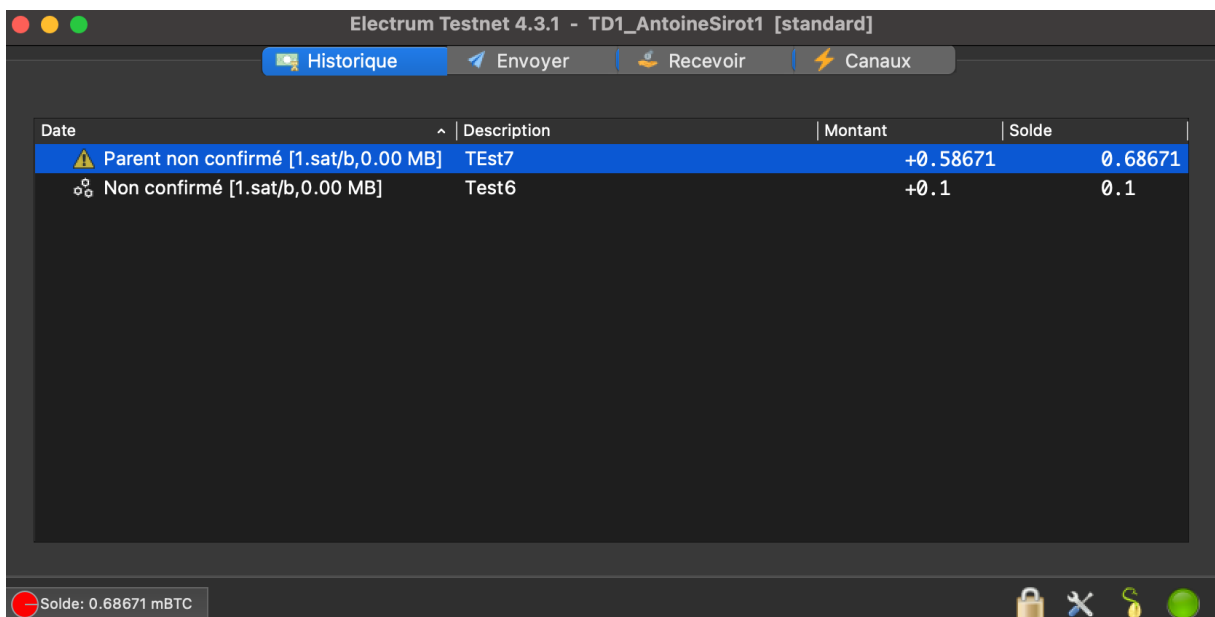


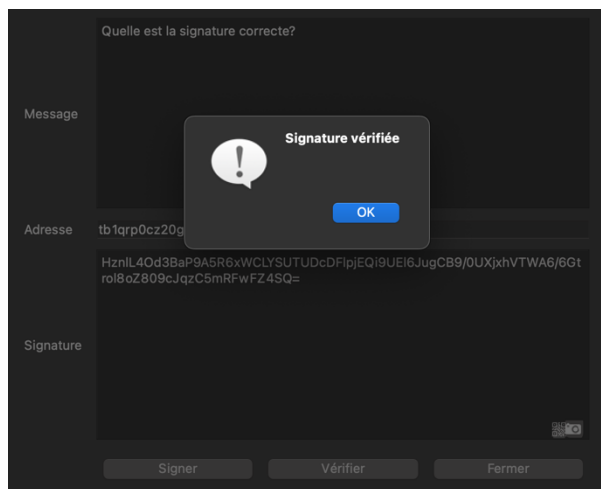
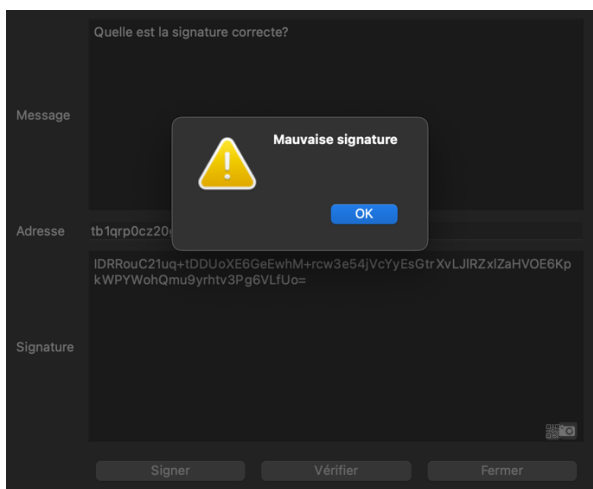
Rapport TD1 – Blockchain Programming

Partie 1 – Tooling :

Premièrement nous avons installé Electrum, nous l'avons lancé sur Testnet puis nous avons récupéré des tBCT. L'image suivante montre Electrum ouvert sur Testnet avec un solde montrant que les étapes précédentes ont été faites.



Ensuite nous avons signé tester les deux signatures que vous nous avez mis à disposition afin de trouver laquelle était la bonne (ce fut la seconde).



Nous vous avons ensuite envoyé un message chiffré que vous avez validé.

Signature correcte : la 2 (HznlL4Od3BaP9A5R6xWCLYSUTUDcDFIpiEQi9UEI6JugCB9/0UXjxhVTWA6/6Gtrol8oZ809cJqzC5mRFwFZ4SQ=)

Mon adresse Bitcoin : tb1qd3nn5qle36r6gvpt3y85hh0r7gz86na4h4rjux

Message : Test de message signé par Antoine Sirot.


Signature : ICTsew0oD+s/o2jVWtXhbp4s2gfmq+vm+tS+HDYZbEYUxIjZ8Fb0rQEz10Ne5DUDYq6vCueKqYtUQi6nJzYCpl=

Puis nous avons déchiffré le message que vous aviez chiffré avec notre clé publique.

Message	Bien reçu, merci
Clé publique	0238df3f3f9dc97c20c09ef7a2640ca2f039e327f3e311fa2996d3d3d72ce6b8
Chiffré	QkIFMQKWObKbn+1wIGG5Jdx76TzAhB/ CC2+v1OpSSct92zmQ7glfOZBDRDWzYxmo7eh9dNB8qaZJqxfjlcyzNAMKR9 qI0I5TIs+UOL1QLF8NNgaccuFic7TrNarWMQ/Skb1gewU=
<div>Chiffrer</div> <div>Déchiffrer</div> <div>Fermer</div>	

Partie 2 – Wallet Management :

Nous avons déjà créé un wallet lors de la partie 1, nous avons donc commencé cette partie par importer un wallet en utilisant une graine que nous possédions déjà.



Magasin de clés

Souhaitez-vous créer une nouvelle graine ou restaurer un portefeuille en utilisant une graine existante ?

☐ Créer une nouvelle graine


☒ Je possède déjà une graine

☐ Utiliser une clé principale

☐ Utiliser un périphérique matériel


Retour

Suivant



Saisir la graine

Veuillez saisir votre graine pour restaurer votre portefeuille.



two usage dash umbrella brain enemy magic false setup
interest only radar

Type de graine: segwit

Options

Retour

Suivant

Nom du portefeuille:	Portefeuille_Importé
Type de portefeuille:	standard
Type de script:	p2wpkh
Graine disponible:	Vrai (segwit)
Type de magasin de clés:	bip32
Réseau Lightning:	Activer
Lightning Node ID:	023f30b9ac3c63f8a80ad167ec0a91a5783dafa60ea9a678357475d1e88513c2bf
Clé publique maîtresse	<div> vpub5V4iGLd8RADLqWaamUE9i5MeEjXQvvLvSpbDWD5hZYhT836B55VWgrnqM2nojSp5ucSyoVtJPkMcrPBMKWkvyAqi7jFz3CwnG8wthDMebJt </div>
Chemin de dérivation:	m/0'
BIP32 root fingerprint:	7255b613

Fermer

Nous avons ensuite créé un wallet en read only (nb : le nom de ce wallet n'est pas pertinent car ce n'était pas un wallet importé mais il possède bien les caractéristiques d'un wallet en read only).

Nom du portefeuille:	Imported_Wallet
Type de portefeuille:	imported [spectateur]
Type de script:	address
Graine disponible:	Faux
Type de magasin de clés:	Pas de magasin de clés
Réseau Lightning:	Not available for this wallet.

Fermer

Nous avons par la suite créé un wallet en multisig.



Créer un nouveau portefeuille

Quel type de portefeuille voulez-vous créer ?

- ☐ Portefeuille standard
- ☐ Portefeuille avec authentification à deux facteurs
- ☒ Portefeuille multi-signatures
- ☐ Importer des adresses Bitcoin ou clés privées

Annuler

Suivant



Portefeuille multi-signatures



Choisissez le nombre de signatures nécessaires pour débloquer les fonds dans votre portefeuille :

De 2 cosignataires

Exiger 2 signatures

Retour

Suivant

Nom du portefeuille:	Multisig_Wallet
Type de portefeuille:	2of2
Type de script:	p2wsh
Graine disponible:	Vrai (segwit)
Réseau Lightning:	Not available for this wallet.

Select keystore

☒ magasin de clefs 1

☐ magasin de clefs 2

Clé publique maîtresse

Vpub5fBrqNv7yZ7RSky9FINiRghySfXYBj4FPtRhfwpmLCNK7CRaK7CCFcde4rKM4iEgQAY6YEcEzktSrfujHJBxjE1binRczaQBZeR5i4UBdj

Chemin de dérivation: m/1'


BIP32 root fingerprint: 08ead204

Fermer

Après avoir créé ce wallet nous avons dump les private keys.

address,private_key
tb1qmh3mrr5mm535nd05sc8vtk02ntpssg3x3q0jeu,p2wpkh:cPBDqC4FvzRCMSGGeWj71coCJGbGfDmNkHicSJg6UbcUxHRTAm9p
tb1qp2zfl6ww2e0jd3szmud55pqva5e8hkfdprh0t4,p2wpkh:cRGCJfmYxSV9CywjQAClLcMpgVzmn6SMHg7EAzwgMTGG445V5wH2
tb1qducm5n4xculv9hy25x8s5dla5jd9fcpevxk0ax,p2wpkh:cSqhbzNVhKWkvs817kg6UquCUgbGWVw2MsvaPBMfxxetTS8HRfpp
tb1qalpyfsr0kws2y4m58zu0ptpu7lnqralqqwfqj6,p2wpkh:cPrGBL6o8ve9xGZxmZ2EVJ89H5uCgDBW4n5DZ5qcrYnk8QoWimoa
tb1qg73zmn5ml8jqrht08cmha4vkuuqe2ukn2cygur,p2wpkh:cUZaw9diuQnD5Dc61rqsnsWB6ZqQZdq5563zjKFBmcDGmbKHjYwJ
tb1qtr3hj4v4v23vv8emwkwjutf4cppy3xmafj7y2c,p2wpkh:cVCaXohfUJ5mw3jhu72CXnkYWvsb3oKM5kf99vefUnKRfYZnG1j
tb1qgp2j5hkp0h4tupkypezkme9def6de0xq2tj6zf,p2wpkh:cTJ9FDzEW63hSaA52mD59fRwUTQCCc5vqzbN34tqAcEtKZcLwZuY
tb1qv5q38v0g5zmcjn4dh2z0mr5rw3kuhw8umdukuh,p2wpkh:cTMVWcnVQZsd5Ds5u5PQt47tZB8Yna4jBppw9D1SR6K53hdTm9HSJ
tb1q6zjc623j7mxdmh79xkk422wjgr755hlfa8u2l2,p2wpkh:cPR2d2jvggW4bagumjpFqZVXLcLYLkfznAGoP6GCKm86TZQg5NNN
tb1q7hwr58njz4c40fxm85jr5a6mstpmwm7txvxw2,p2wpkh:cQ2SZmryP8NHP9dV15BmLoFFBvwDLwBpzdfyiXM2RaFLXa3WigHA
tb1q8hehszmhmy3zm9dcjce0qf8lz3996rrqrve7re,p2wpkh:cN9trf6RNYau4zk4ydi1GyU9d4wodFAQa2c9GkLBJ8MYXSk33dLM

Puis nous en avons importé dans un autre wallet.




Créer un nouveau portefeuille

Quel type de portefeuille voulez-vous créer ?

- ☐ Portefeuille standard
- ☐ Portefeuille avec authentification à deux facteurs
- ☐ Portefeuille multi-signatures
- ☒ Importer des adresses Bitcoin ou clés privées

Annuler



Suivant



Importer les adresses Bitcoin

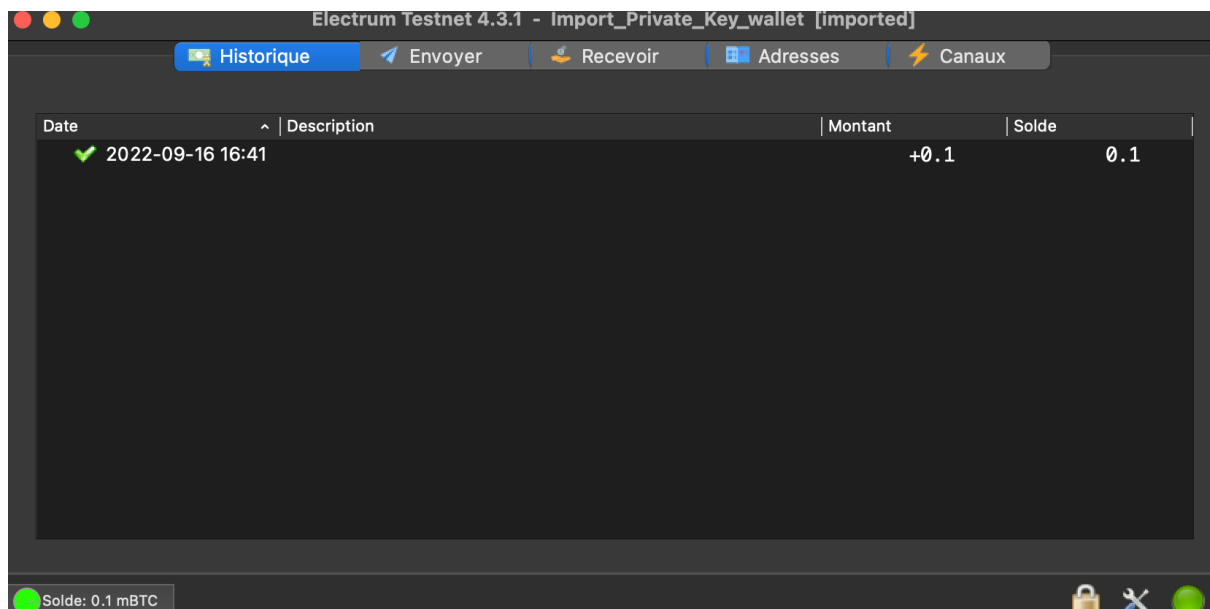
Entrer une liste d'adresses Bitcoin (cela créera un portefeuille spectateur) ou une liste de clés privées. Info

p2wpkh:cPrGBL6o8ve9xGZxmZ2EVJ89H5uCgDBW4n5DZ5qcrYnk8Qo
Wimoa
p2wpkh:cSqhbzNVhKWkvs817kg6UquCUgbGWVw2MsvaPBMfxxetTS8H
Rfpp



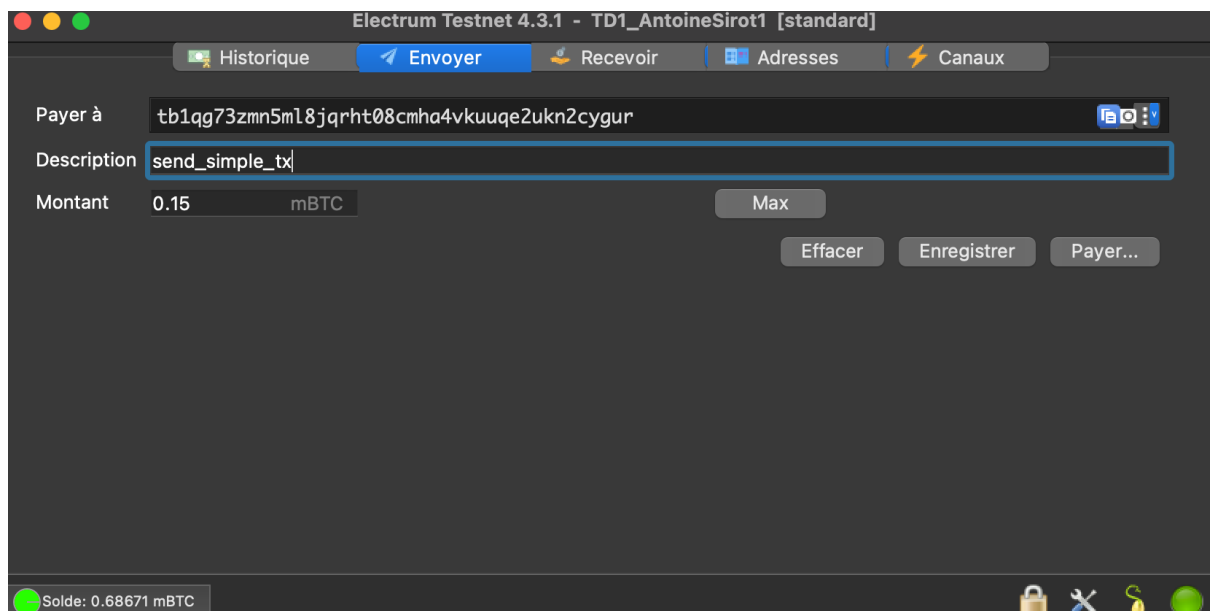
Retour

Suivant



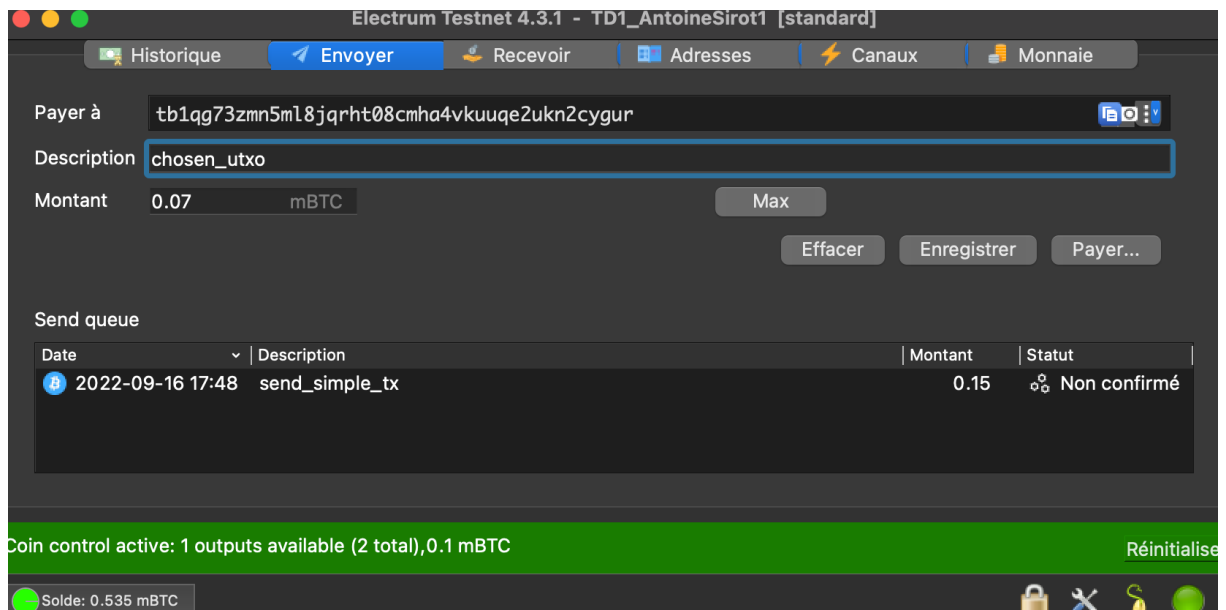
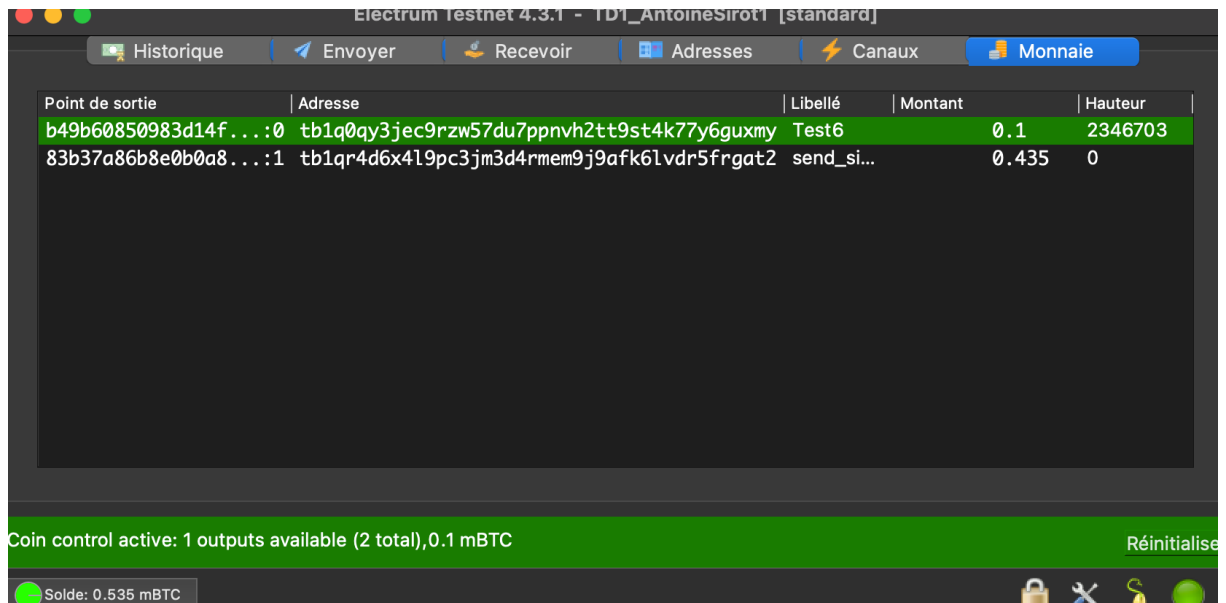
Partie 3 – Transactions Management :

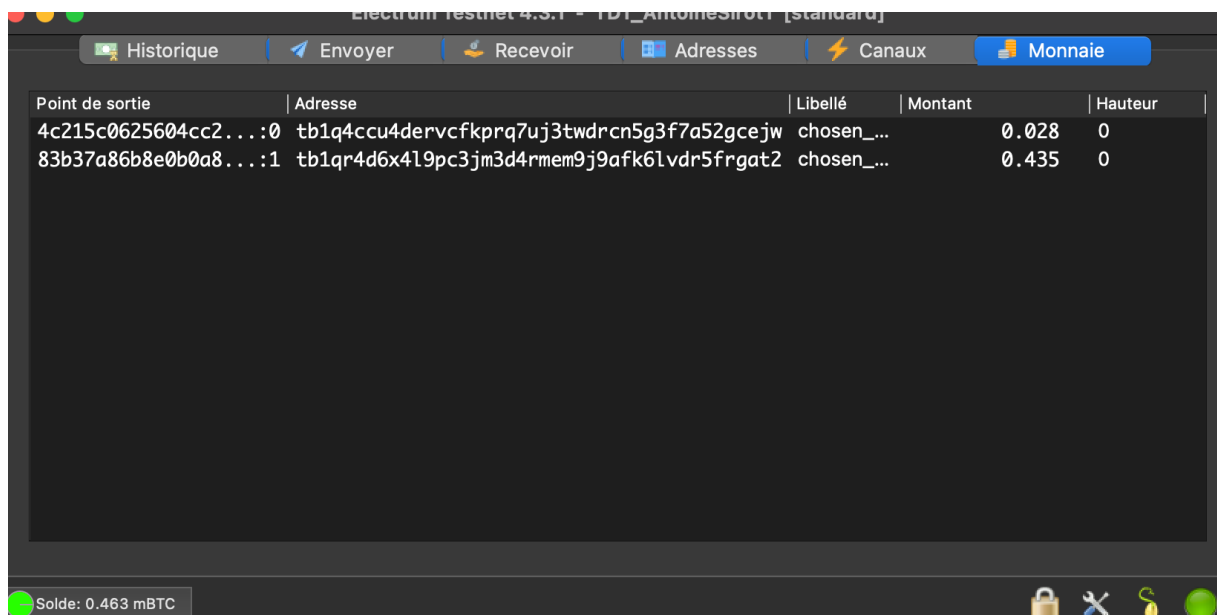
Pour commencer cette troisième partie nous avons envoyé une transaction d'un wallet à un autre.



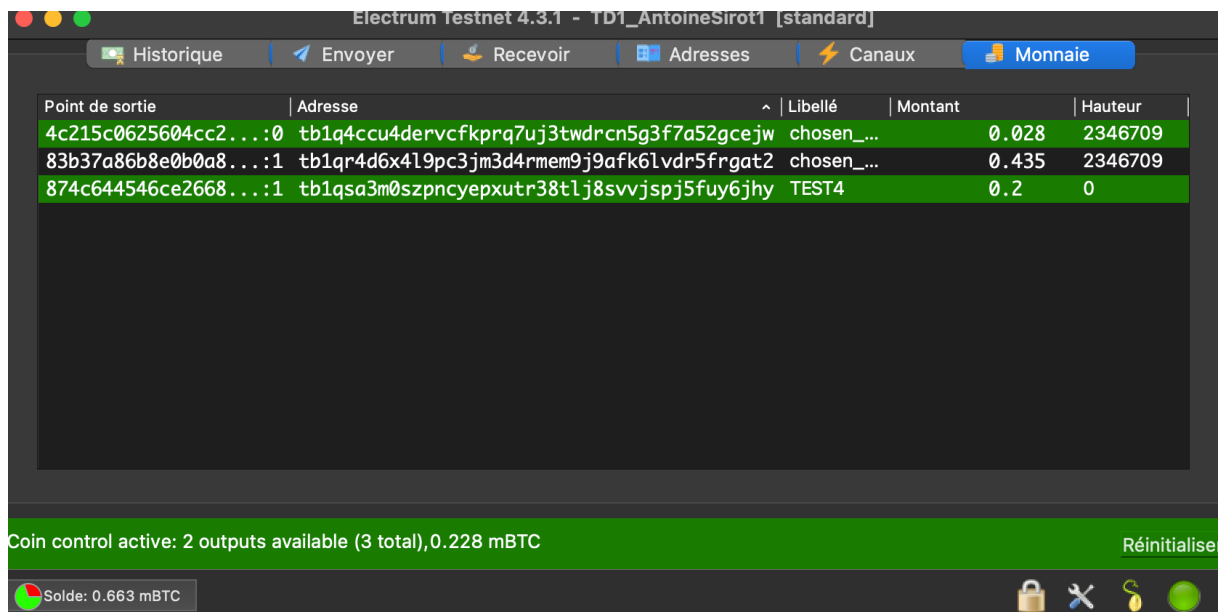
Point de sortie	Adresse	Libellé	Montant	Hauteur
f8e366531a170416...	tb1qa1pyfsr0kws2y4m58zu0tpu71ngra1qgwfqj6	bitcoinfaucet2	0.1	2346703
83b37a86b8e0b0a8...	tb1qg73zmn5m18jqrht08cmha4vkuuqe2ukn2cygur	receive	0.15	0
4c215c0625604cc2...	tb1qg73zmn5m18jqrht08cmha4vkuuqe2ukn2cygur	receive	0.07	0

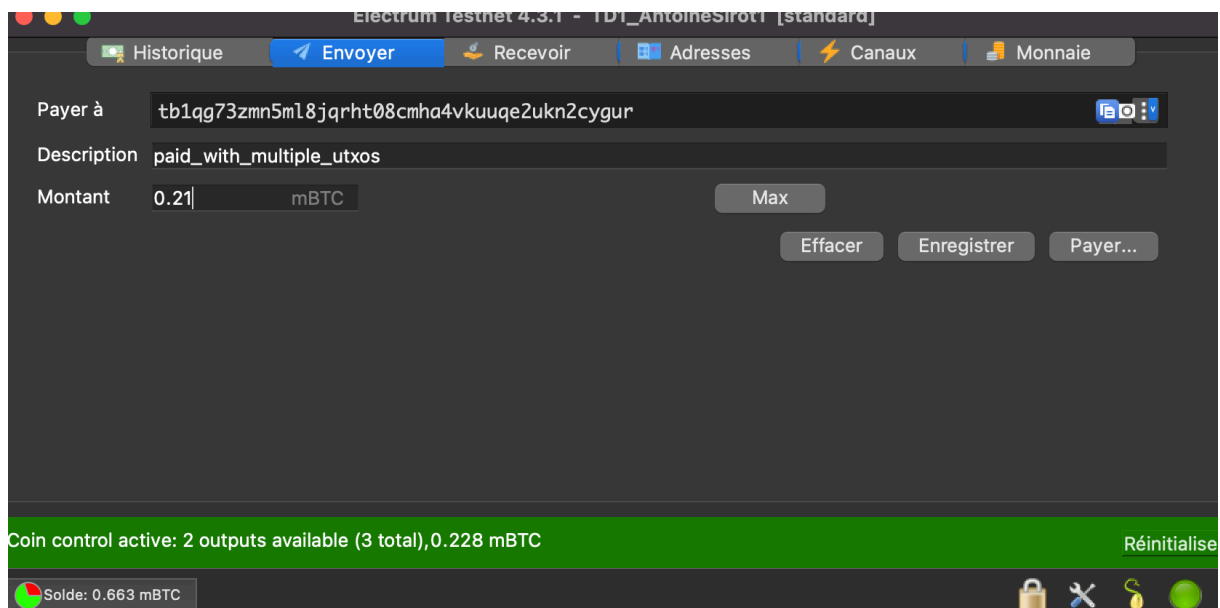
Nous avons ensuite commencé à manipuler les différents UTXO. Tout d'abord nous avons envoyé une transaction d'un UTXO spécifique.



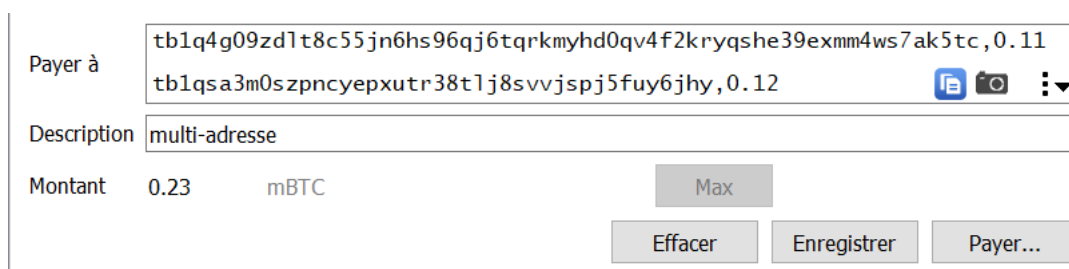


Nous avons ensuite dépensé plusieurs UTXO choisis en une seule transaction.

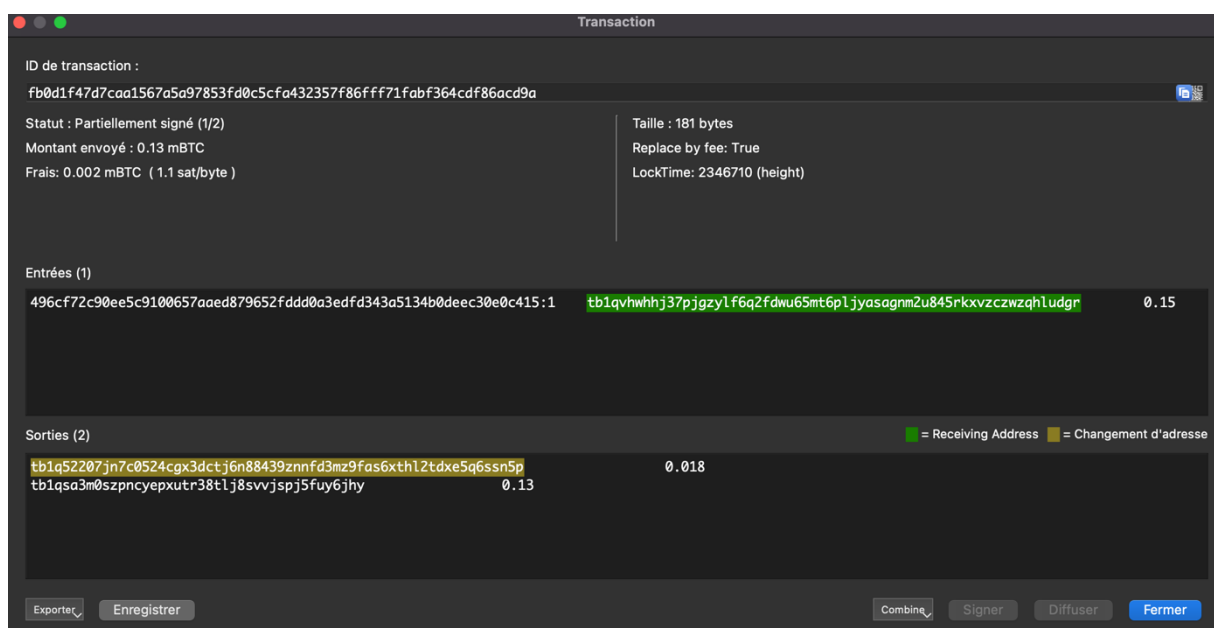




Ensuite nous avons envoyé des fonds à plusieurs adresses en une seule transaction.



Nous avons par la suite envoyé une transaction avec notre wallet multisig avec 2 signatures.



ID de transaction :

fb0d1f47d7caa1567a5a97853fd0c5cfa432357f86fff71fabf364cdf86acd9a



Statut : Signé

Montant envoyé : 0.13 mBTC

Frais: 0.002 mBTC (1.1 sat/byte)

Taille : 180 bytes

Replace by fee: True

LockTime: 2346710 (height)

Entrées (1)

496cf72c90ee5c9100657aa
tb1qvhwhhj37pjgzy1f6q2

Information



Paielement envoyé.

fb0d1f47d7caa1567a5a97853fd0c5cfa432357f86fff71fabf364cdf86acd9a

OK

Sorties (2)

■ = Receiving Address ■ = Changement d'adresse

tb1q52207jn7c0524cgx3dctj6n88439znnfd3mz9fas6xth12tdxe5q6ssn5p 0.018
tb1qsa3m0szpncyepxutr38t1j8svvjspj5fuy6jhy 0.13

Exporter

Enregistrer

Combine

Signer

Diffuser

Fermer