How to Setup a MultiSig Wallet

Nicolas T. Courtois

- **U**niversity **C**ollege **L**ondon, UK

Goals

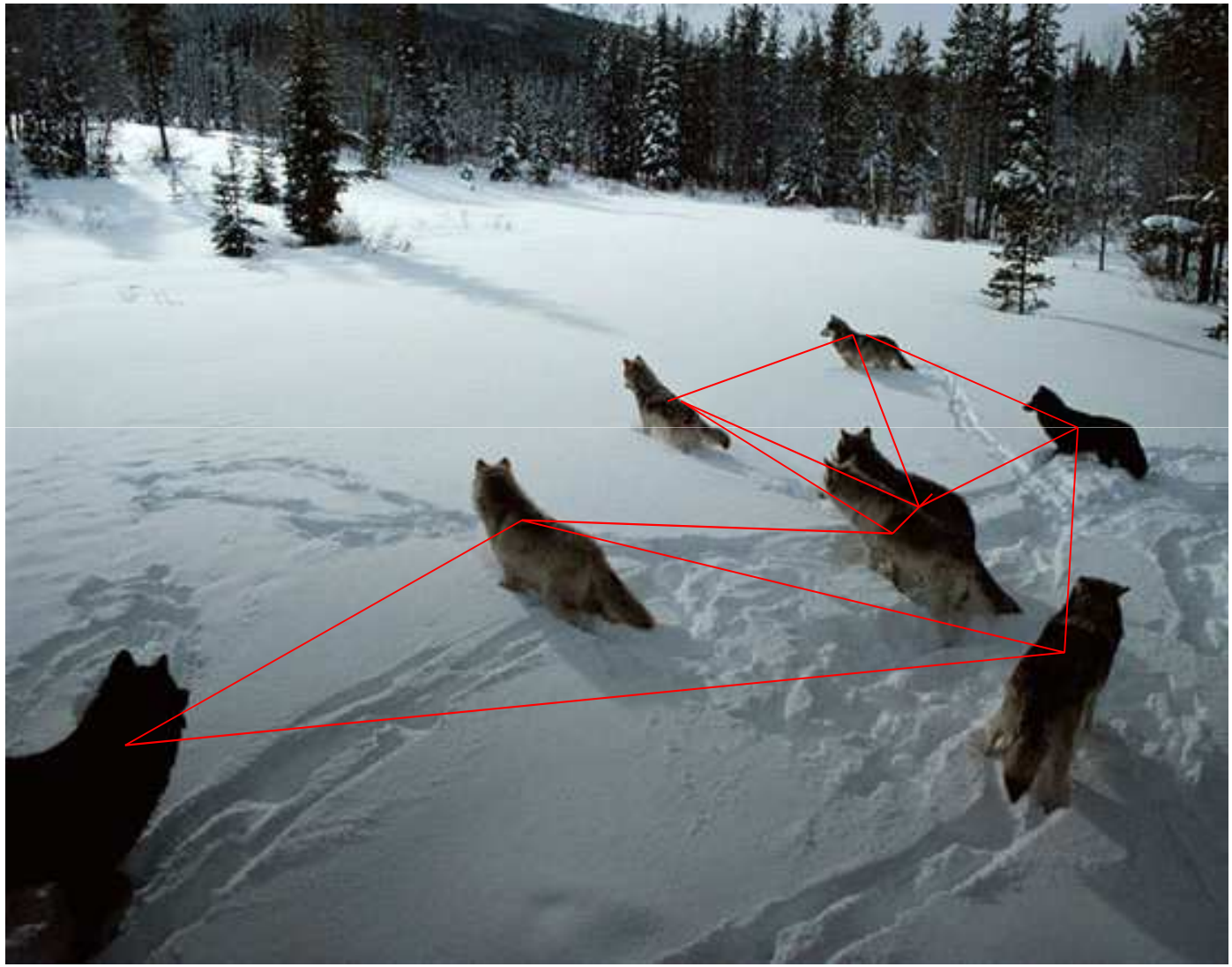
Prevent your bitcoins from being stolen.

Expert advice, yet practical.

We failed to protect our DATA

We failed to protect our MONEY

Solution = Decentralized P2P



Goals

Prevent your bitcoins from being stolen.

How to Manage Keys in Practice?

Not easy, many pitfalls, see our paper:

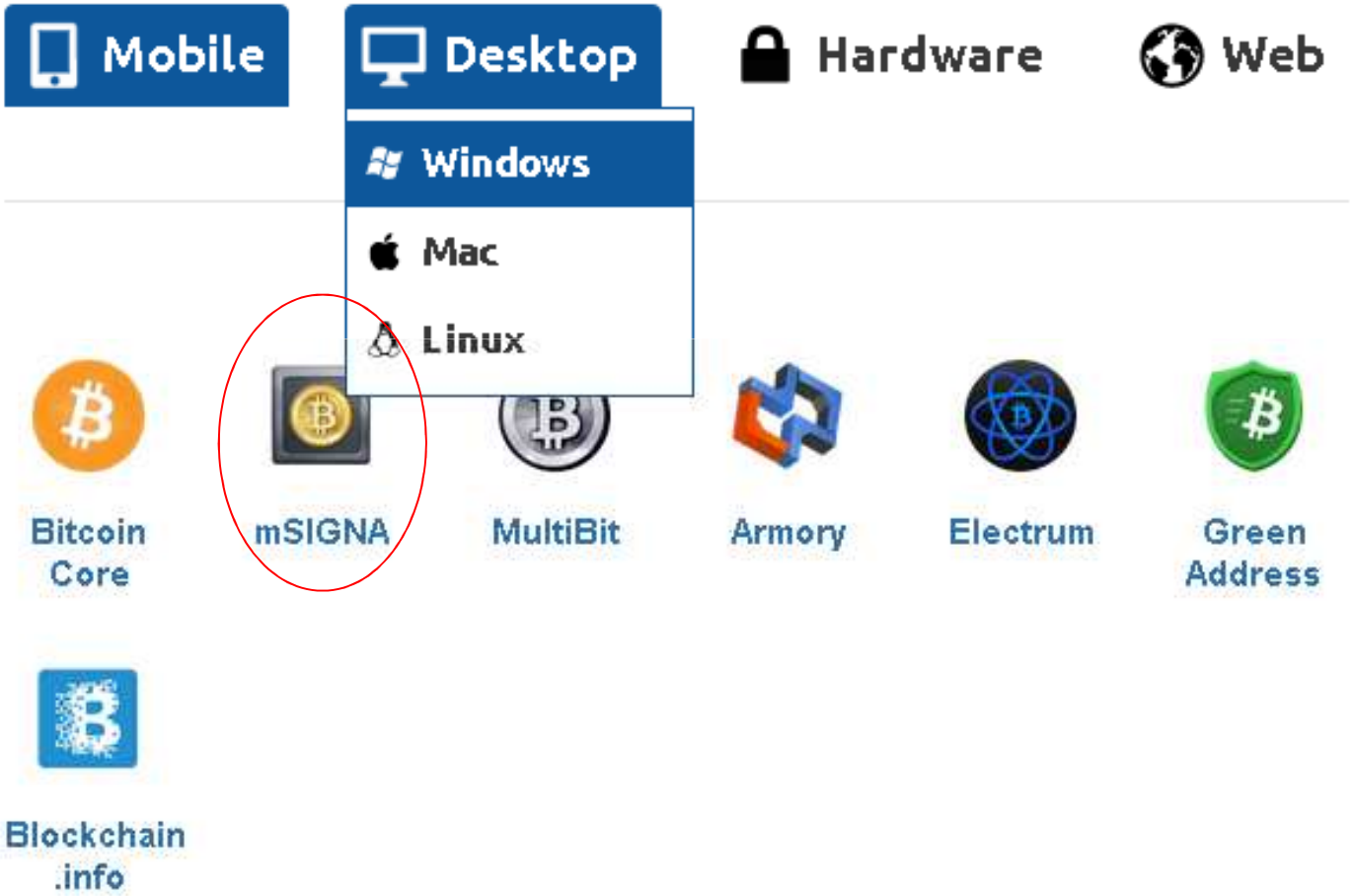
Nicolas T. Courtois, Pinar Emirdag and Filippo Valsorda: Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events, 16 Oct 2014, http://eprint.iacr.org/2014/848

Wallets


11:00
KEYS
BALANCE
TRANSACTIONS
1Lke9VyQHixh
8zxteh7mENSr
4wsX5N6BeN
249.9 mBTC
~USD 184.43
Receiving 25 mBTC
Send
Receive
1 BTC ~ USD 738.00 (Bitstamp)

Wallets - PC

https://bitcoin.org/en/choose-your-wallet



1. Download + Install

Prepare 1 offline computer and 3 online computers, any of Win/Mac/Linux.

Not supported on tablets/phones yet…

Download and install, e.g. for windows:
https://ciphrex.com/downloads/?url=/releases/win64/setup-0.8.7.exe

Install on all your computers!

2. Create Master Backup

On offline computer:

-select “New Vault”

-name it like

“master-backup.vault”

-select where
to save it

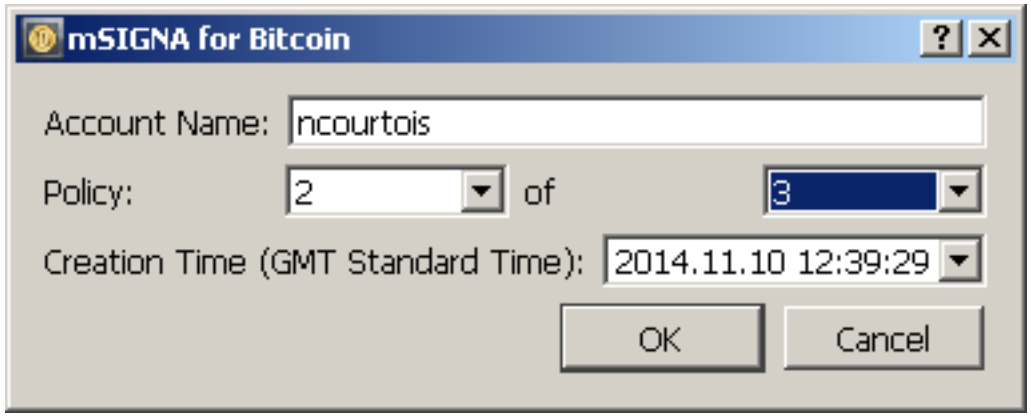
-later it could be erased
and kept only on CD/USB
in a safe as backup…

(NEVER NEEDED unless sth. bad happens)

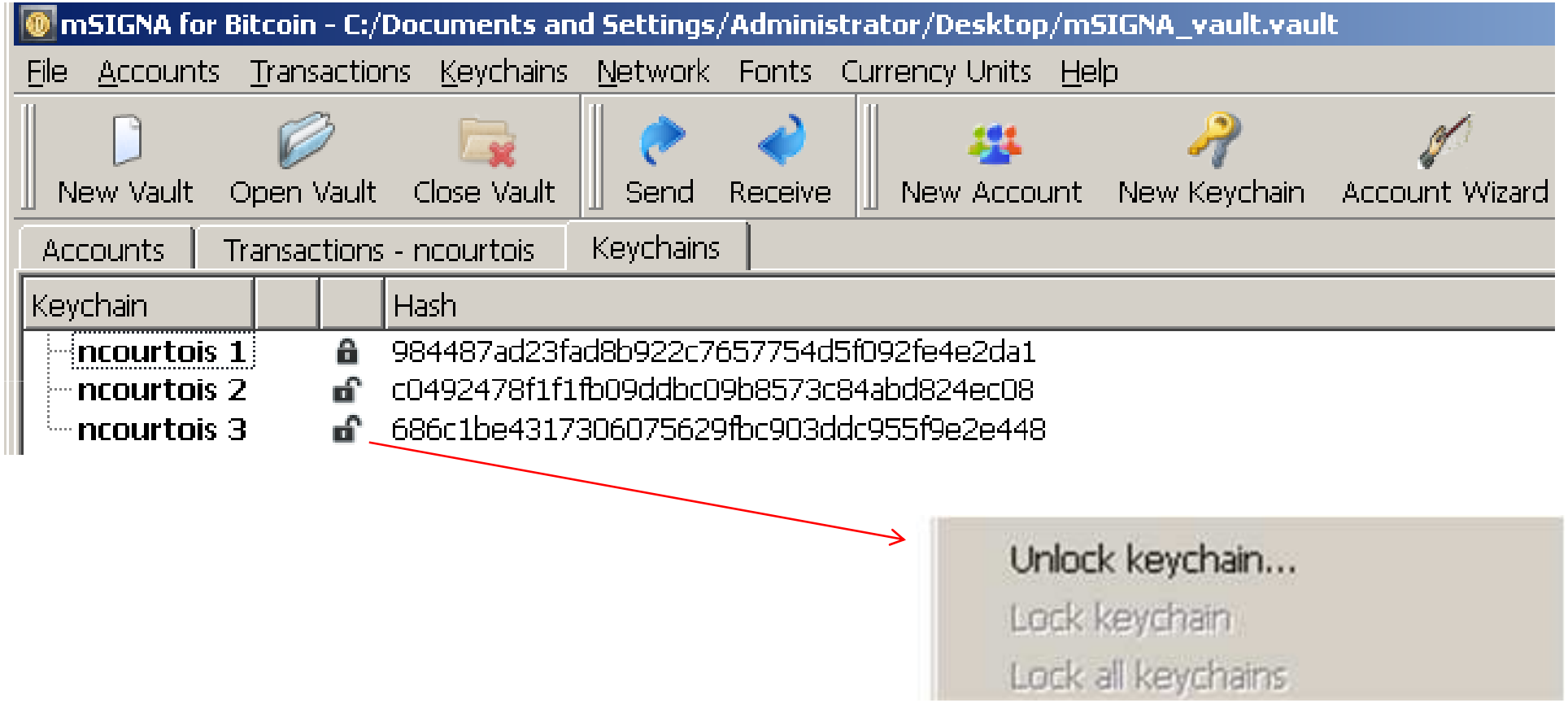
2. Create A Master 2out3 Wallet

Done in 1 click:

Select a name and 2 out of 3



3. It will automatically create this:



- Unlock all the three with right-click.

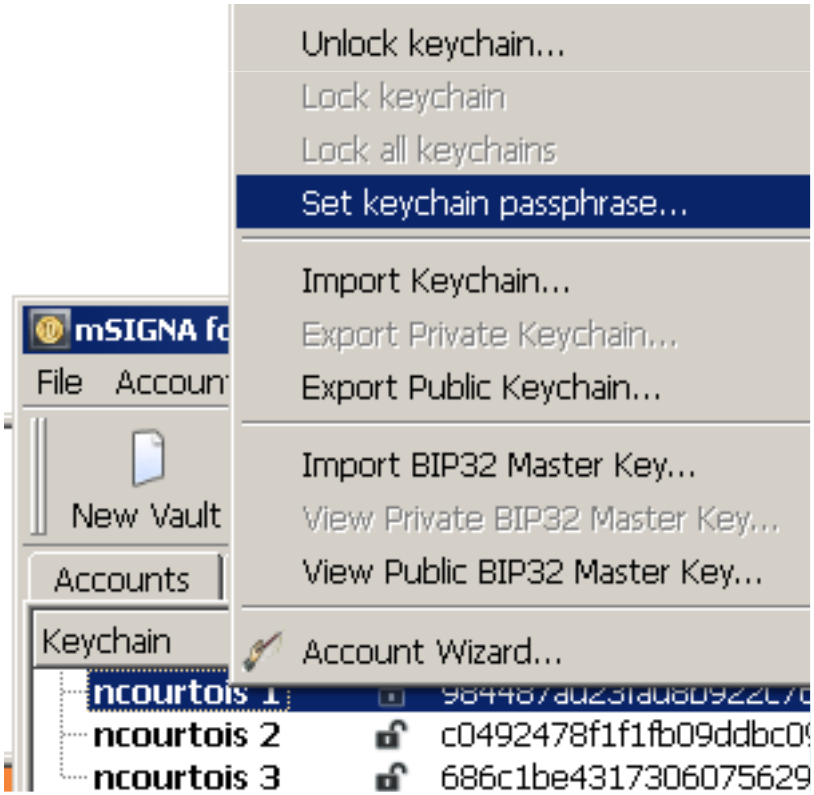
4. Create 3 Passwords

- Select 3 strong passwords

⇒a DIFFERENT one for each keychain!

⇒will be later exported to 3 different devices.

⇒can write them down
on paper and keep
in a safe together
with the current
“master-backup.vault”
file…



5. Export 3 Private Masters

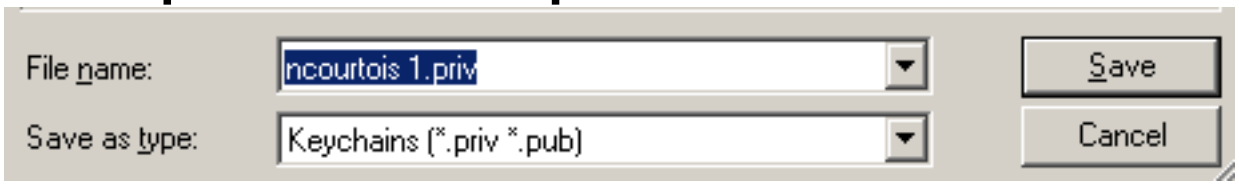
- Right Click,

"Export Private…

5. Export 3 Private Masters

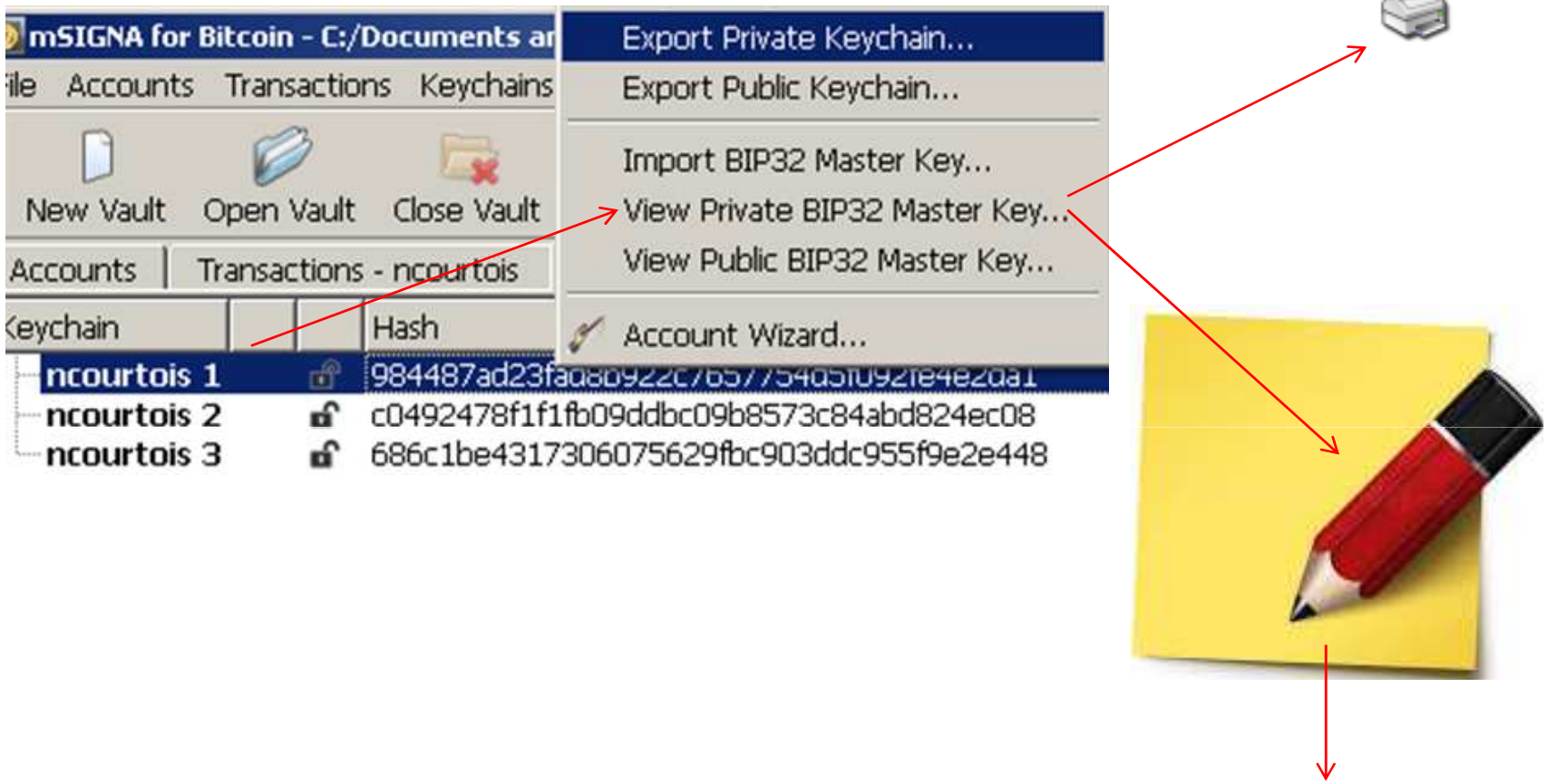
- Right Click, "Export Private…

- Save as 3 Files, password protected,



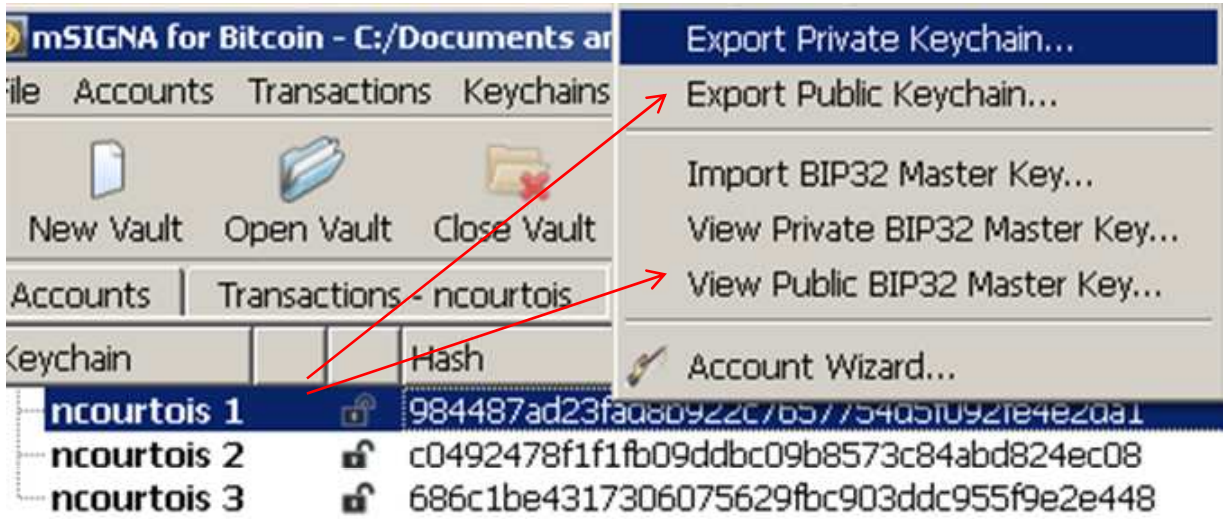
- Move to 3 online PCs – NOT now, later…

*5b. Plain-Text Option



- Enter it in plaintext format to 3 online PCs

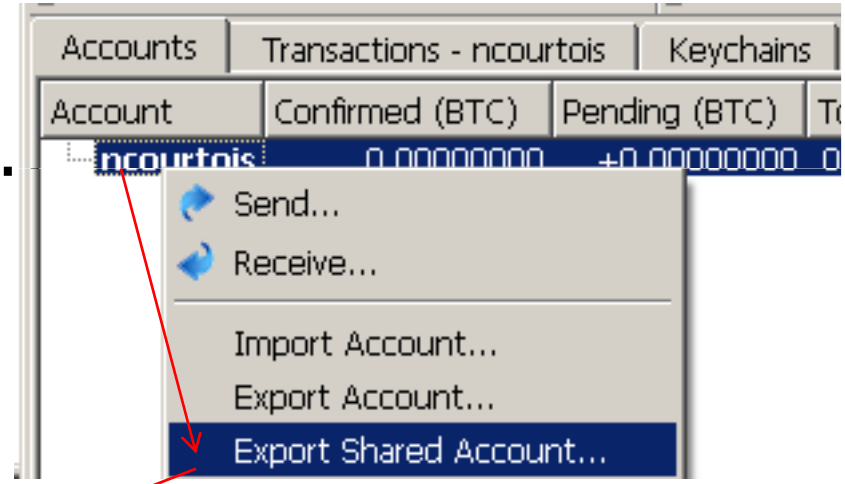
****5c. Read-Only Options



- Not really needed in our setup.
- in theory these 3 exports allow to see the money and accept payments, BUT not to spent any of it.
- however here we do not need these exports. we use another method.

6. Export Shared Account

- Contains all the public masters to generate public keys to accept many payments on distinct sub-accounts
- Right Click, “Export Shared Account…
- Saved as "ncourtois.sharedacct"



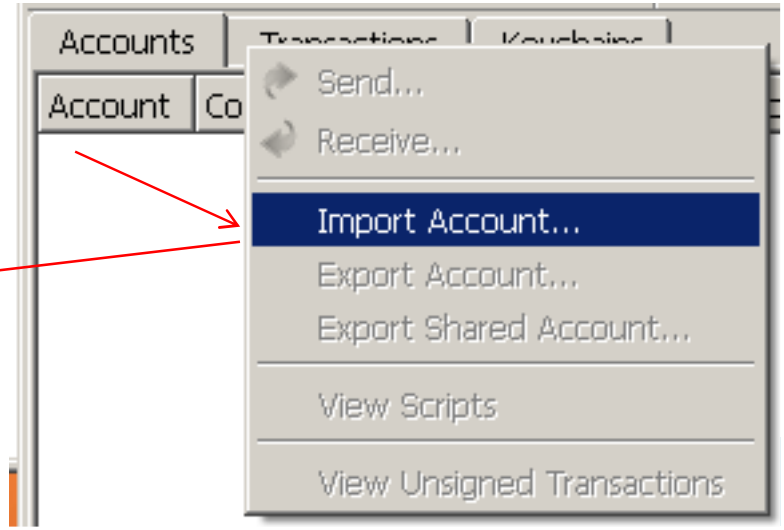
- Export to all 3 hot PCs

6. Import Shared Account 3x

On each computer: Create empty “ncourtois_PC2.vault”

1. Import just 1 private key!

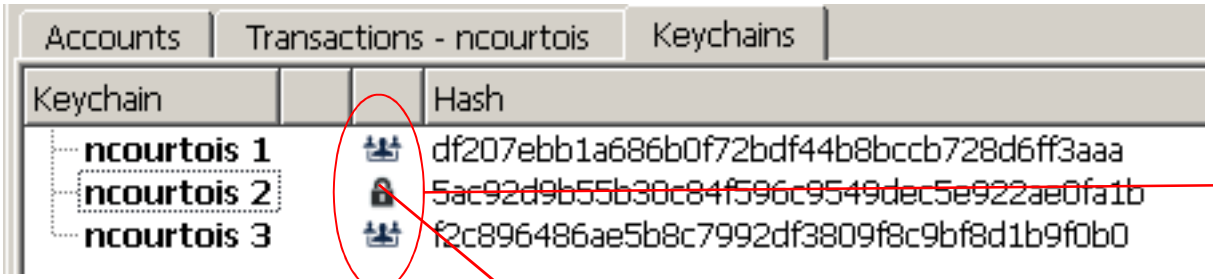
2. Import the shared account file



6. If Done Correctly: Should Look Like This:

Accounts tab:

Keychains tab: **PC number2**



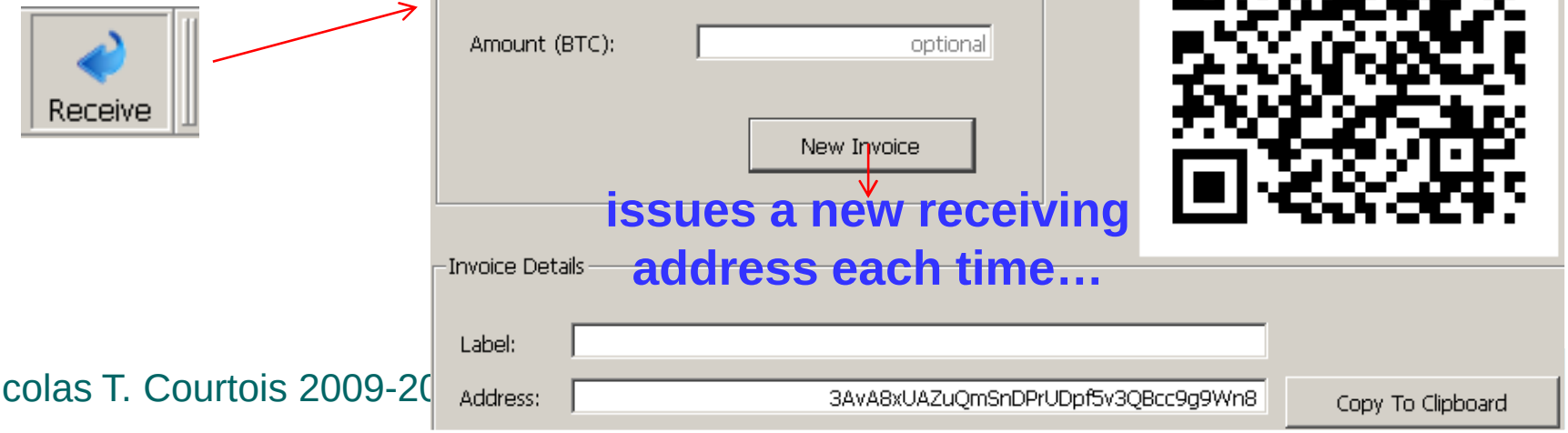
only 1 private master on this computer

don't forget to unlock to spend BTC

2 machines needed to spend any coins

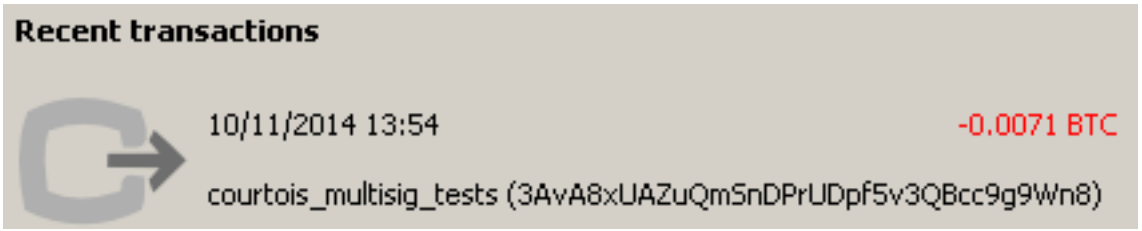
7. Claim Payments

- Each payment can have a different multisig key!
  - Good for anonymity
  - Protects against NSA breaking the bitcoin Ellptic Curve.
- On PC2:



8. Sb. Pays

- Another person sends money to this multisig address:



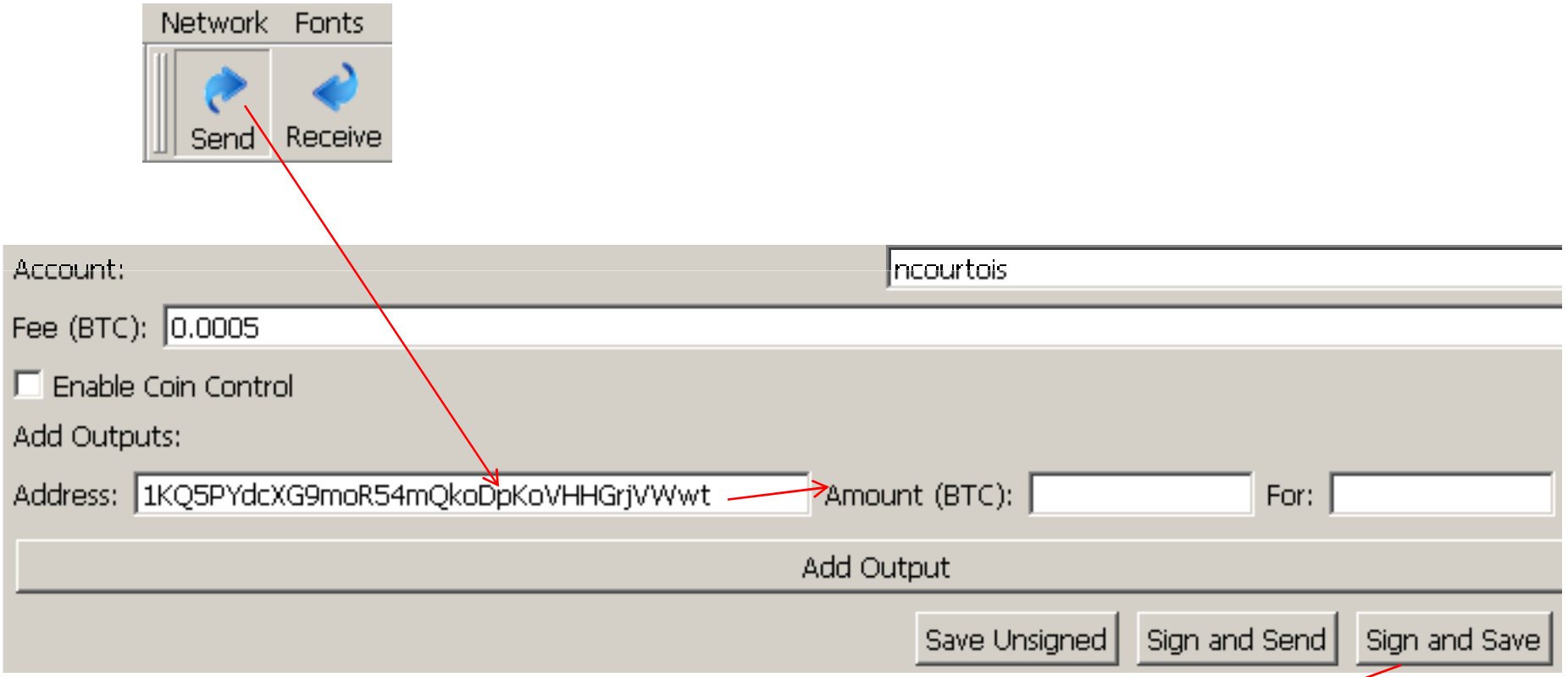
- Will appear when mSIGNA when synchronized…

8b. Manual Import

- If impatient, export rawtx on Satoshi client console:
- **getrawtransaction f3ead1113cfab073a3242471b6f3b45ac42773b7f7df208f0a05b49a5ad51cc5**
- Save as *.rawtx
- import into mSIGNA
- works!

9a. Creating Multisig Payment

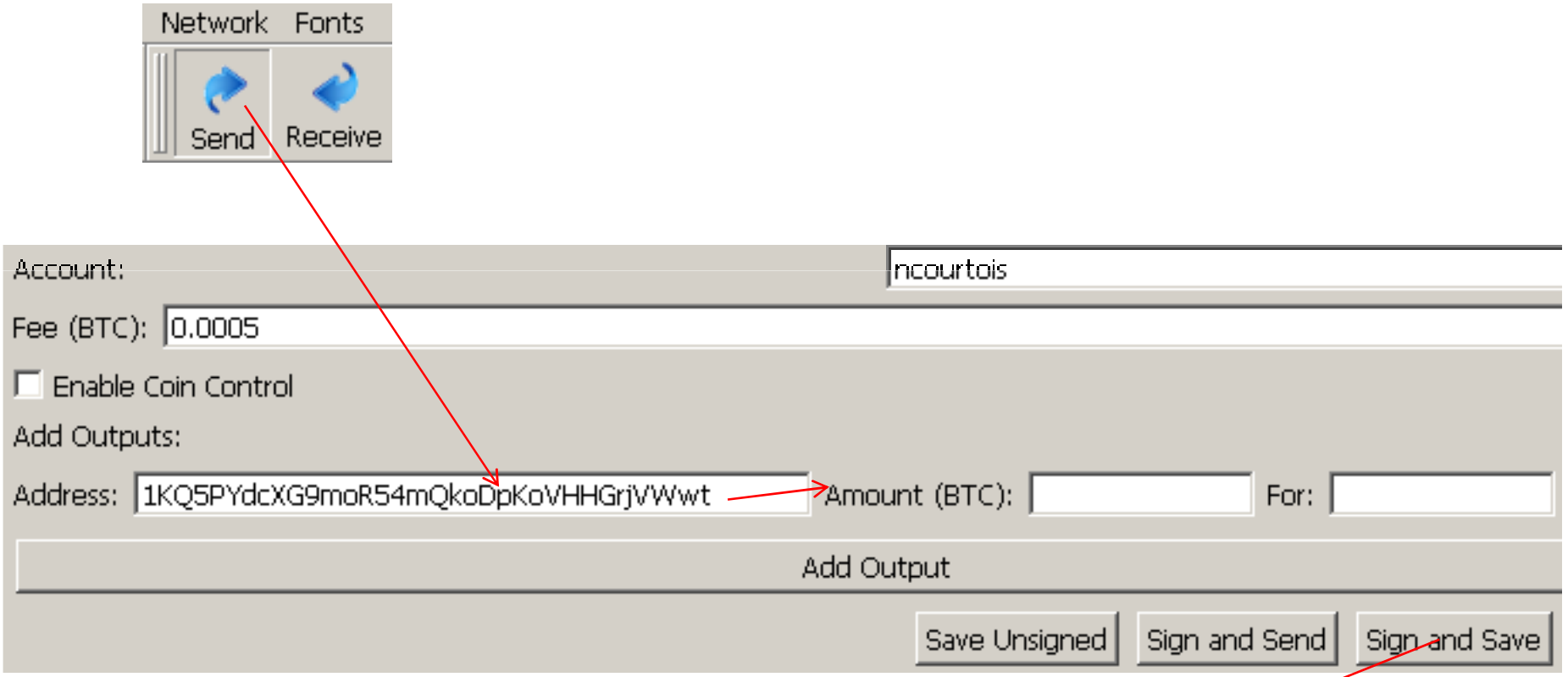
- Requires 2 PCs, One PC, One Signature



only saves locally, 1 signature

9b. Creating Multisig Payment

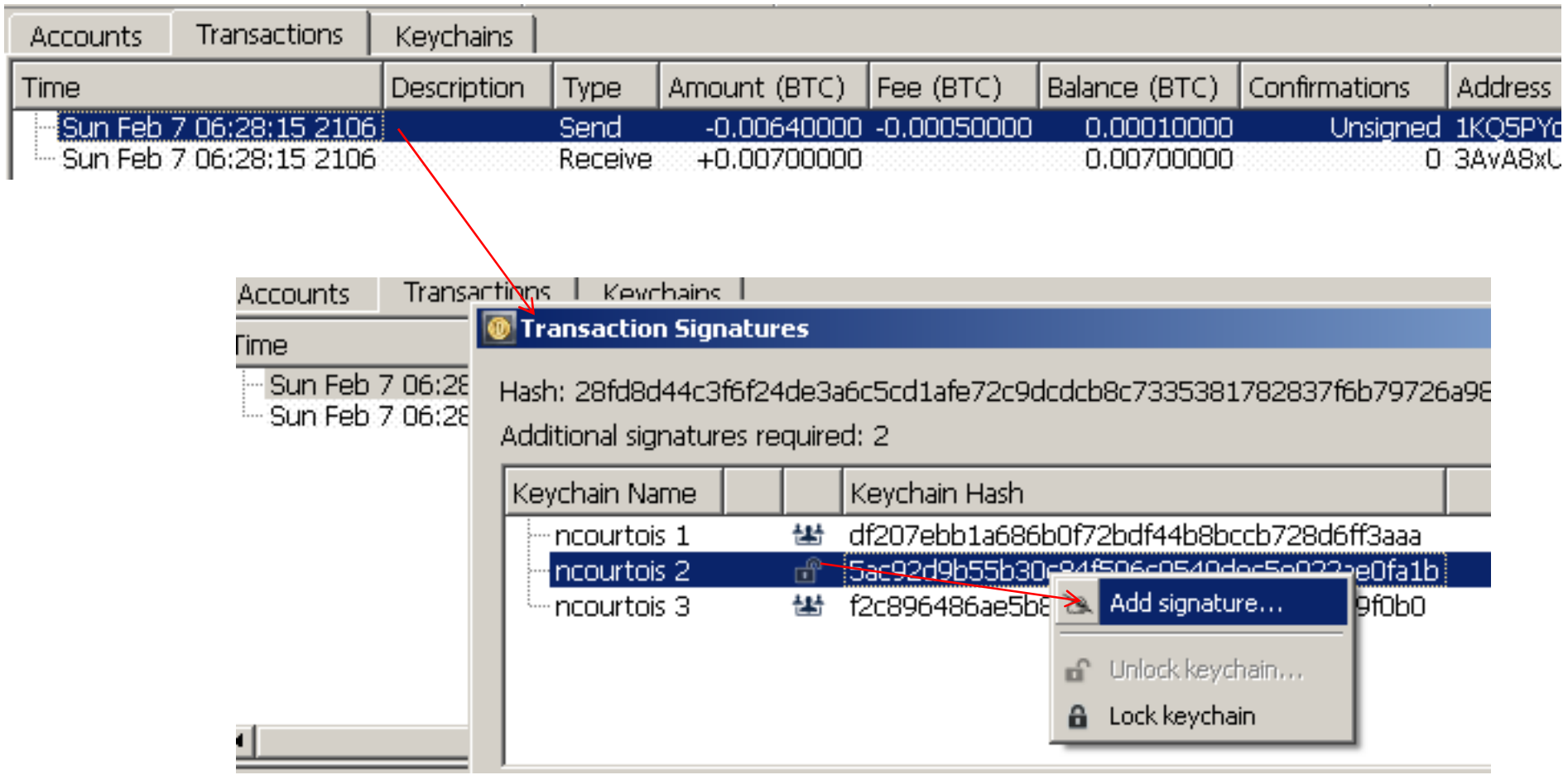
- Requires 2 PCs, One PC, One Signature



<u>WARNING:</u> WILL NOT SIGN if Private Key is locked

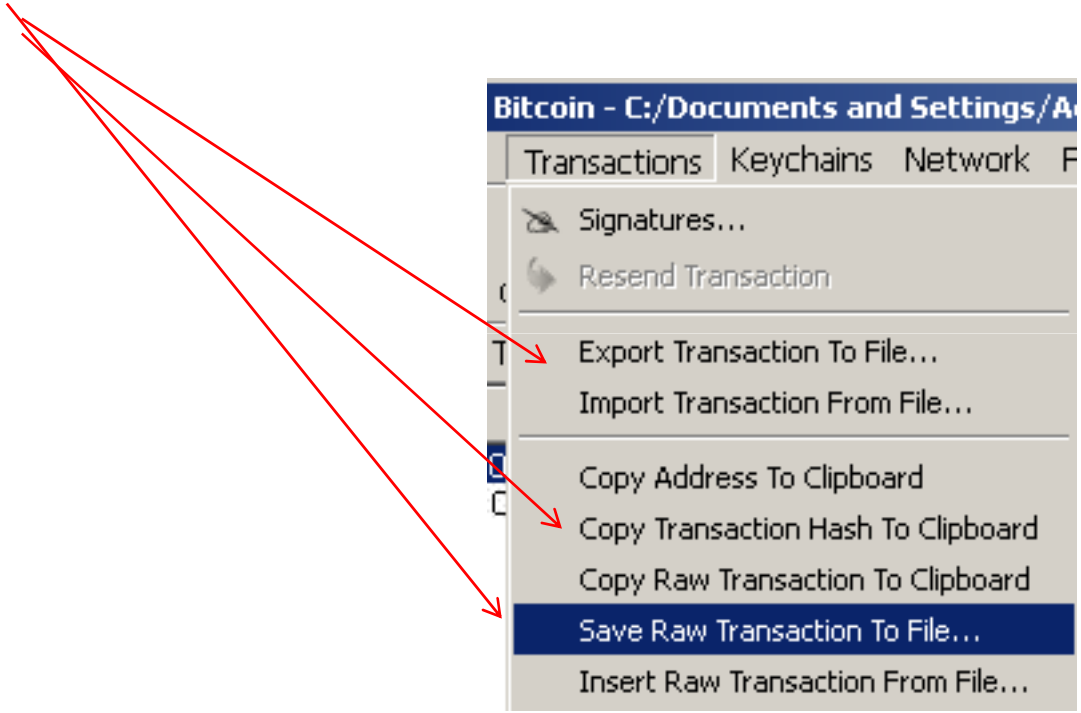
9c. Double Check

- 1st PC



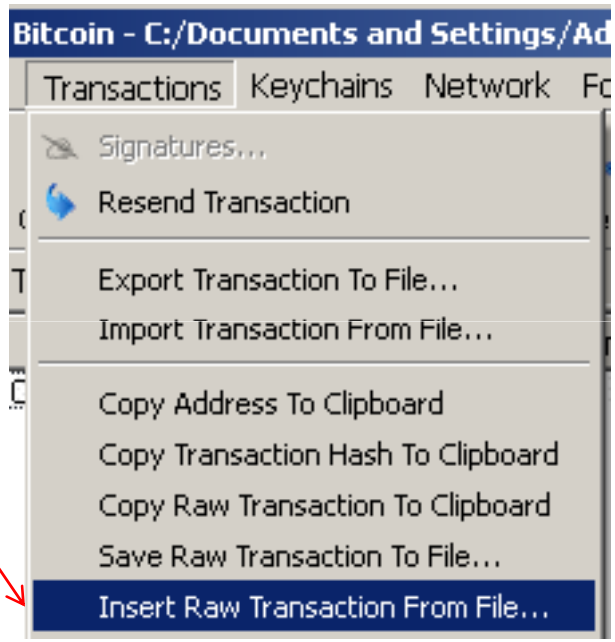
9d. Export Tx with 1 Sig

- export to another PC



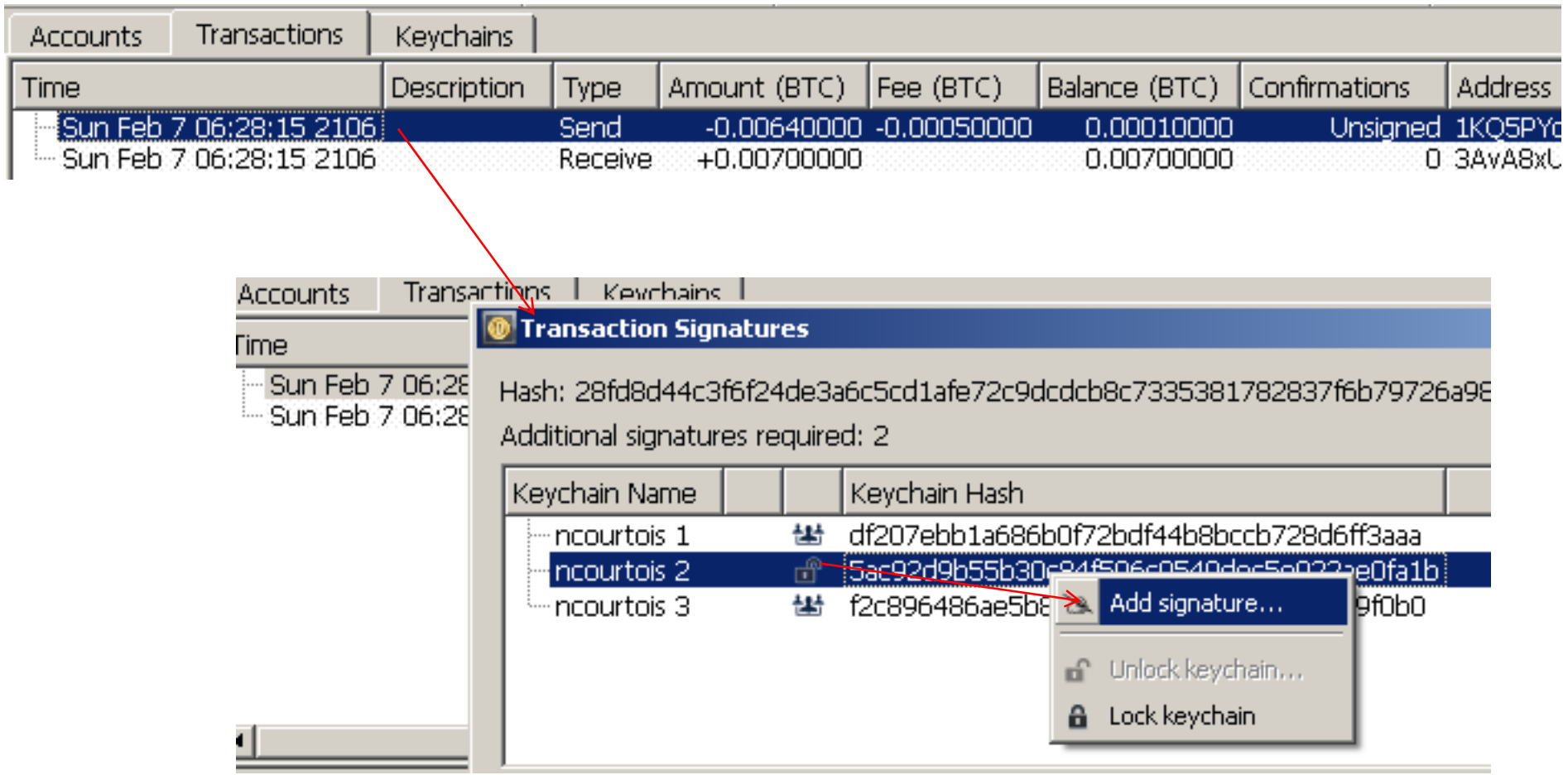
9e. Import Raw Tx

- 2nd PC



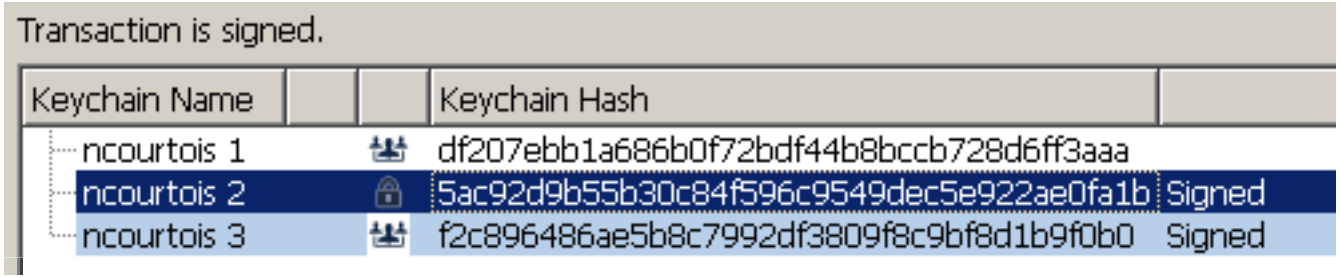
9f. Check 1 Signature, Add Another

- 2nd PC



9g. Once A Transaction Has 2 Signatures

- Verify here:



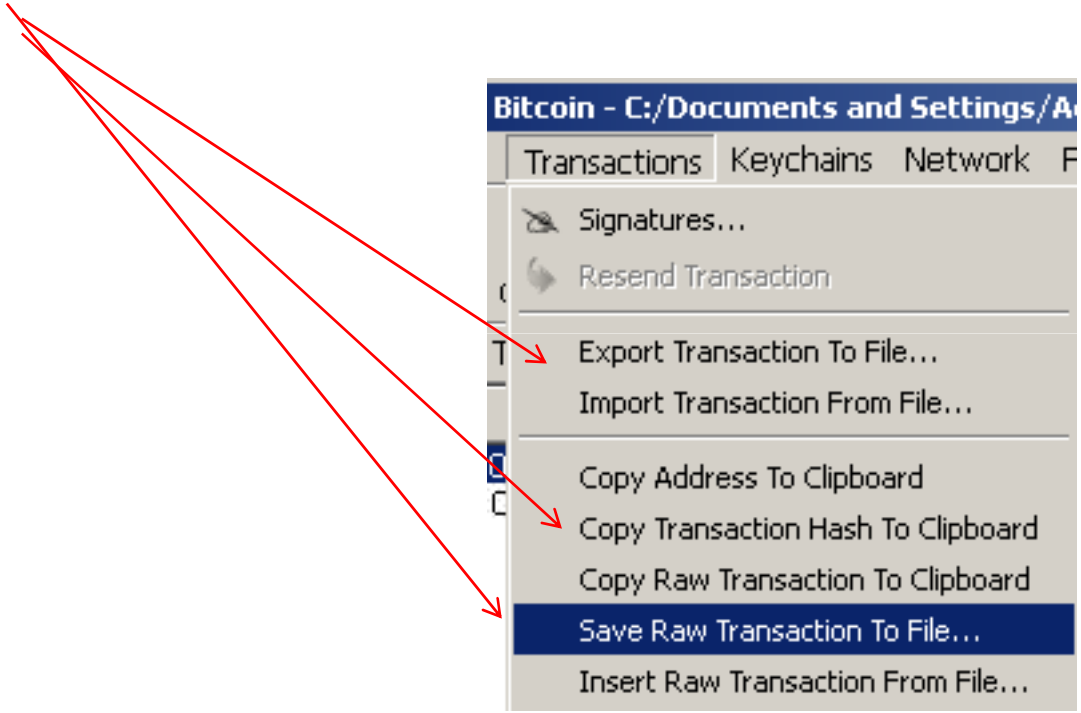
9h. Once A Transaction Has 2 Signatures

- Now you can either
- DELETE
- or SEND this transaction to the bitcoin network (automatic or manual)

Money will be spent now!

**9i. Use Satoshi Client to Diffuse It

- OPTIONAL: export to a file



****9j. Use Satoshi Console

- OPTIONAL: Open the saved .rawtx file
- In Satoshi console type:
- sendrawtransaction

0100000001c51cd55a9ab4050a8f20dff7b77327c45ab4f3b6712424a373b0fa3c11d1eaf301000000fdfe0000483045022003093912 3d5399f01487464f756a8214fcad8a2d7f59aba40bcbe6ad1e4a0a61022100a48b72dec7892fcb0f3e9751ad64e01b5cb987ec00547655b386f27dc15c3b74014830450220367ac6c52e264e9b9f09db32b0d17370c694a64f8a91861f724d4d30975ec622022100b59f376bb8efda0c1a473eaec5f440eb1b8067cd736dd563ea7a01b24f137af3014c69522102a53ba7c3660d9bf04bc6ff4424993410e8b268d7ae364b44389e1569f88fceeb210328afa52561eb08c82c8d4a95bbc5609e539e3ca15fbaffa7a2bd61e240b71f402103aa0f14c3aea36bcca32ceb0177c8fe262014c7cfc7f6b4850ae783d3bf017fa353aeffffffff0200c4090000000001976a914c9cf7ea770e7ae147ad17ee3eec57b7be50e433588ac102700000000000017a914924a26c5067f1ab693c2fcd9399a1087c0562dca8700000000

- it has worked instantly!