How to Setup
a MultiSig Wallet

Nicolas T. Courtois

University College London, 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:
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

Nicolas T. Courtois 2009-2014
**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:

<table>
<thead>
<tr>
<th>Account</th>
<th>Confirmed (BTC)</th>
<th>Pending (BTC)</th>
<th>Total (BTC)</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ncourtois</td>
<td>0.00000000</td>
<td>+0.00000000</td>
<td>0.00000000</td>
<td>2 of ncourtois 1, ncourtois 2, ncourtois 3</td>
</tr>
</tbody>
</table>

Keychains tab: **PC number2**

- only 1 private master on this computer
- 2 machines needed to spend any coins
- don’t forget to unlock to spend BTC
7. Claim Payments

• Each payment can have a different multisig key!
  – Good for anonymity
  – Protects against NSA breaking the bitcoin elliptic curve.

• On PC2:

  ![Image of crypto currency payment interface]

  issues a new receiving address each time...
8. Sb. Pays

• Another person sends money to this multisig address:

![Recent transactions]

10/11/2014 13:54  
-0.0071 BTC

courtois_multisig_tests (3AvA8xUAzuQmSnDPpUDip5v3QBcc9g9Whn8)

• 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
9b. Creating Multisig Payment

- Requires 2 PCs, One PC, One Signature

**WARNING:** 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:

<table>
<thead>
<tr>
<th>Keychain Name</th>
<th>Keychain Hash</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ncourtois 1</td>
<td>df207ebb1a686b0f72bdf44b8bccb728d6ff3aaa</td>
<td></td>
</tr>
<tr>
<td>ncourtois 2</td>
<td>5ac92d9b55b30c84f596c9549dec5e922ae0fa1b</td>
<td>Signed</td>
</tr>
<tr>
<td>ncourtois 3</td>
<td>f2c896486ae5b8c7992df3809f8c9bf8d1b9f0b0</td>
<td>Signed</td>
</tr>
</tbody>
</table>
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`  
  
  ```
  0100000001c51cd55a9ab4050a820ddf7f77327c45ab4f36b712424a373b0fa3c11d1ea3010000000fde0000483045020003083123d5399f0148746f756a8214fcaad8a2d7f59aba40bcebe6ad1e4a0a61022100a48b72dec7892cbb0f3e9751ad64e01b5cb878ec00547655b3861f7d7c15c3b74014830450200367ac6c52e264e96b9190db32b0d17370c694a8a918b11724d4d30975ec622022100b59f376bb8efda0c1a473eaeec5f440eb1b8067cd736dd563ea7a01b24137af3014c69522102a53ba7c3660d9b04b6f8f4424993410e8b28d7ae364b44389e15f5988fceedb210320afa52516eb06a8d2c95b56c50e433588ac10270000000000017a914924a26c5067f1ab693c25cd9399a1087c955dcaeb70000000
  ```

- it has worked instantly!