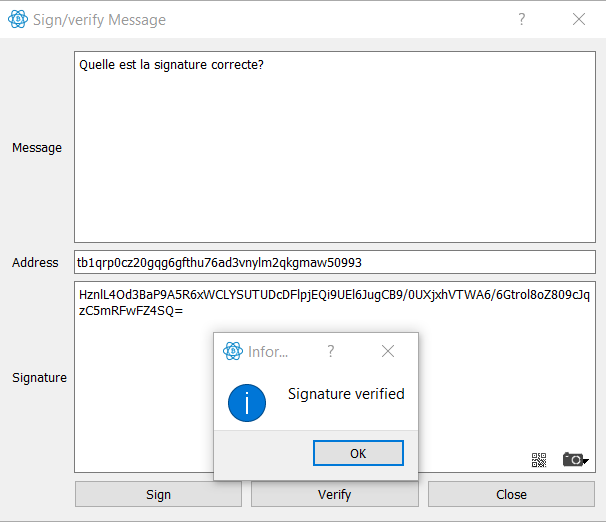
TD1 – Blockchain Programming :

Tom LERO & Brandon MONCOUCUT

Tooling (5 pts)

1. Vérifiez la signature suivante:  
   message: <Quelle est la signature correcte?>  
   signature 1:IDRRouC21uq+tDDUoXE6GeEwhM+rcw3e54jVcYyEsGtrXvLJlRZxlZaHVOE6KpkWPYWohQmu9yrhtv3Pg6VLfUo=  
   signature 2: HznlL4Od3BaP9A5R6xWCLYSUTUDcDFlpjEQi9UEl6JugCB9/0UXjxhVTWA6/6Gtrol8oZ809cJqzC5mRFwFZ4SQ=



1. Vous écrivez un message, et vous le signez avec votre adresse Bitcoin
2. Vous m'envoyez un email avec
   1. La signature valide pour le point 1

HznlL4Od3BaP9A5R6xWCLYSUTUDcDFlpjEQi9UEl6JugCB9/0UXjxhVTWA6/6Gtrol8oZ809cJqzC5mRFwFZ4SQ=

* 1. Votre adresse bitcoin

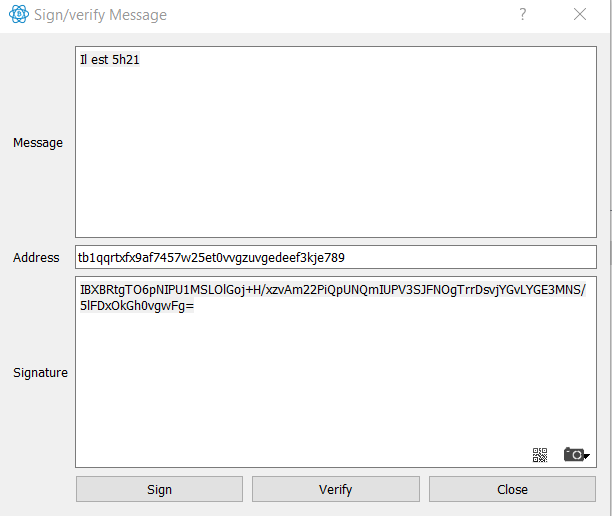
tb1qqrtxfx9af7457w25et0vvgzuvgedeef3kje789

* 1. Votre message pour le point 2

Il est 5h21

* 1. La signature pour le point 2

IBXBRtgTO6pNIPU1MSLOlGoj+H/xzvAm22PiQpUNQmIUPV3SJFNOgTrrDsvjYGvLYGE3MNS/5lFDxOkGh0vgwFg=



1. Vous chiffrez un message pour ma clé publique
2. Vous m'envoyez par email votre message chiffré, ainsi que votre clé publique

Encrypted : QklFMQOICoH3qr/6j6xk6UTGskHwDJbiD2rqY0Qh+zPdM9WTvMLnJ3ChHsypNV13nlgxwl+fMLbEqwOoHlyNDTFwZS0QhjFuIbN3ArLBnhcZn2p8Mw==

Public Key : 02c651d01dc58a76026de6fa9a892e6d434996ffaa89921edd81d5dbdb8d5fcb79

1. Je le déchiffre

ok

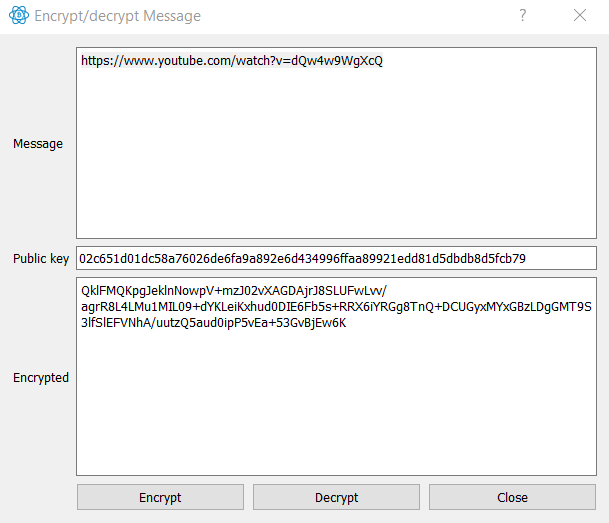
1. Je vous renvoie un message chiffré

QklFMQKpgJeklnNowpV+mzJ02vXAGDAjrJ8SLUFwLvv/agrR8L4LMu1MIL09+dYKLeiKxhud0DIE6Fb5s+RRX6iYRGg8TnQ+DCUGyxMYxGBzLDgGMT9S3lfSlEFVNhA/uutzQ5aud0ipP5vEa+53GvBjEw6K

1. Vous le déchiffrez

<https://www.youtube.com/watch?v=dQw4w9WgXcQ>

1. Vous me renvoyez le message déchiffré par email



Wallet management (5 pts)

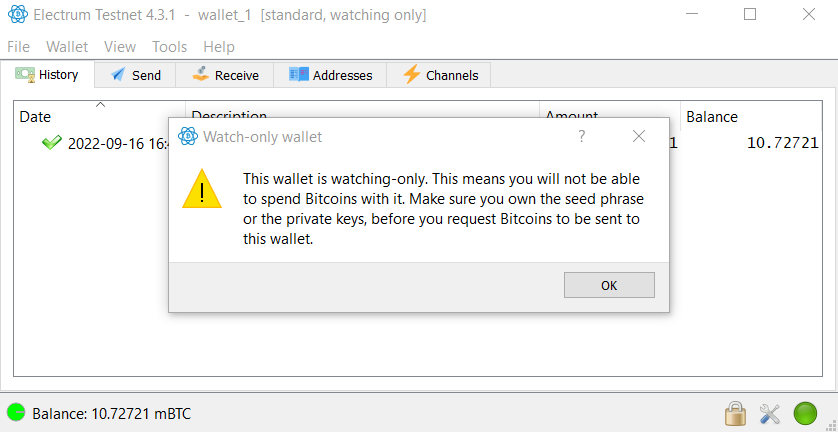
• Créer un wallet



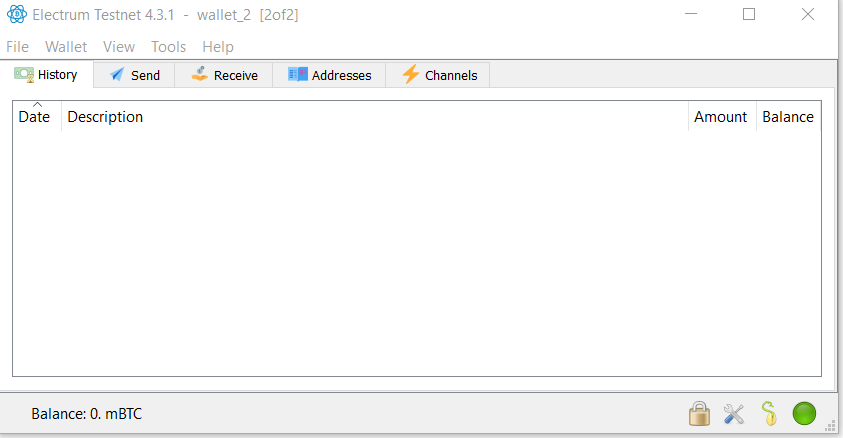
• Importer un wallet

OK

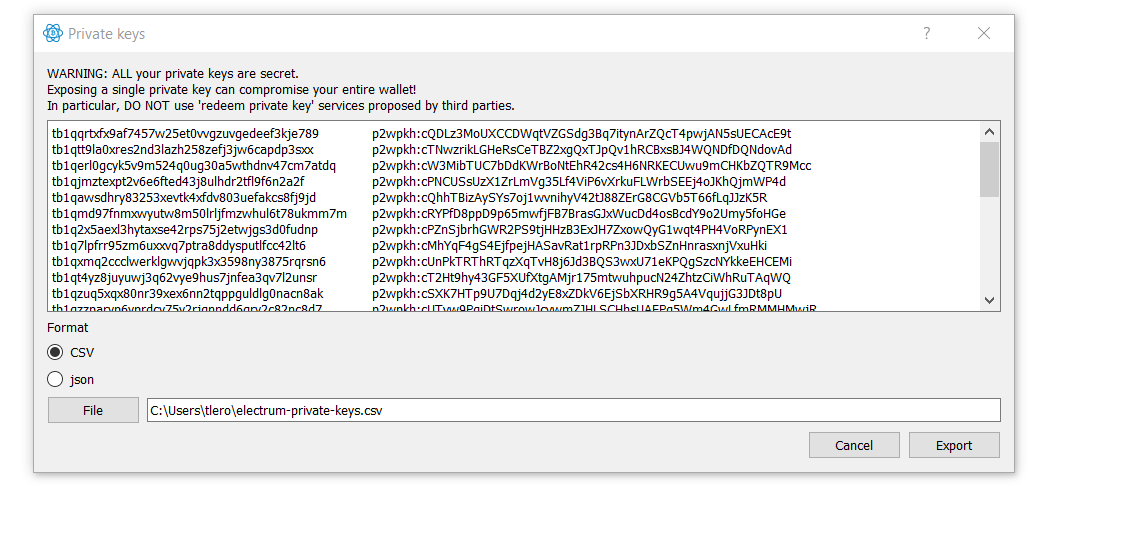
• Créer un wallet read only



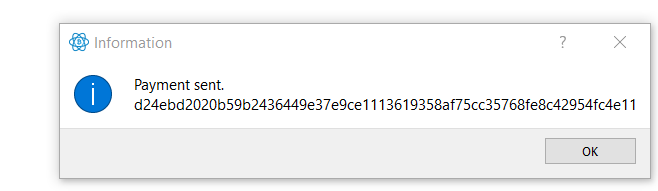
• Créer un wallet multisig



• Dump private keys

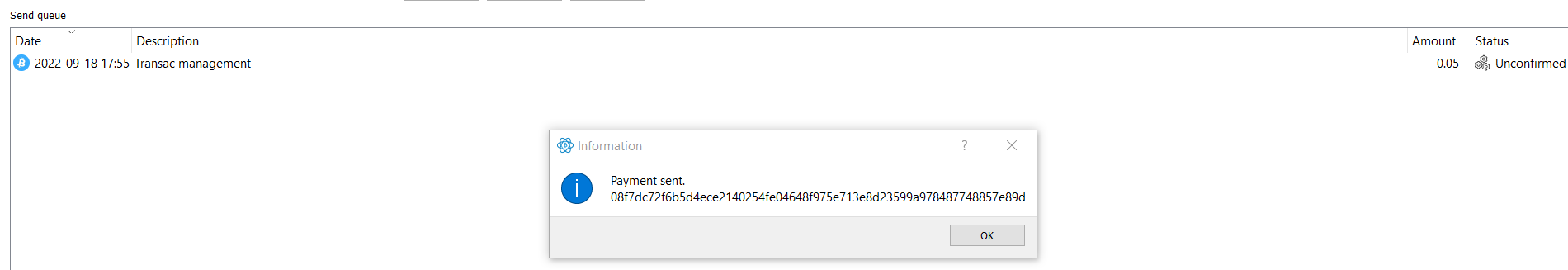


• Import private keys

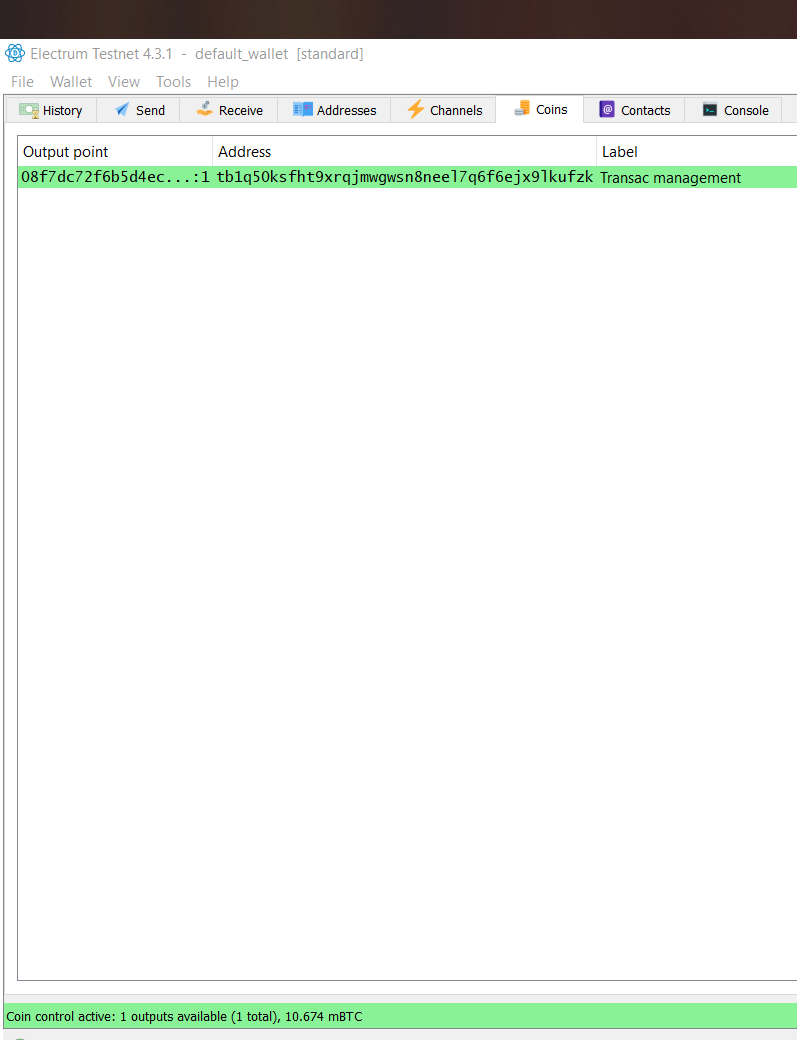


Transactions management (5 pts)

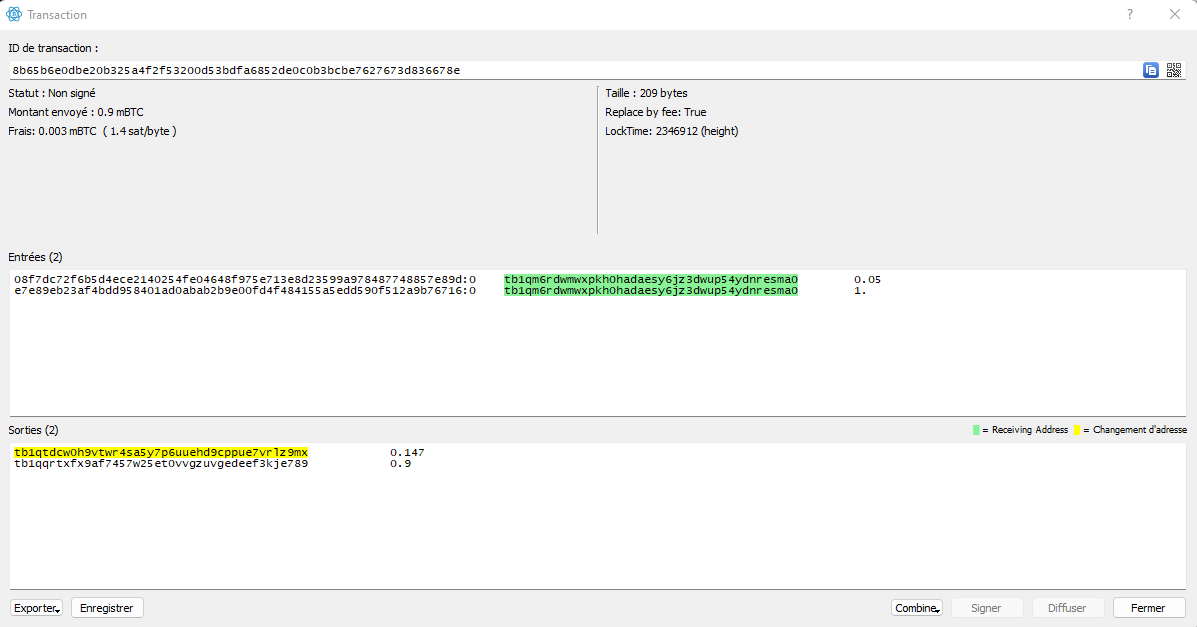
• Envoyer une tx simple



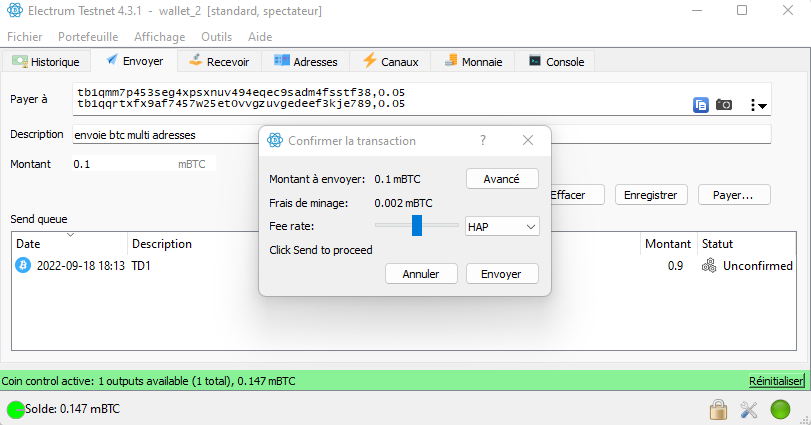
• Dépenser un UTXO specific



• Dépenser plusieurs UTXO dans une seule tx



• Envoyer des fonds à plusieurs addresses en une seule tx



• Emettre une tx multisig

• Exporter une liste des UTXOs de votre wallet

Cold storage (5 pts)

• Boot on tails

• Créer un cold wallet

• Importer un wallet read only sur une machine connectée à internet

• Créer une tx sur une machine connectée

• Signer la tx sur une machine déconnectée

• Broadcaster la tx depuis la machine connectée