## **SPÉCIFICITÉS**

| Lancée en 2017  |
|---|
| Un processus d'auto-amendement du protocol piloté par une gouvernance onchair<br>permet d'éviter les hardfork |
| Liquid Proof of Stake   |
| Michelson VM, prouvée en Coq  |
| Token natif \$XTZ (prononcé « tez »)  |
| Standards FA1.2 (FT) & FA2 (multi-assets)   |

#### MIAGE M2 - QUALITÉ DU SI - THOMAS HAESSLÉ & QUENTIN BURG



# **TEZOS**

**SPÉCIFICITÉS** 

Lancée en 2017



Un processus d'auto-amendement du protocol piloté par une gouvernance onchain permet d'éviter les hardfork

**Liquid Proof of Stake** 

Michelson VM, prouvée en Coq

Token natif \$XTZ (prononcé « tez »)

Standards FA1.2 (FT) & FA2 (multi-assets)

MIAGE M2 - QUALITÉ DU SI - THOMAS HAESSLÉ & QUENTIN BURG

# **CONTRATS**

**TEZOS** 

Tout contrat dispose d'un compte de XTZ (account model != UTXO model)

### Deux types d'adresses:

- Les contrats implicites, liés à un manager qui possède la clé privée. Le hash de la clé publique correspond à l'adresse, précédé par "tz1" (Ed25519 curve), "tz2" (Secp256k1 curve), or "tz3" (P256 curve), en fonction de la Signature Algorithm's elliptic curve (see ECDSA). Ces contrats disposent d'un opération "transfert" implicitement
- Les smart contracts crée par une opération "origination". Ils n'ont pas de pair de clés publique/privée. Leur adresse débute par "KT1"