

How to Setup a MultiSig Wallet



Nicolas T. Courtois

Goals

Prevent your bitcoins from being stolen.

Expert advice, yet practical.

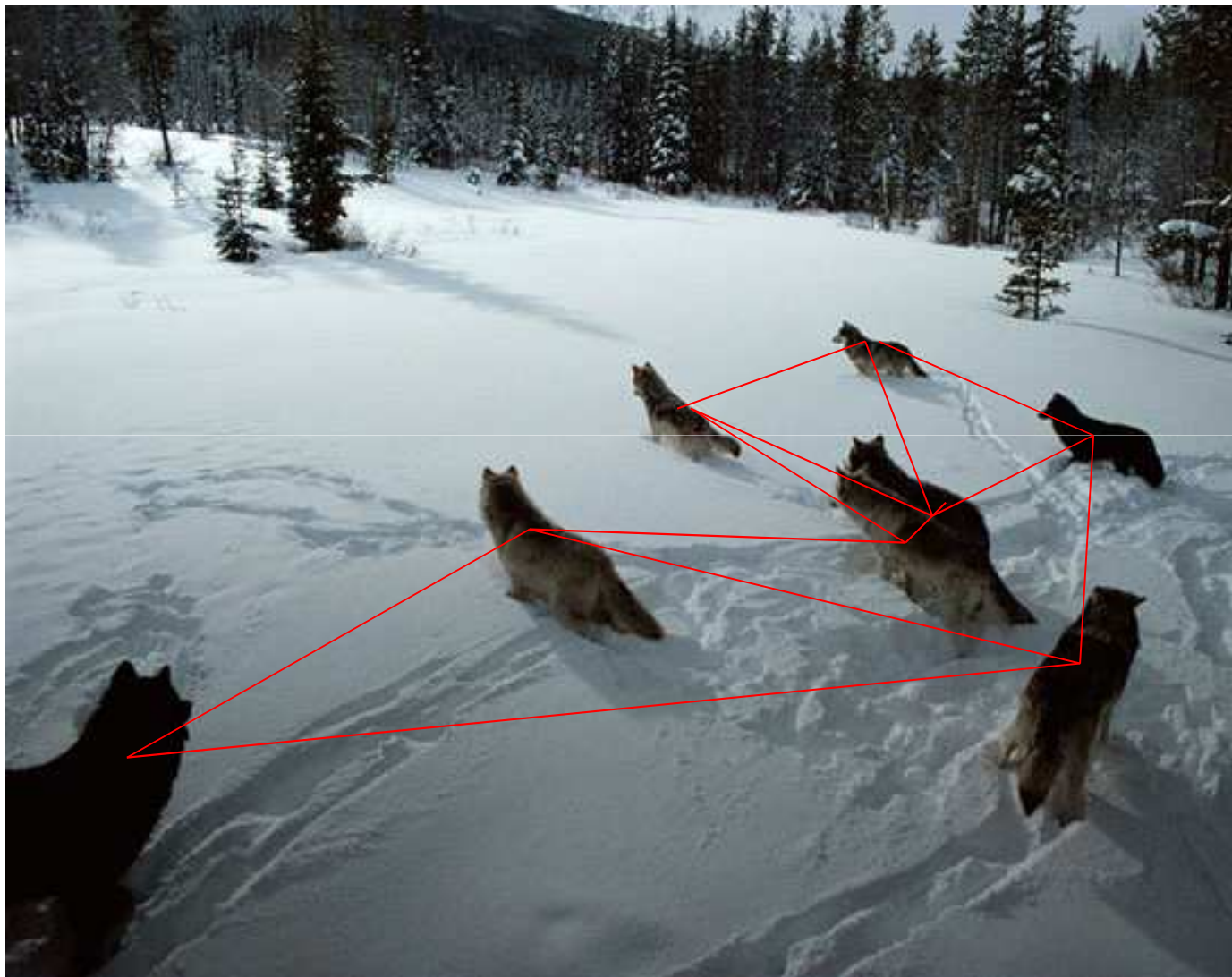
We failed to protect our DATA



We failed to protect our **MONEY**



Solution = Decentralized P2P



Goals

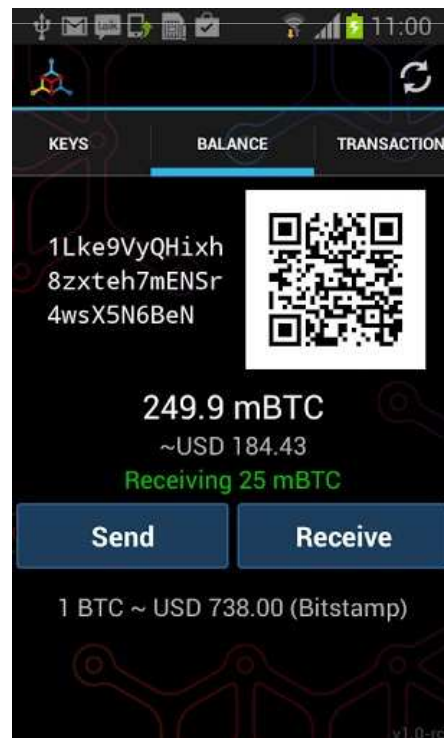
Prevent your bitcoins from being stolen.

How to Manage Keys in Practice?

Not easy, many pitfalls, see our paper:

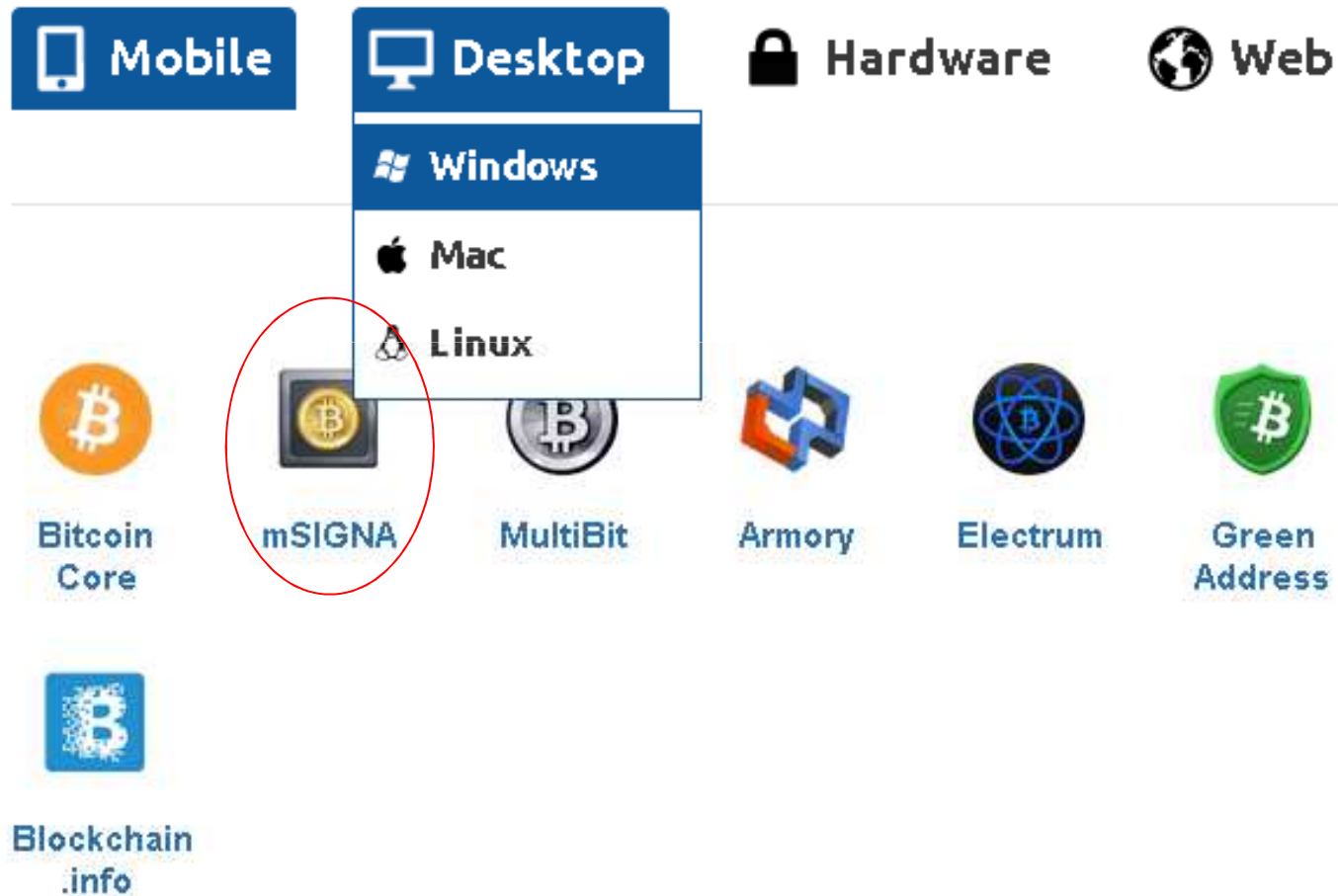
Nicolas T. Courtois, Pinar Emirdag and Filippo Valsorda: [Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events](http://eprint.iacr.org/2014/848), 16 Oct 2014, <http://eprint.iacr.org/2014/848>

Wallets



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)

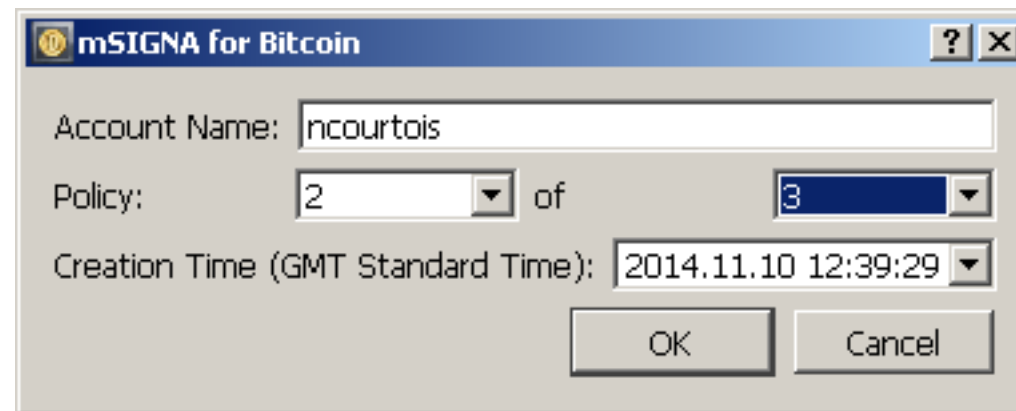


2. Create A Master 2out3 Wallet

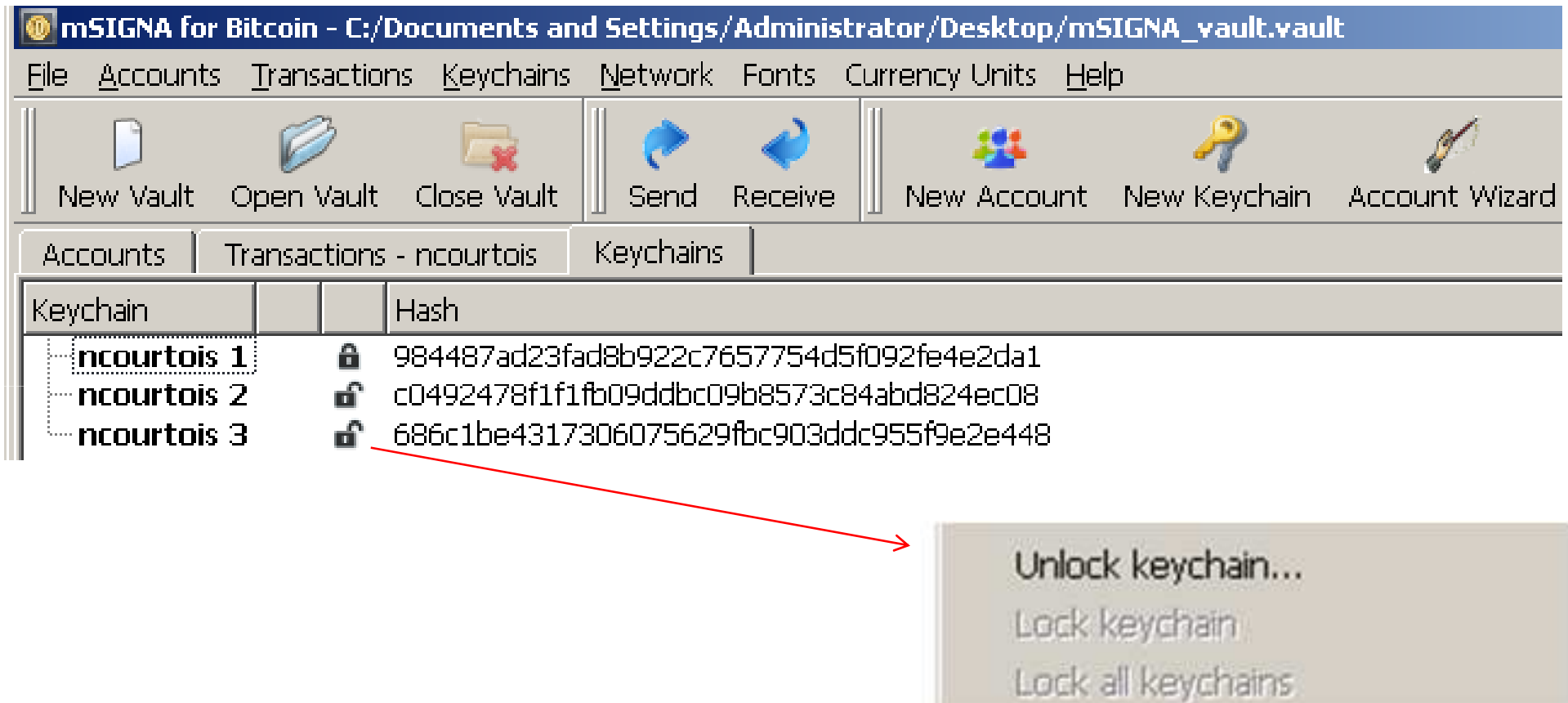
Done in 1 click:



Select a name and 2 out of 3



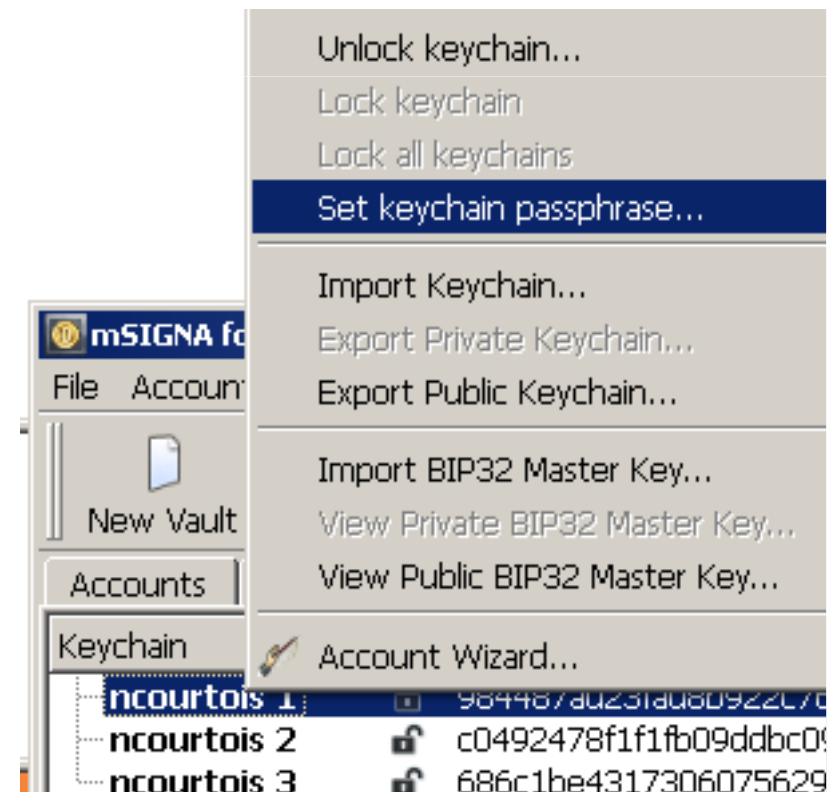
3. It will automatically create this:



- 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...”

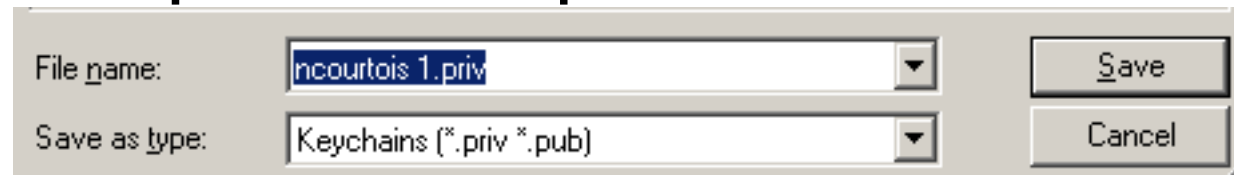


5. Export 3 Private Masters

- Right Click,
“Export Private...”



- Save as 3 Files, password protected,



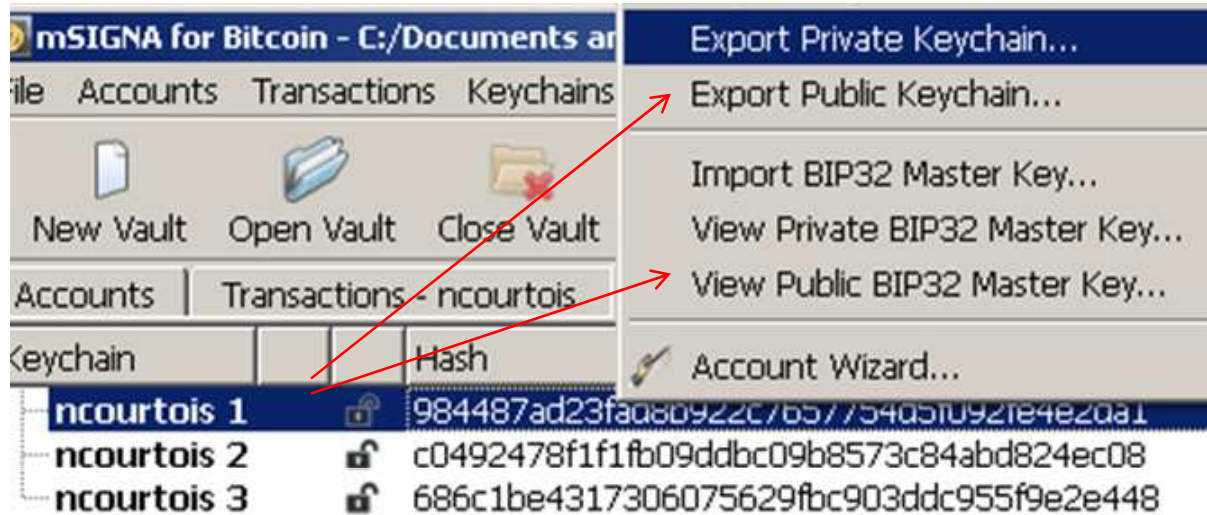
- Move to 3 online PCs – NOT now, later...

*5b. Plain-Text Option



- Enter it in plaintext format to 3 online PCs

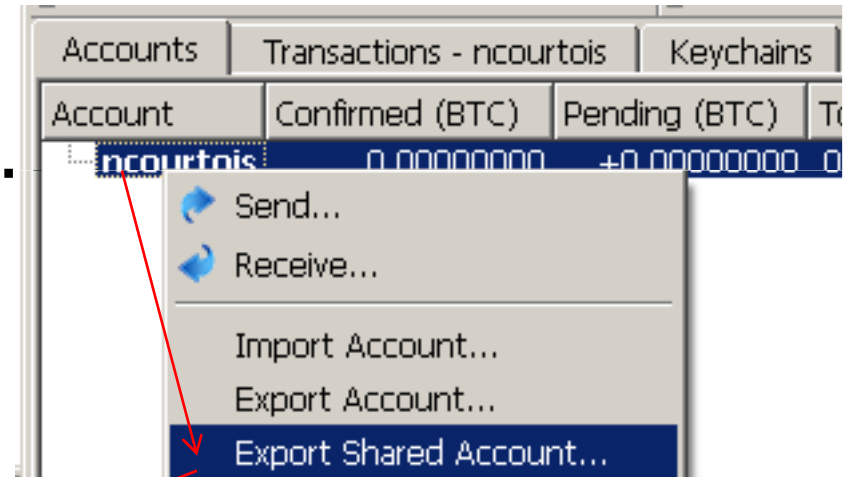
****5c. Read-Only Options



- 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



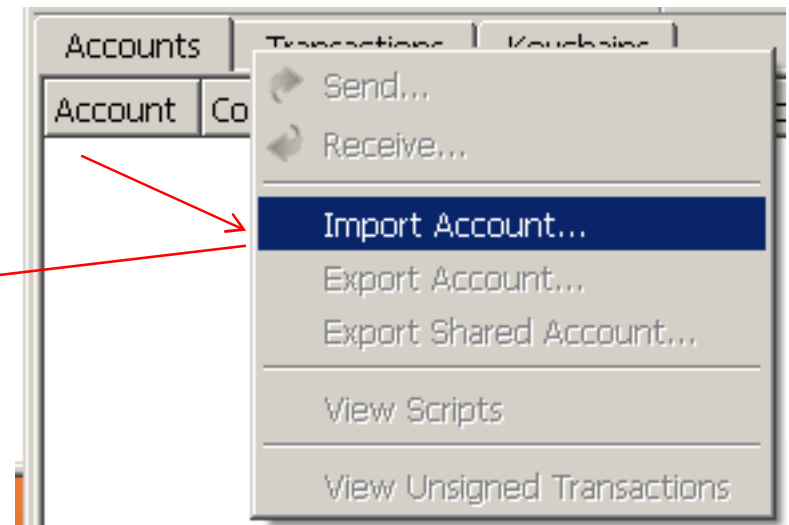
6. Import Shared Account 3x

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:

Account	Confirmed (BTC)	Pending (BTC)	Total (BTC)	Policy
ncourtois	0.00000000	+0.00000000	0.00000000	2 of ncourtois 1, ncourtois 2, ncourtois 3

Keychains tab: **PC number2**

Keychain	Hash
ncourtois 1	df207ebb1a686b0f72bdf44b8bccb728d6ff3aaa
ncourtois 2	5ac92d9b55b30c84f596c9549dec5e922ae0fa1b
ncourtois 3	f2c896486ae5b8c7992df3809f8c9bf8d1b9f0b0

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

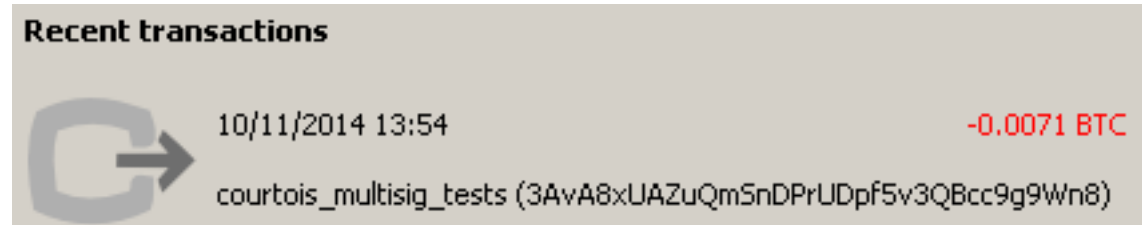
- Each payment can have a different multisig key!
 - Good for anonymity
 - Protects against NSA breaking the bitcoin Elliptic Curve.
- On PC2:



The screenshot shows a 'Request Payment' interface. It includes a 'Request Payment' section with a dropdown menu for 'Account' (set to 'ncourtois'), input fields for 'Invoice Label' and 'Amount (BTC)' (both marked as 'optional'), and a 'New Invoice' button. A red arrow points from the 'Receive' icon to the 'New Invoice' button. Below this, a blue text annotation reads 'issues a new receiving address each time...'. To the right is a large QR code. Below the QR code is an 'Invoice Details' section with a 'Label' field and an 'Address' field containing the value '3AvA8xUAZuQmSnDPrUDpf5v3QBcc9g9Wn8'. A 'Copy To Clipboard' button is located at the bottom right.

8. Sb. Pays

- Another person sends money to this multisig address:



- Will appear when mSIGNA when synchronized...

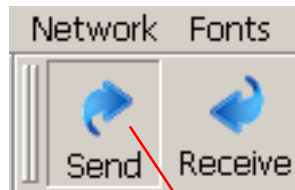
8b. Manual Import

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

Accounts		Transactions		Keychains					
Time	Description	Type	Amount (BTC)	Fee (BTC)	Balance (BTC)	Confirmations	Address	Tr	
Sun Feb 7 06:28:15 2106		Receive	+0.00700000		0.00700000	0	3AvA8xUAZuQmSnDPrUDpf5v3QBcc9g9Wn8 f3e		

9a. Creating Multisig Payment

- Requires 2 PCs, One PC, One Signature



Account:

Fee (BTC):

Enable Coin Control

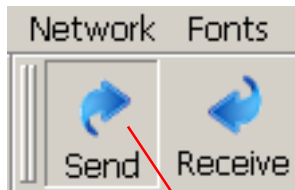
Add Outputs:

Address: Amount (BTC): For:

only saves locally, 1 signature

9b. Creating Multisig Payment

- Requires 2 PCs, One PC, One Signature



Account:

Fee (BTC):

Enable Coin Control

Add Outputs:

Address: Amount (BTC): For:

WARNING: WILL NOT SIGN if Private Key is locked

9c. Double Check

- 1st PC

Accounts		Transactions		Keychains			
Time	Description	Type	Amount (BTC)	Fee (BTC)	Balance (BTC)	Confirmations	Address
Sun Feb 7 06:28:15 2106		Send	-0.00640000	-0.00050000	0.00010000	Unsigned	1KQ5PYc
Sun Feb 7 06:28:15 2106		Receive	+0.00700000		0.00700000		0 3AvA8xL

Transaction Signatures

Hash: 28fd8d44c3f6f24de3a6c5cd1afe72c9dcdcb8c7335381782837f6b79726a9e

Additional signatures required: 2

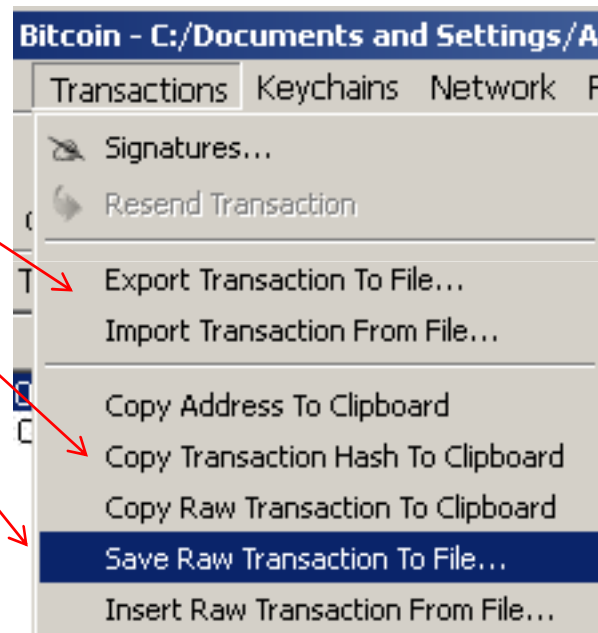
Keychain Name	Keychain Hash
ncourtois 1	df207ebb1a686b0f72bdf44b8bccb728d6ff3aaa
ncourtois 2	5ac92d9b55b30c94f506c0540d6c5a022e0fa1b
ncourtois 3	f2c896486ae5b8e9f0b0

Context menu options:

- Add signature...
- Unlock keychain...
- Lock keychain

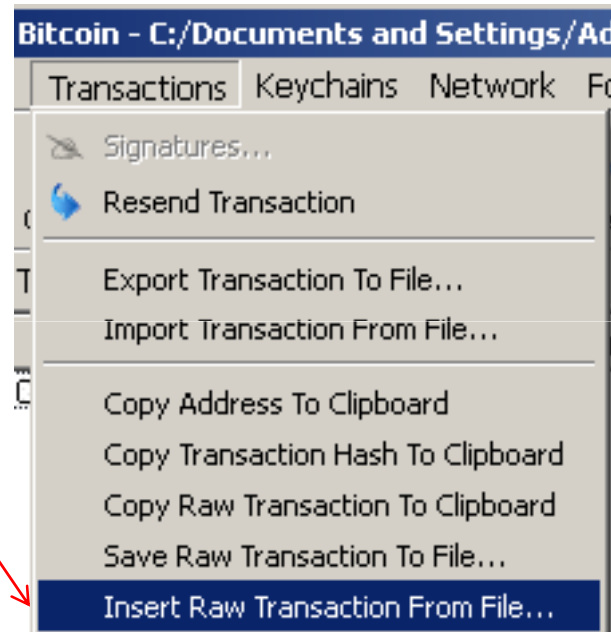
9d. Export Tx with 1 Sig

- export to another PC



9e. Import Raw Tx

- 2nd PC



9f. Check 1 Signature, Add Another

- 2nd PC

Time	Description	Type	Amount (BTC)	Fee (BTC)	Balance (BTC)	Confirmations	Address
Sun Feb 7 06:28:15 2106		Send	-0.00640000	-0.00050000	0.00010000	Unsigned	1KQ5PYc...
Sun Feb 7 06:28:15 2106		Receive	+0.00700000		0.00700000		0 3AvA8xL...

Transaction Signatures

Hash: 28fd8d44c3f6f24de3a6c5cd1afe72c9dcdcb8c7335381782837f6b79726a9E

Additional signatures required: 2

Keychain Name	Keychain Hash
ncourtois 1	df207ebb1a686b0f72bdf44b8bccb728d6ff3aaa
ncourtois 2	5ac92d9b55b30c94f506c0540d6c5a022e0fa1b
ncourtois 3	f2c896486ae5b8e9f0b0




Context menu options:

- Add signature...
- Unlock keychain...
- Lock keychain

9g. Once A Transaction Has 2 Signatures

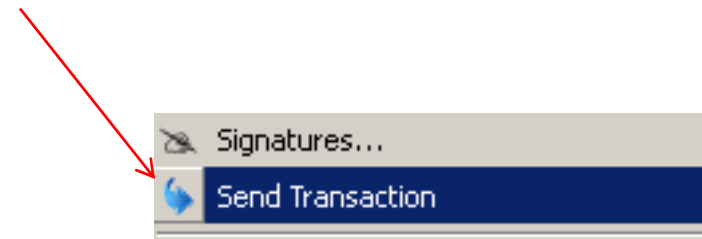
- Verify here:

Transaction is signed.

Keychain Name		Keychain Hash	
ncourtois 1		df207ebb1a686b0f72bdf44b8bccb728d6ff3aaa	
ncourtois 2		5ac92d9b55b30c84f596c9549dec5e922ae0fa1b	Signed
ncourtois 3		f2c896486ae5b8c7992df3809f8c9bf8d1b9f0b0	Signed

9h. Once A Transaction Has 2 Signatures

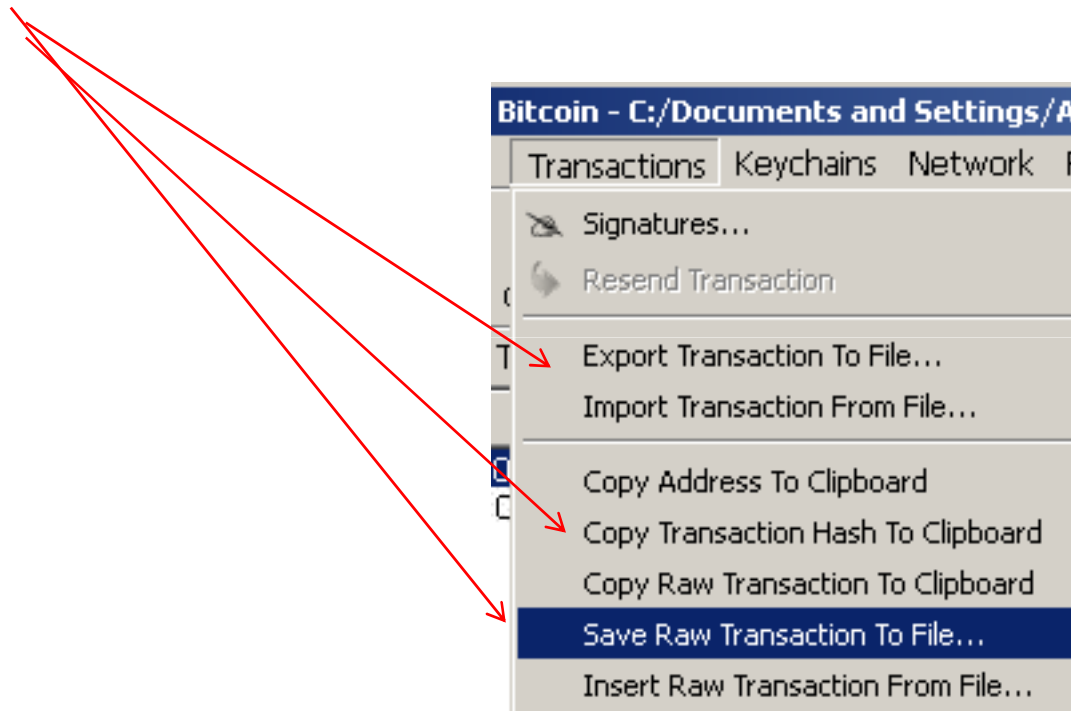
- Now you can either
- DELETE
- or SEND this transaction to the bitcoin network (automatic or manual)



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
- it has worked instantly!

```
0100000001c51cd55a9ab4050a8f20dff7b77327c45ab4f3b6712424a373b0fa3c11d1eaf301000000dfef00004830450220030939123d5399f01487464f756a8214fcad8a2d7f59aba40bcbe6ad1e4a0a61022100a48b72dec7892fcb0f3e9751ad64e01b5cb987ec00547655b386f27dc15c3b74014830450220367ac6c52e264e9b9f09db32b0d17370c694a64f8a91861f724d4d30975ec622022100b59f376bb8efda0c1a473eae5f440eb1b8067cd736dd563ea7a01b24f137af3014c69522102a53ba7c3660d9bf04bc6ff4424993410e8b268d7ae364b44389e1569f88fceb210328afa52561eb08c82c8d4a95bbc5609e539e3ca15fbaffa7a2bd61e240b71f402103aa0f14c3aea36bcca32ceb0177c8fe262014c7cfc7f6b4850ae783d3bf017fa353aeffff0200c40900000000001976a914c9cf7ea770e7ae147ad17ee3eec57b7be50e433588ac1027000000000000017a914924a26c5067f1ab693c2fcd9399a1087c0562dca8700000000
```