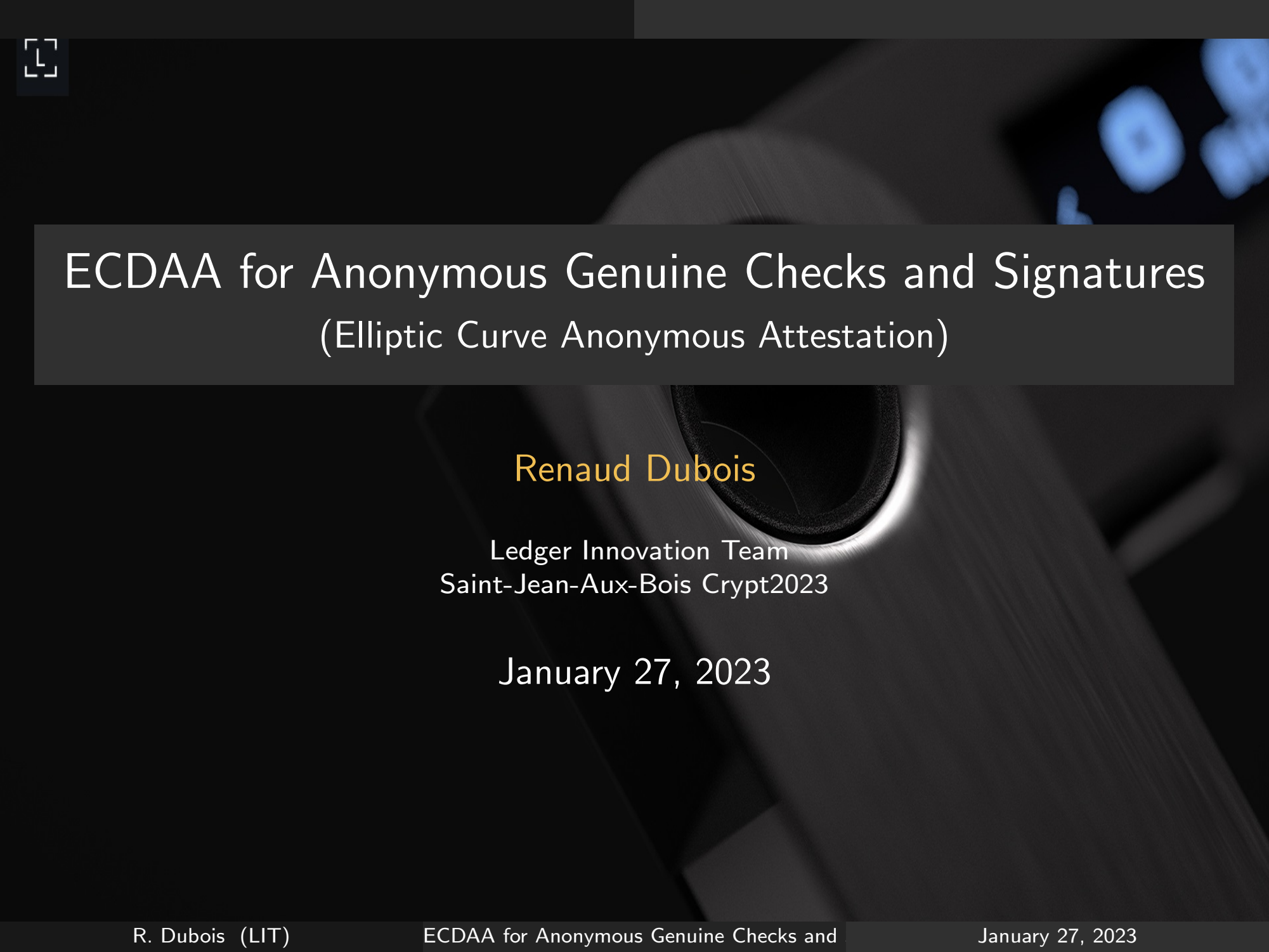


ECDAA for Anonymous Genuine Checks and Signatures

(Elliptic Curve Anonymous Attestation)

Renaud Dubois

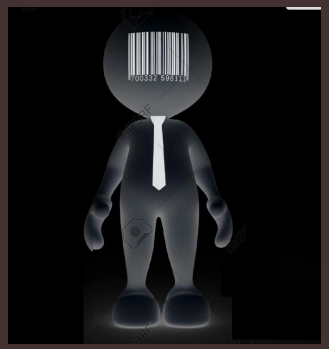
Ledger Innovation Team
Saint-Jean-Aux-Bois Crypt2023

January 27, 2023

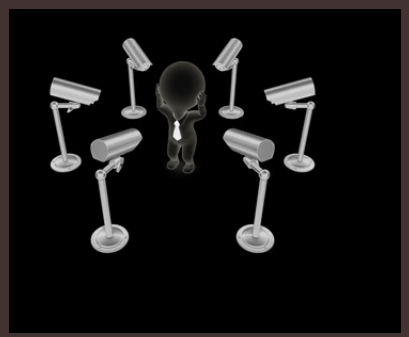
The Fight for Privacy

Stakes

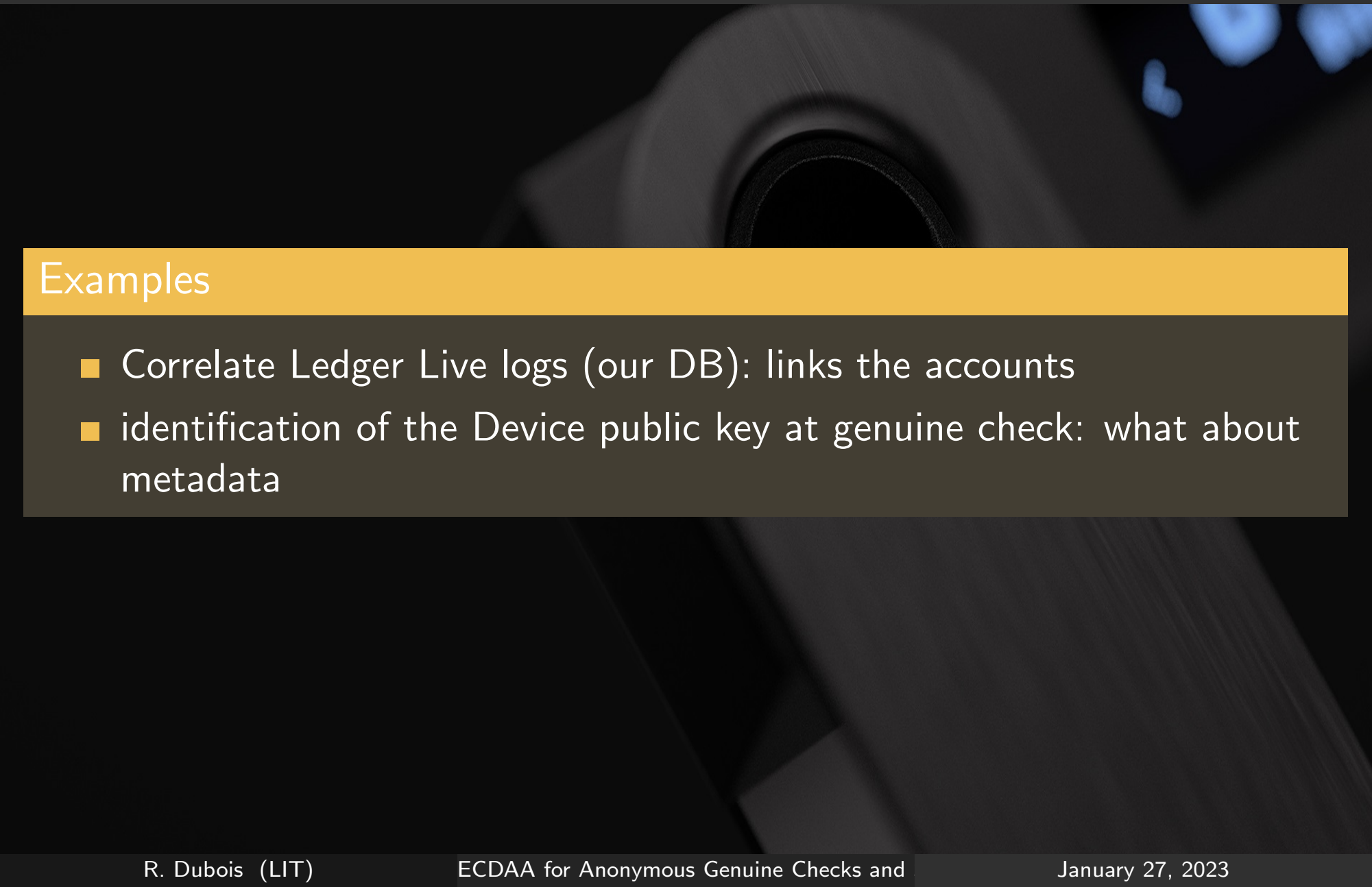
- Threat 1 : value your privacy or you're the product



- Threat 2 : Legislator surveillance



The Fight for Privacy

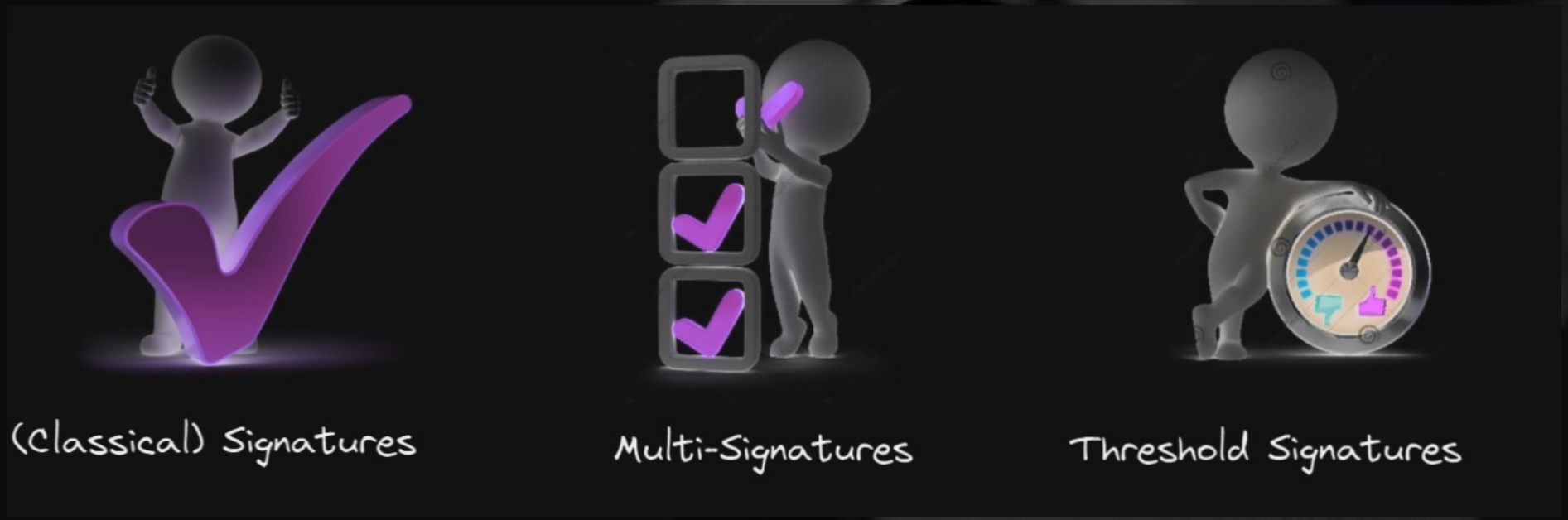


Examples

- Correlate Ledger Live logs (our DB): links the accounts
- identification of the Device public key at genuine check: what about metadata

Summary

Signatures schemes



ECDSA Musig2 FROST

Starknet meetup presentation

Anonymous Signatures schemes

Additional properties

- group anonymity : The required anonymity property is that it is impossible for the verifier to identify from which member of the group the signature was issued.
- linkability: enables an entity to identify if two signatures of the same message have been issued by the same user, without knowing the identity of that user.

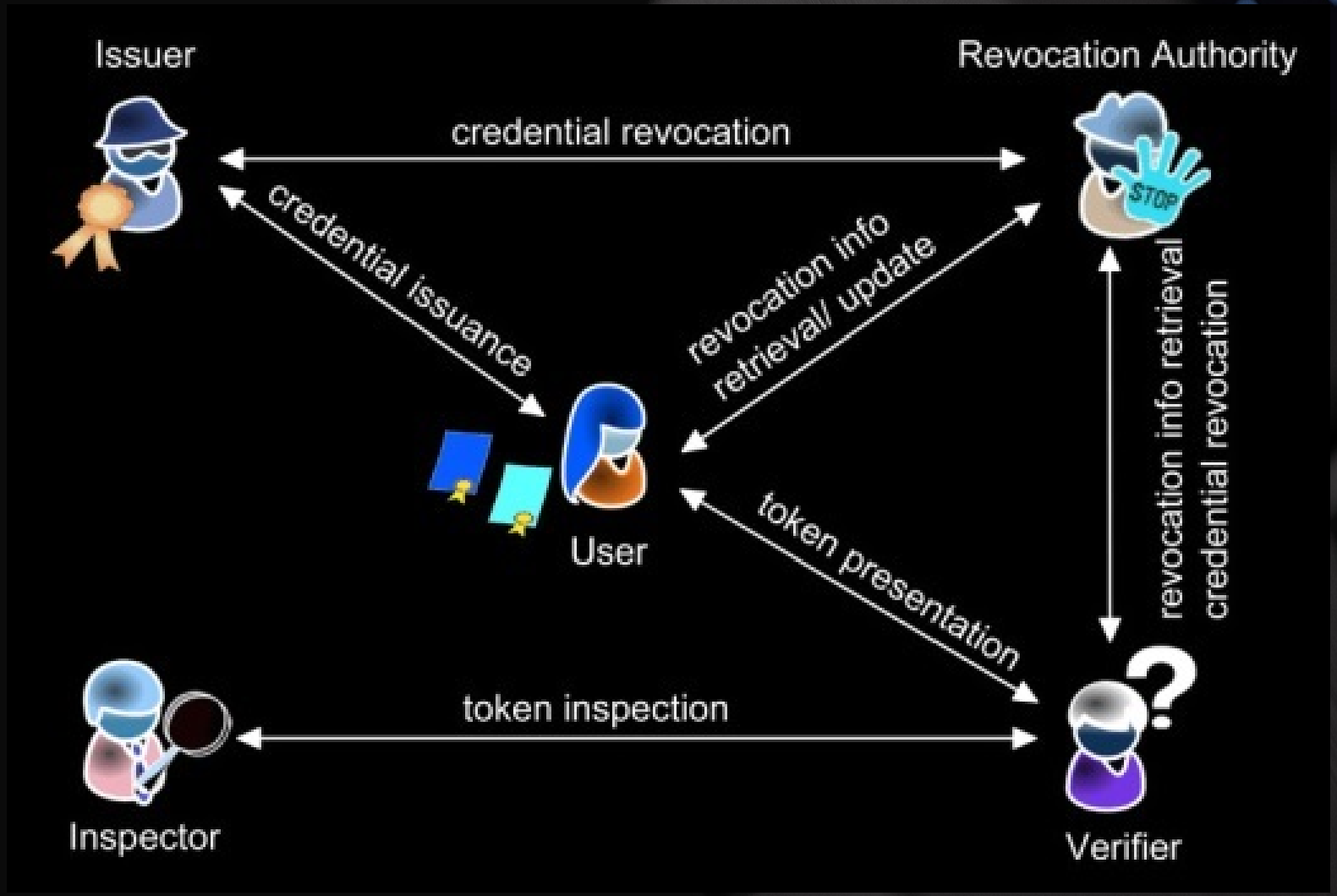
Anonymous Signatures schemes

Schemes

- Decentralized : Ring Signatures, Linkable Ring Signatures (blog post).
- Centralized : Anonymous Attestations

In Decentralized schemes, user select the Ring, in centralized there is an additional entity: the issuer.

Anonymous Credentials

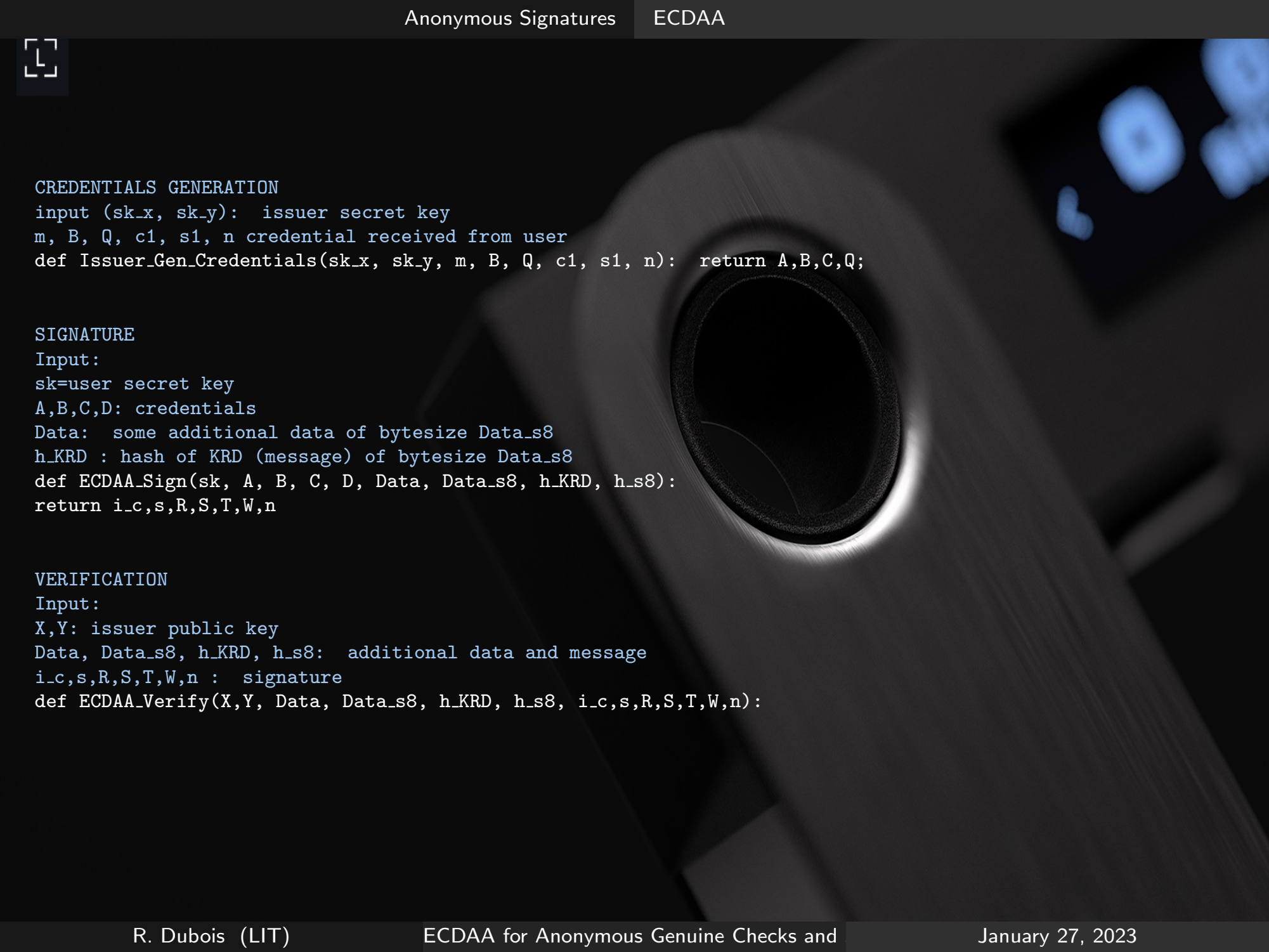


ECDAA

ECDAA is anonymous, linkable and centralized.
FIDO 2 draft

TCG (Trusted Computing Group)

It uses advanced cryptographic mechanisms: pairing over elliptic curves.

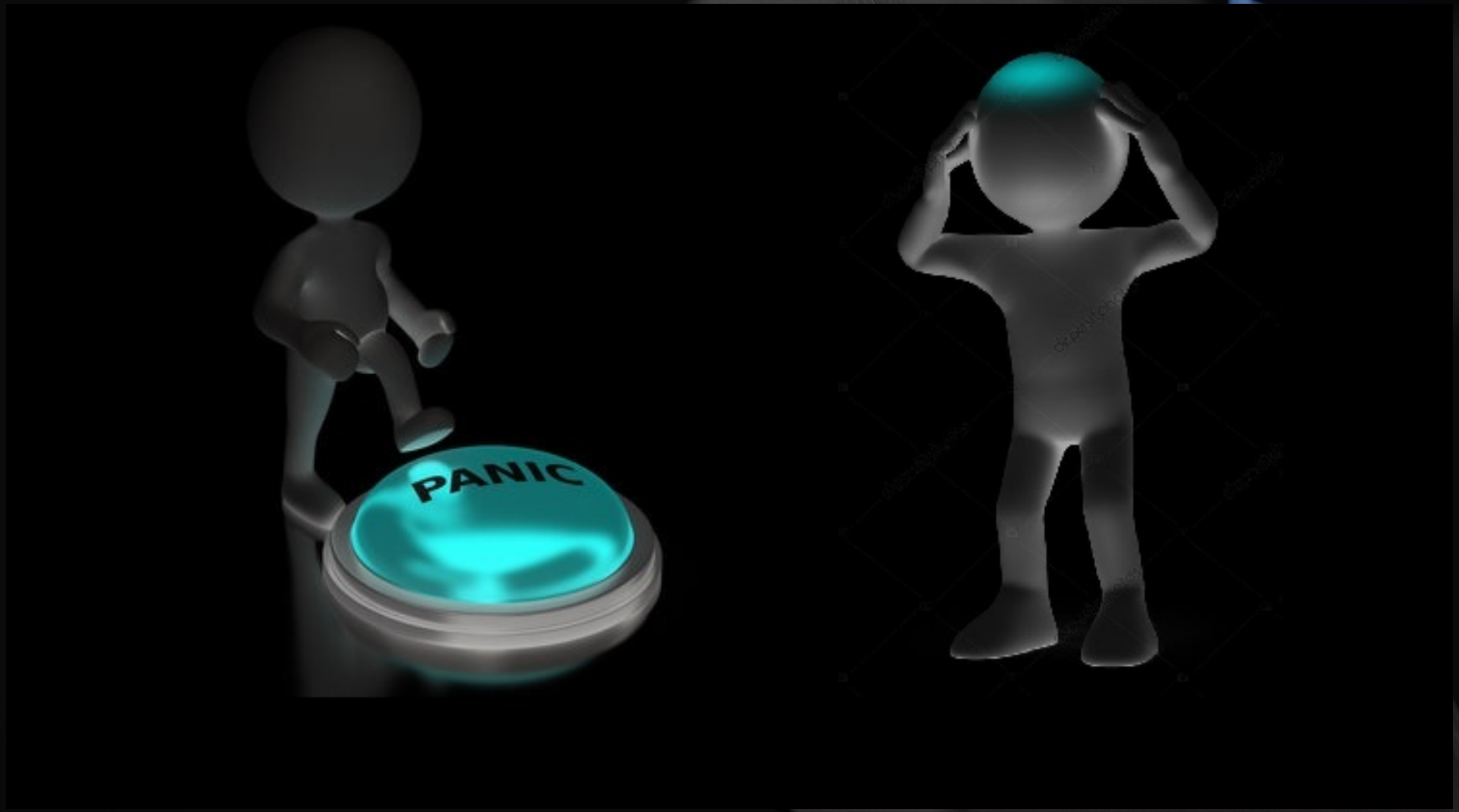


CREDENTIALS GENERATION
input (sk_x, sk_y): issuer secret key
m, B, Q, c1, s1, n credential received from user
def Issuer_Gen_Credentials(sk_x, sk_y, m, B, Q, c1, s1, n): return A,B,C,Q;

SIGNATURE
Input:
sk=user secret key
A,B,C,D: credentials
Data: some additional data of bytesize Data_s8
h_KRD : hash of KRD (message) of bytesize Data_s8
def ECDAA_Sign(sk, A, B, C, D, Data, Data_s8, h_KRD, h_s8):
return i_c,s,R,S,T,W,n

VERIFICATION
Input:
X,Y: issuer public key
Data, Data_s8, h_KRD, h_s8: additional data and message
i_c,s,R,S,T,W,n : signature
def ECDAA_Verify(X,Y, Data, Data_s8, h_KRD, h_s8, i_c,s,R,S,T,W,n):

Disclaimer



Pairing Based Cryptography

Pairing stands for the bilinear map property of Pairing-friendly curves:

$$e(aP, bq) = e(P, Q)^{ab}$$

$$e(P, Q + R) = e(P, Q).e(P, R)$$

In classical ECC, the space of exponent is linear and enables a wild lot of things (ECDSA, ECDH). The secret function applied to build the protocol is linear. Very roughly, the secret function in PBC is quadratic.
Composing linear function,leads to degree 1, composing bilinear you can do anything !

Pairing Based Cryptography

This extra degree of freedom enables powerfull features:

- short digital signatures that are efficiently aggregatable
- identity-based cryptography
- single-round multi-party key exchange
- KZG commitments.
- Snarks
- Ring, linkable, anonymous signatures

Pairing Based Cryptography

Pairing are more complex to implement:

- G2 : requires quadratic extension field (it is like using complex numbers over FF)
- GT: requires dodecaic field (imagine complex numbers, but in dimension 12)

G1 Generator
G1x
0x17F1D3A73197D7942695638C4FA9AC0FC3688C4F9774B905A14E3A3F171BAC58
G1y
0x08B3F481E3AAA0F1A09E30ED741D8AE4FCF5E095D5D00AF600DB18CB2C04B3ED

G2 Generator

G2x
11559732032986387107991004021392285783925812861821192530917403151452391805634*i +
10857046999023057135944570762232829481370756359578518086990519993285655852781
G2y
40823678758634336813322034031454355683168513275934012081057410762141200935 31*i+
84956539231234314176049732474892724384181905872636001487702806493069581019 30

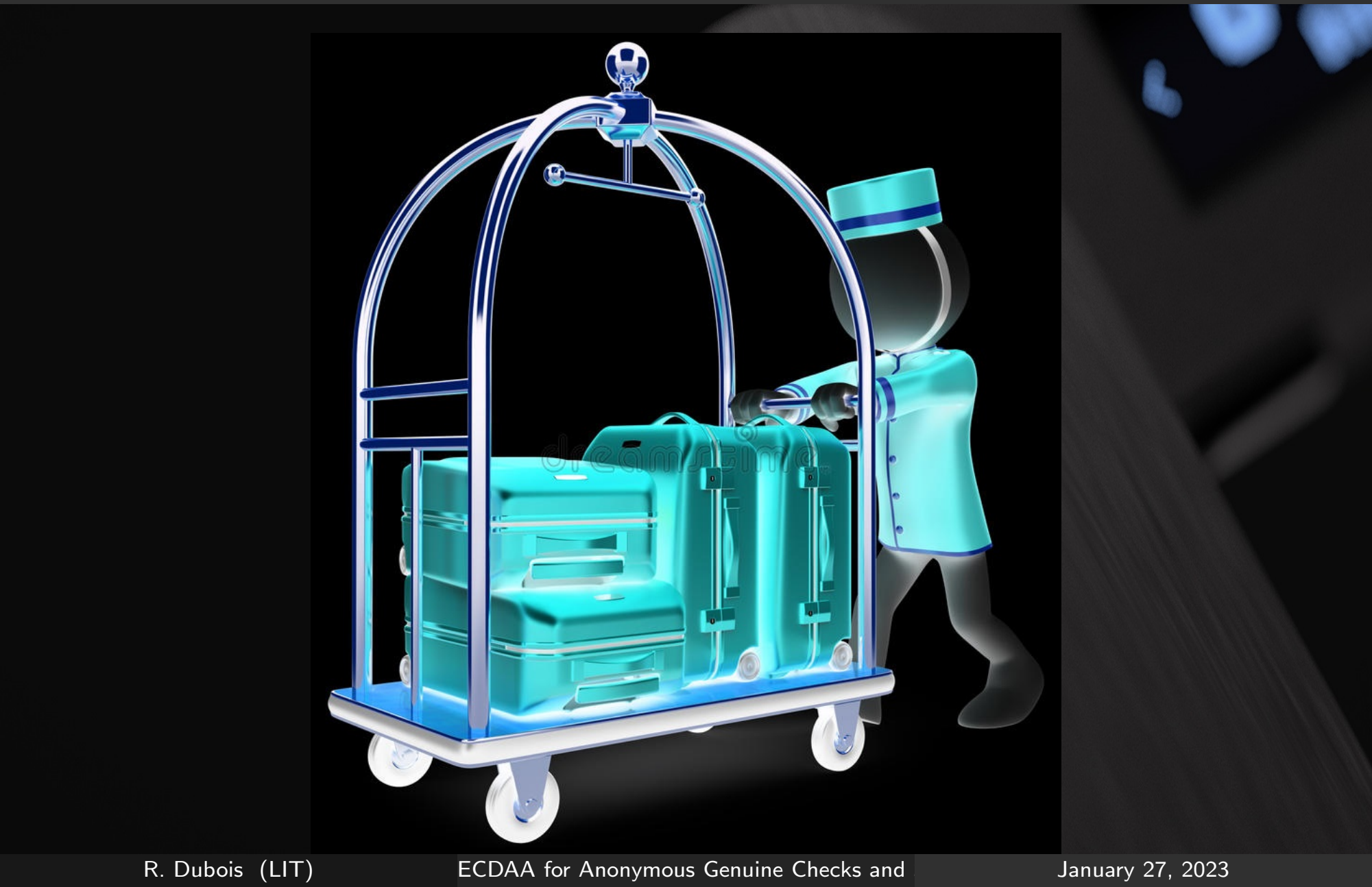
Pairing Based and EVMs

Available in solidity as precompiled over the curve altbn128 (bn254 ethereum):

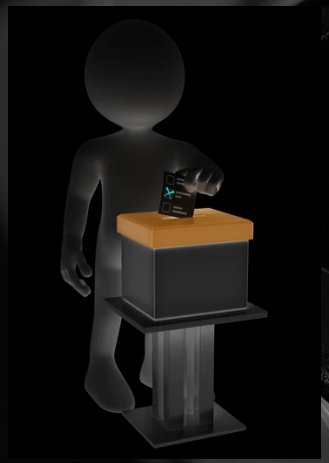
0×06	ecAdd	150	x1 y1 x2 y2	x y	Point addition (ADD) on the elliptic curve 'alt_bn128'
0×07	ecMul	6000	x1 y1 s	x y	Scalar multiplication (MUL) on the elliptic curve 'alt_bn128'
0×08	ecPairing	45000	x1 y1 x2 y2 ... xk yk	success	Bilinear function on groups on the elliptic curve 'alt_bn128'

Available in Cairo through Nethermind and Garaga.
Notice that the cost of a pairing is x15 compared to a ecRecover (ECDSA).
Not available in Nano.

Use cases

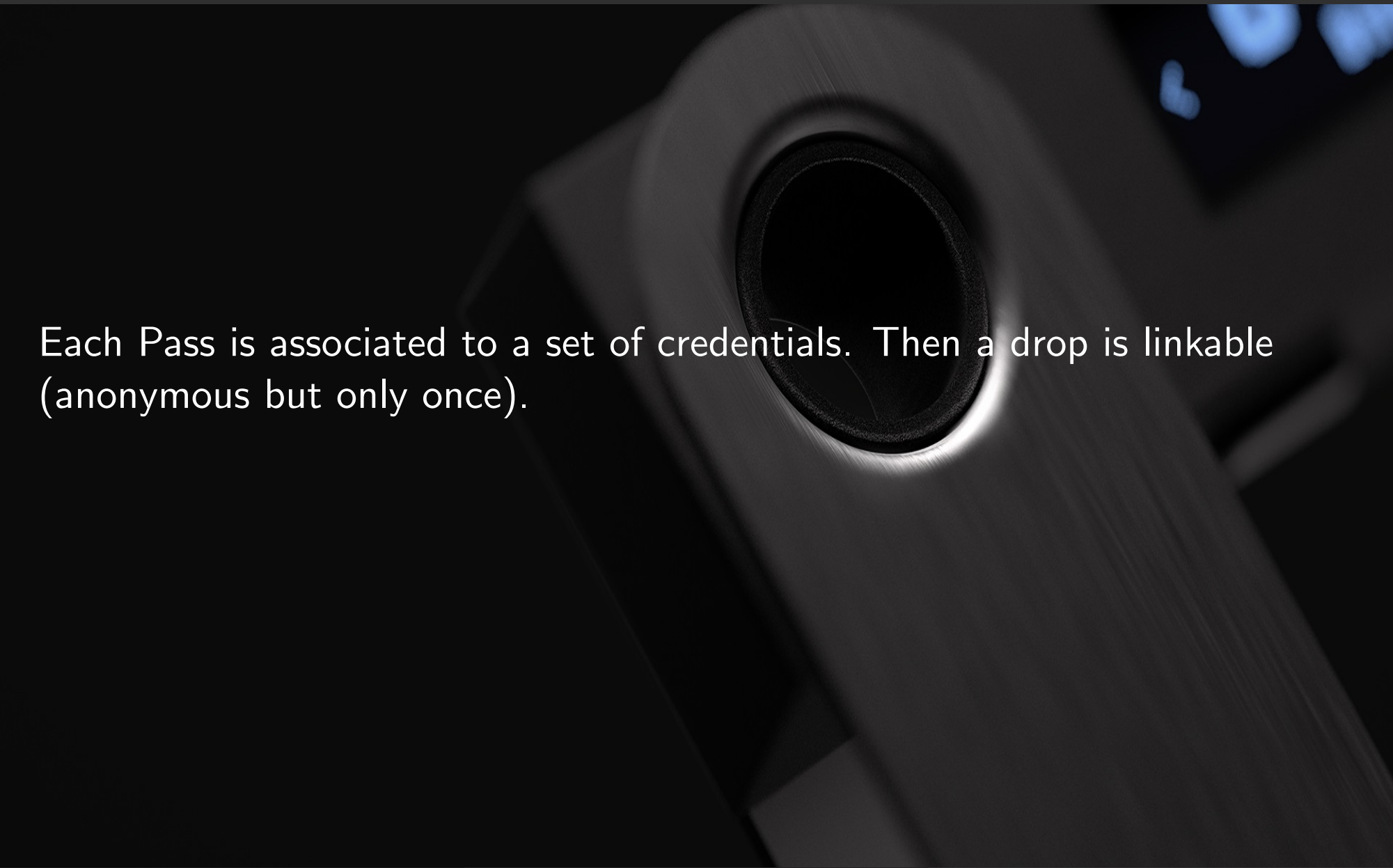


ZKProof-of-Ledger :Genuine Check



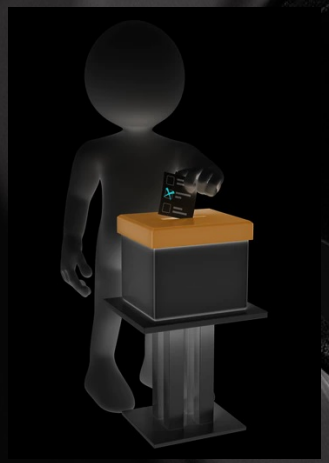
Each time a Nano authenticates, use ECDAA, LL doesn't learn anything other than genuinity.
No linkability required.
The credentials could be deterministically generated for anti replay.

Safe and Private Infinity Pass: Airdrop

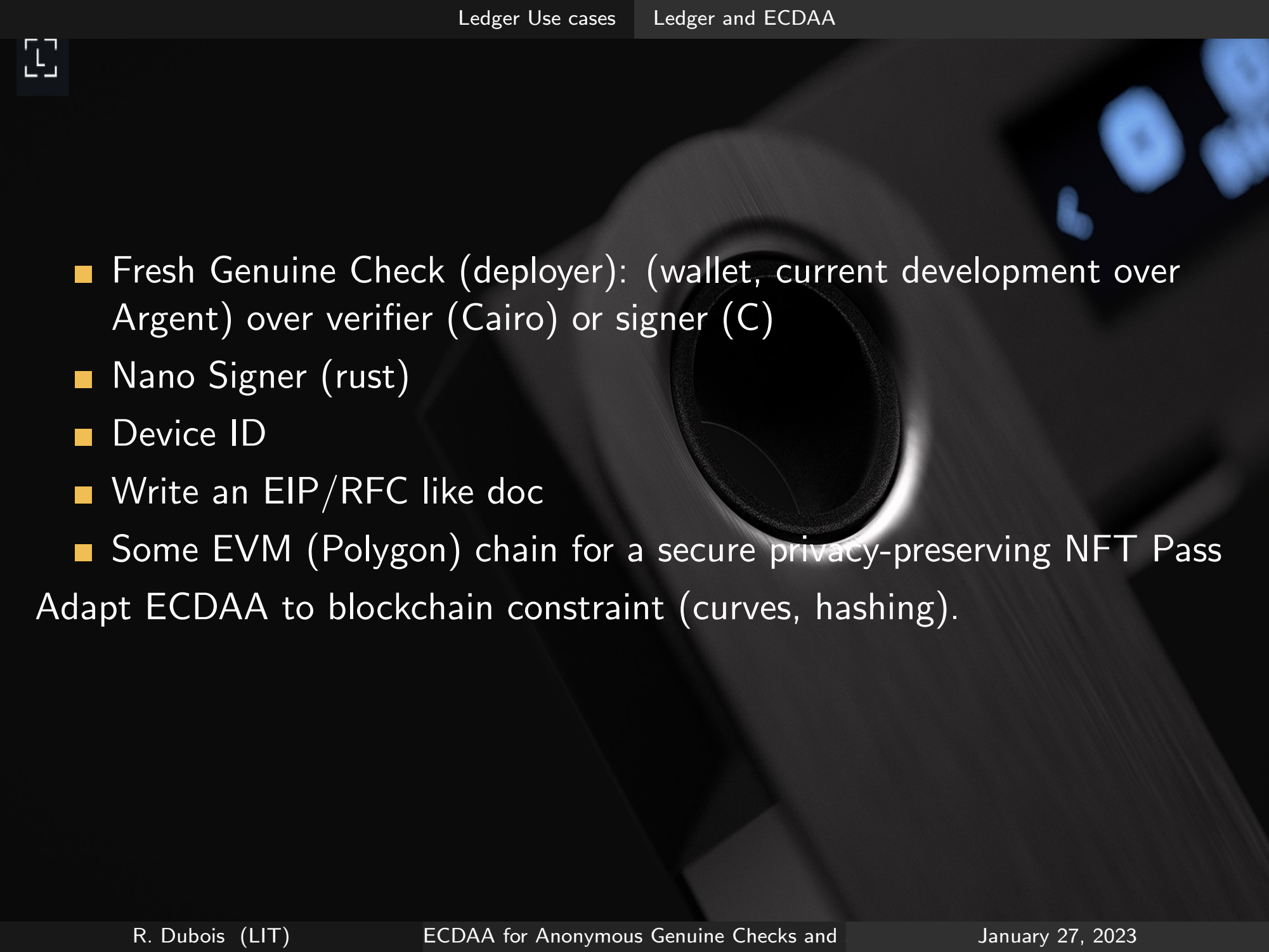


Each Pass is associated to a set of credentials. Then a drop is linkable (anonymous but only once).

Voting system

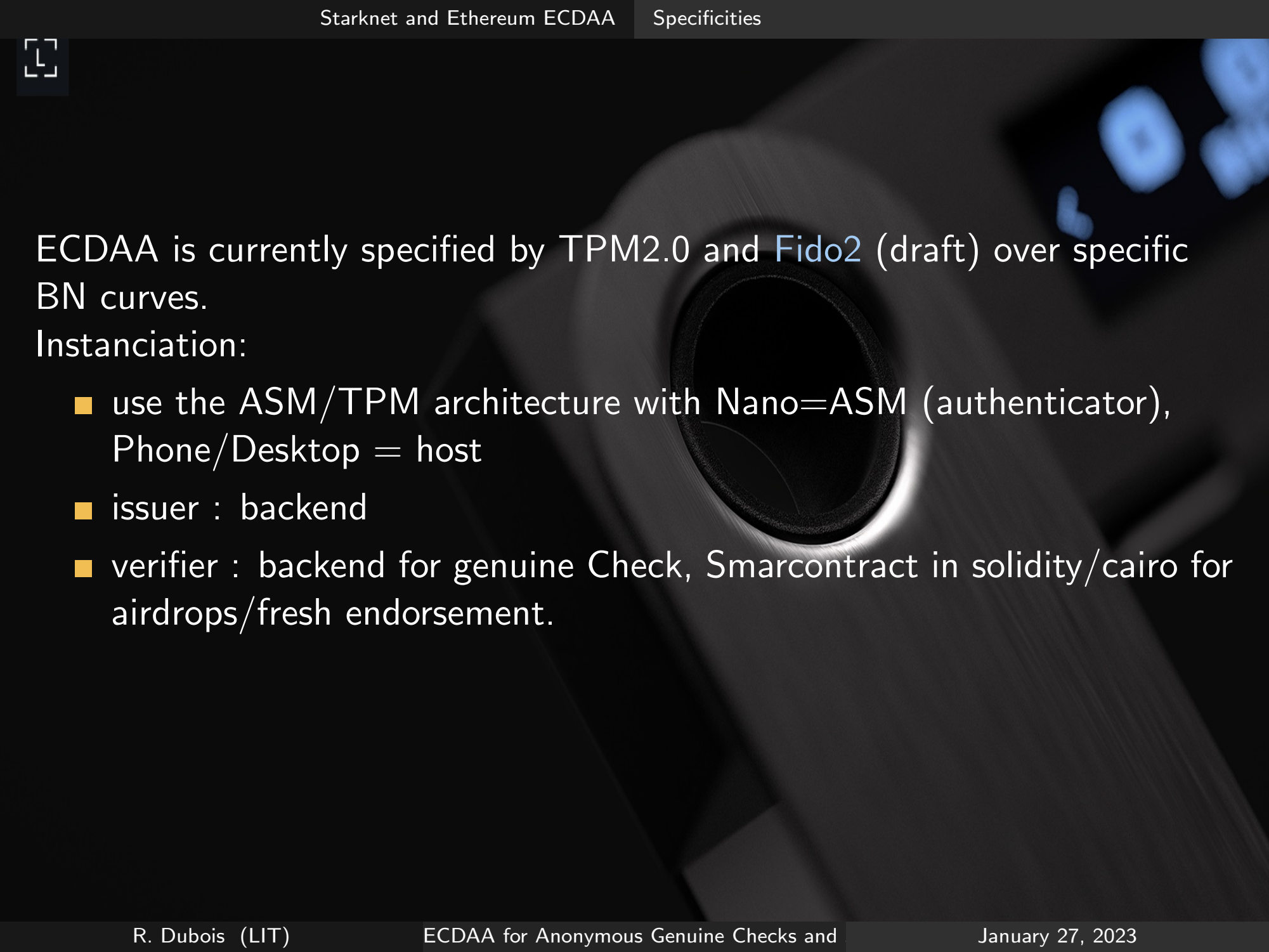


Each vote is a linkable signature of a given message.
Tag=’election’, Message=’Nico President’, ECDAA(credentials, Tag, Message).



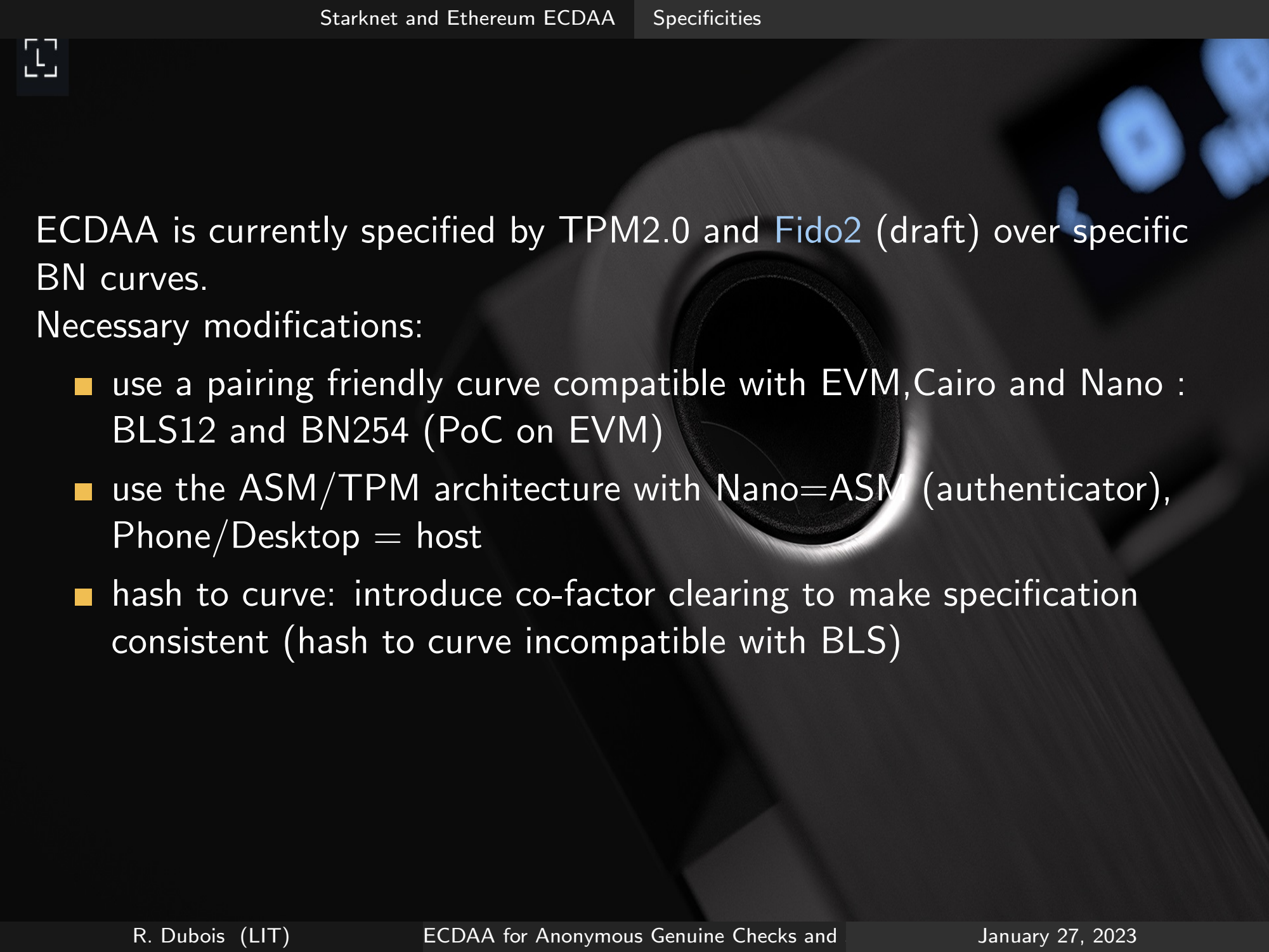
- Fresh Genuine Check (deployer): (wallet, current development over Argent) over verifier (Cairo) or signer (C)
- Nano Signer (rust)
- Device ID
- Write an EIP/RFC like doc
- Some EVM (Polygon) chain for a secure privacy-preserving NFT Pass

Adapt ECDAA to blockchain constraint (curves, hashing).



ECDAA is currently specified by TPM2.0 and Fido2 (draft) over specific BN curves.
Instanciation:

- use the ASM/TPM architecture with Nano=ASM (authenticator), Phone/Desktop = host
- issuer : backend
- verifier : backend for genuine Check, Smarcontract in solidity/cairo for airdrops/fresh endorsement.



ECDAA is currently specified by TPM2.0 and Fido2 (draft) over specific BN curves.
Necessary modifications:

- use a pairing friendly curve compatible with EVM,Cairo and Nano : BLS12 and BN254 (PoC on EVM)
- use the ASM/TPM architecture with Nano=ASM (authenticator), Phone/Desktop = host
- hash to curve: introduce co-factor clearing to make specification consistent (hash to curve incompatible with BLS)

Status

Current status:

Target	Completion	Comment
Simulation (HLS)	95%	Add more testing
Cairo	5%	working on synchronization of hash over curve
Solidity	10%	All building blocks synchronized Perfect Guild Training !
Nano	0%	Need Dev NanoX Grom, let's rust it !
Back end	0%	use of HLS for PoC

Questions ?

C Library

SCAN ME

Slides

SCAN ME

Cairo&Sage

SCAN ME