A First Look at the Usability of Bitcoin Key Management

Shayan Eskandari*
David Barrera†, Elizabeth Stobert‡, and Jeremy Clark**

* Concordia University / BitAccess
**Concordia University, †ETH Zurich, ‡Carleton University
Why?

- Key management is a decade old usability problem
- Bitcoin has introduced new use cases for public key cryptography
- No one has looked at the usability of bitcoin key managements yet
- If it's not usable, Bitcoin won't flourish
Key Management

• Keys are something you *have* instead of *know*

• *Usable Public Key Cryptography*

  • Public Keys should be accessible

  • Private Keys should be securely stored and accessible in case signing is needed
Bitcoin, Eh?

- Cryptocurrency deployed in 2009 with current market cap of $3+ Billion

- A Public ledger holds the list of every transaction in the network, called Blockchain (~25GB)

- Pair of cryptographic keys:
  - Public Verification Key: For receiving Bitcoin (Bitcoin Address)
  - Private Signing Key: For Sending Bitcoin
What’s this about?

• Goal is to identify usability issues and advantages of existing techniques, and propose design recommendation for future Bitcoin clients.

• We did a survey of six Bitcoin key management techniques and usability evaluation of their related tools.
What to do with a key?

• Two obvious places:
  • store on your computer
  • store on a website
• we talk about these two first and then another four
Bitcoin Key Management Techniques
Key in Local Storage

- Store the private keys locally
- Can generate and keep unlimited number of keys
- No other parties are involved

- Wallets are accessible to all other applications
- Should be kept secure and safe
  - Could be stolen
  - Malwares
- Not Portable

  e.g Bitcoin Core (Bitcoin-qt)
Bitcoin Key Management Techniques
Hosted Wallets

• Hosting the private keys
• Standard web authentication mechanism
• Password recovery
• Reduce application complexity (on Mobile devices)
• Cross-Device portability

• Should trust third party
  e.g. Online exchanges
Bitcoin Key Management Techniques
Password-Protected Wallets

• Same as Key in Local Storage but password encrypted

• Address Physical Theft and some digital stealing methods

• Forgetting Password = Losing access to the keys
• User might be confused that his password would work on all devices to access his funds

  e.g. MultiBit
Bitcoin Key Management Techniques
Password-derived Keys

• Derive keys from a password (PBKDF2)
• Cross-Device portability

• Only generates one pair of keys
• Forgetting Password = Losing access to the keys
• Rainbow table attacks

*e.g. BrainWallet*
Bitcoin Key Management Techniques

Offline Storage of Keys

- USB Thumbdrive in a vault
- Paper wallets
  - QR Code
- No trust in third parties
- Inaccessible for immediate use
- Funds might be stolen if observed
- Might lose access to the change address
Change Address

2.3 BTC  →  1 BTC → Bob
Alice

1.3 BTC → Alice’s change address
Bitcoin Key Management Techniques
Air-Gapped Storage

• **Offline device** for holding private keys and signing
• **Online device** for everything else

• *e.g.* Armory

• Hardware Security Modules
  • Signing oracle
  • *e.g.* Trezor
Evaluation Framework¹

10 Criteria

• Malware Resistant
• Key Stored Offline
• No Trusted Third Party
• Resistant to Physical Theft
• Resistant to Physical Observation

• Resilient to Password Loss
• Resilient to Key Churn
• Immediate Access
• No New User Software
• Cross-Device Portability

Scoring: Full (●) - Half (○) and empty for none

¹ Bonneau, Joseph, et al. “The quest to replace passwords”
### Evaluation Result

<table>
<thead>
<tr>
<th>Category</th>
<th>Example</th>
<th>Malware Resistant</th>
<th>Key(s) Kept Offline</th>
<th>No Trusted Third Party</th>
<th>Resistant to Physical Theft</th>
<th>Resistant to Physical Observation</th>
<th>Resilient to Password Loss</th>
<th>Resilient to Key Churn</th>
<th>Immediate Access to Funds</th>
<th>No New User Software</th>
<th>Cross-device Portability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keys in Local Storage</td>
<td>Bitcoin Core</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Password-protected Wallets</td>
<td>MultiBit</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Offline Storage</td>
<td>Bitaddress</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Air-gapped Storage</td>
<td>Armory</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Password-derived Keys</td>
<td>Brainwallet</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Hosted Wallet (Hot)</td>
<td>Coinbase.com</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Hosted Wallet (Cold)</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Hosted Wallet (Hybrid)</td>
<td>Blockchain.info</td>
<td>○ ○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Cash</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Online Banking</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

**TABLE I.** A comparison of key management techniques for Bitcoin (contrasted with traditional financial services). ● indicates the category of client is awarded the benefit in the corresponding column. ○ partially awards the benefit. Details provided inline.
Evaluation Result

Summary

• No single superior approach

• Hosted wallets are the most similar to online banking

• All techniques have potential usability pitfalls
Usability Evaluation
Cognitive Walkthrough

- Expert Evaluation (2 experts)
- Focus is on novice user and emphasizes learnability
- Three Questions:
  1. Will the user see what to do?
  2. Will the user see how to do it?
  3. Will the user know if they have performed the correct action?
- Focus on problems specific to key management within Bitcoin software, not the usability of clients themselves.
Cognitive Walkthrough

Core Tasks

• **T1** - Configure a new Bitcoin address and obtain its balance

• **T2** - Spend Bitcoin

• **T3** - Spend Bitcoin from a secondary device

• **T4** - Recover from loss of main credentials
Cognitive Walkthrough
Guidelines \(^2\)

- **G1** Users should be aware of the steps they have to perform to complete a core task.
- **G2** Users should be able to determine how to perform these steps.
- **G3** Users should know when they have successfully completed a core task.
- **G4** Users should be able to recognize, diagnose, and recover from non-critical errors.
- **G5** Users should not make dangerous errors from which they cannot recover.
- **G6** Users should be comfortable with the terminology used in any interface dialogues or documentation.
- **G7** Users should be sufficiently comfortable with the interface to continue using it.
- **G8** Users should be aware of the application’s status at all times.

\(^2\) Clark, Jeremy, et al - Usability of anonymous web browsing
Cognitive Walkthrough
Demo - Offline Storage (Paper Wallet)

bitaddress.org

T1 - Configure a new Bitcoin address and obtain its balance
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness...
OR type some random characters into this textbox

Donations: 1NiNja1bUmhsOTXozBRBEtR8LeF9TgbZBN
GitHub Repository (zip)

Version History (2.9.8)
527B 5C82 B1F6 B2DB 72A0
ECBF 8749 7B91 6397 4F5A
(PGP) (sig)

Copyright bitaddress.org. JavaScript copyrights are included in the source. No warranty.
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness... 233
OR type some random characters into this textbox

617091f9e314ba6c31897c18ed6fd484e9774008480178a6f95fca3b62321dc845
ff8ad0c56aaf084b01140054461c0072e9d47edfbcb481b93dc67afdf79a7cb7c7
6fffc542b0dd90eef5bced70b3ed65a3b64326a876c8c0ace83babd305deab51c
bc64f294b04ee5f5080c6caca221a7aac0d6559ad8f84af93238464c5879225633
a70e6640d411f0899c64c0aba0cf05eac87924e2bbcd687ae88a52b404342034b
f442f7ac677ae6d13b3b82921b4f1f46a24eae59716bb9a5e4abe52dc624cac5d
5514a662d91a3801f9f570218c0cc5a8f2349d3b793b27a5086bc148972a05fdd
415055d2690c32b322c886a622ef8e08ed3213de45c696b18

Donations: 1NINja1bUmhSoTXozBRBEtR8LeF9TgZBN
GitHub Repository (zip)

Version History (2.9.8)
527B 5CB2 B1F6 B2DB 72A0
ECBF 8749 7B91 6397 4F5A
(PGP) (sig)

Copyright bitaddress.org. JavaScript copyrights are included in the source. No warranty.
A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you are familiar with PGP you can download this all-in-one HTML page and check that you have an authentic version from the author of this site by matching the SHA256 hash of this HTML with the SHA256 hash available in the signed version history document linked on the footer of this site. If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will not be retrievable. Your Bitcoin private key should be kept a secret. Whomever you share the private key with has access to spend all the bitcoins associated with that address. If you print your wallet then store it in a zip lock bag to keep it safe from water. Treat a paper wallet like cash.

Add funds to this wallet by instructing others to send bitcoins to your Bitcoin address.
A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you are familiar with PGP you can download this all-in-one HTML page and check that you have an authentic version from the author of this site by matching the SHA256 hash of this HTML with the SHA256 hash available in the signed version history document linked on the footer of this site. If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will not be retrievable. Your Bitcoin private key should be kept a secret. Whomever you share the private key with has access to spend all the bitcoins associated with that address. If you print your wallet then store it in a zip lock bag to keep it safe from water. Treat a paper wallet like cash.

Add funds to this wallet by instructing others to send bitcoins to your Bitcoin address.

Check your balance by going to blockchain.info or blockexplorer.com and entering your Bitcoin address.

Spend your bitcoins by going to blockchain.info and sweep the full balance of your private key into your account at their website. You can also spend your funds by downloading one of the popular bitcoin p2p clients and importing your private key to the p2p client wallet. Keep in mind when you import your single key to a bitcoin p2p client and spend funds your key will be bundled with other private keys in the p2p client wallet. When you perform a transaction your change will be sent to another bitcoin address within the p2p client wallet. You must then backup the p2p client wallet and keep it safe as your remaining bitcoins will be stored there. Satoshi advised that one should never delete a wallet.
<table>
<thead>
<tr>
<th>Height</th>
<th>Age</th>
<th>Transactions</th>
<th>Total Sent</th>
<th>Relayed By</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>342317</td>
<td>5 minutes</td>
<td>1</td>
<td>25.00 BTC</td>
<td>F2Pool</td>
<td>0.25</td>
</tr>
<tr>
<td>342316</td>
<td>6 minutes</td>
<td>1867</td>
<td>9,771.76 BTC</td>
<td>121.40.205.76</td>
<td>967.22</td>
</tr>
<tr>
<td>342315</td>
<td>29 minutes</td>
<td>1972</td>
<td>15,013.72 BTC</td>
<td>Eligius</td>
<td>881.2</td>
</tr>
<tr>
<td>342314</td>
<td>1 hour 5 minutes</td>
<td>328</td>
<td>1,852.91 BTC</td>
<td>F2Pool</td>
<td>248.03</td>
</tr>
<tr>
<td>342313</td>
<td>1 hour 9 minutes</td>
<td>483</td>
<td>2,834.88 BTC</td>
<td>123.56.40.59</td>
<td>273.22</td>
</tr>
<tr>
<td>342312</td>
<td>1 hour 16 minutes</td>
<td>339</td>
<td>1,410.93 BTC</td>
<td>KnCMiner</td>
<td>169.01</td>
</tr>
</tbody>
</table>

**Latest Transactions**

- 3a23ce75a7... (LuckyBit hot wallet) < 1 minute | 0.00436528 BTC
- e6cb41d413a471c5b25fb77c0... < 1 minute | 0.36882973 BTC
- 9fd7d2732186795f3d50f460f... < 1 minute | 0.0454669 BTC
- 865d849cbe85bc6ed77c3890e... < 1 minute | 0.10030819 BTC

**Search**

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Address / ip / SHA hash

**NEWS**

- The Next Big Boost for Bitcoin Mining: Oil Immersion Cooling
  - GRC Cooling < 1 minute
- Bitcoin Panel Seeks Regulation Redo at New Jersey Hearing
  - CoinDesk 19 minutes ago
**Bitcoin Address** Addresses are identifiers which you use to send bitcoins to another person.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong> 1JCMTL8wPLPWBivCZckvvhVYKW5Ja9MgkN</td>
<td><strong>No. Transactions</strong> 0</td>
</tr>
<tr>
<td><strong>Hash 160</strong> bc9fc9bb43df3f3bde77fd4597f93068f9f9100</td>
<td><strong>Total Received</strong> 0 BTC</td>
</tr>
<tr>
<td><strong>Tools</strong> Taint Analysis - Related Tags - Unspent Outputs</td>
<td><strong>Final Balance</strong> 0 BTC</td>
</tr>
</tbody>
</table>

**Transactions (Oldest First)**

No transactions found for this address, it has probably not been used on the network yet.
Discussion

• No solution just trade offs

• Metaphors and Abstractions
  • Send Coin vs. Digitally Sign a transaction
  • Generate Change addresses without user notification

• Technical Language
Questions?

“Bitcoin’s usability limitations, particularly those related to key management, pose challenges to its rising popularity.”

Contacts:

s_eskand@encs.concordia.ca
david.barrera@inf.ethz.ch
elizabeth.stobert@gmail.com
j.clark@concordia.ca