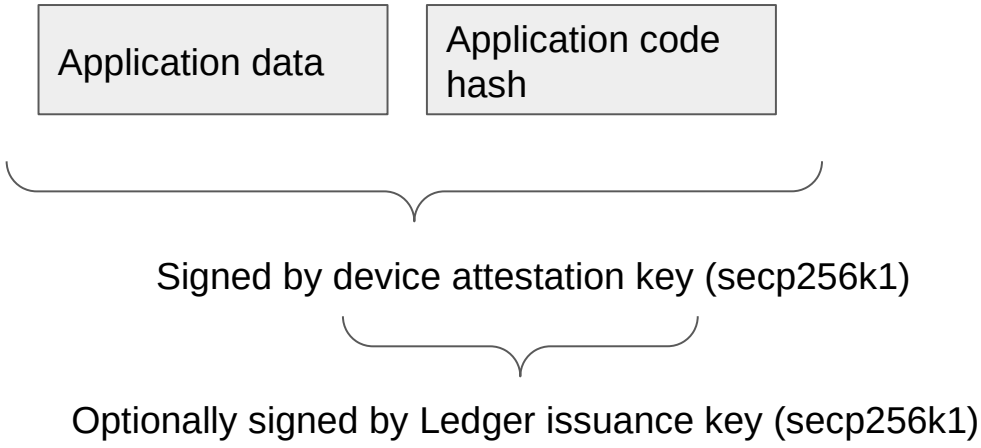
Standardized last name

Standardized first name

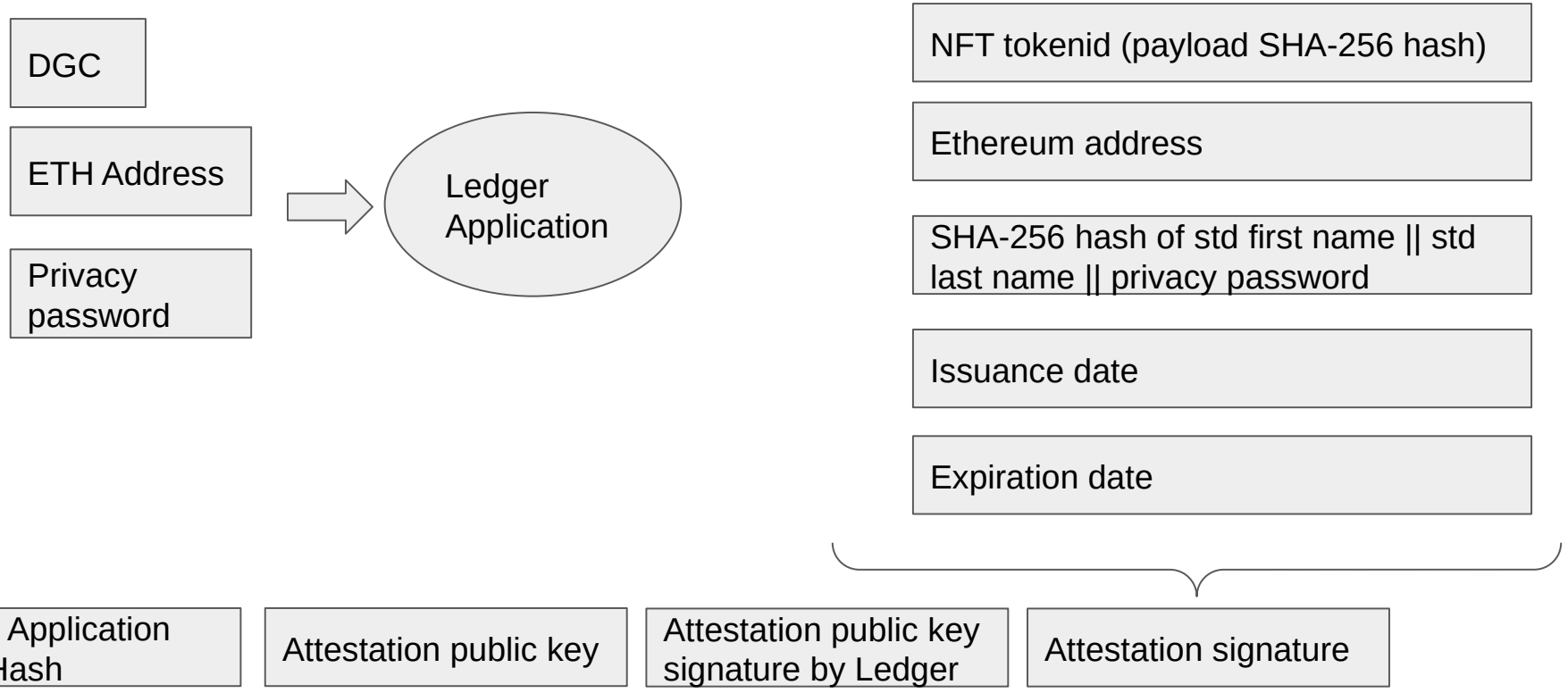
Ledger as a Trusted Computing platform

Open development environment (https://developers.ledger.com)

Attestation mechanism, optionally stamped by Ledger (https://buildmedia.readthedocs.org/media/pdf/ledger/latest/ledger.pdf 9.2.2)



Digital Green Certificate receipt



Minting smart contract logic

Verify that the format of the receipt is correct

Verify that the device attestation public key is signed by Ledger

Verify that the receipt data is signed by the device attestation public key

Mint to the Ethereum address provided in the receipt, using the receipt tokenid

Stores the original address onchain

Hard part of the job already done by Provable some time ago (
https://github.com/provable-things/ethereum-api/blob/master/provableAPI_0.6.sol#L1142
)

Fun with the NFT

Ledger

Single tap proof that the NFT has been issued for the correct address and key (for example ETH message signing of the current timestamp)

Pfizer Slock.it powered door only opens if you’re vaccinated with the right product

[your creative idea here]

Next things to do

Ledger

Support more Trusted Computing platforms (new SGX ECDSA attestation ?)

Same thing with a zero knowledge proofs and moon maths ?

Wer code ser ?

Ledger

Soon (™) - likely next week

Will point to it on twitter (@btchip)

Thank you
@btchip