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


Auto Body & Paint
Current
Light snow
-16°C
Feels Like: -27
Air Quality
15 Good
UV Report
0 Low
Afternoon
Sunday
2-4cm
-15°
Evening
Sunday
<1cm
-14°
Overnight
Sunday
-13°
Morning
Monday
~1cm
-13°
Monday
Feb 09
-10° -13°
Tuesday
-8° -15°
The Weather Network
Montréal, QC

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

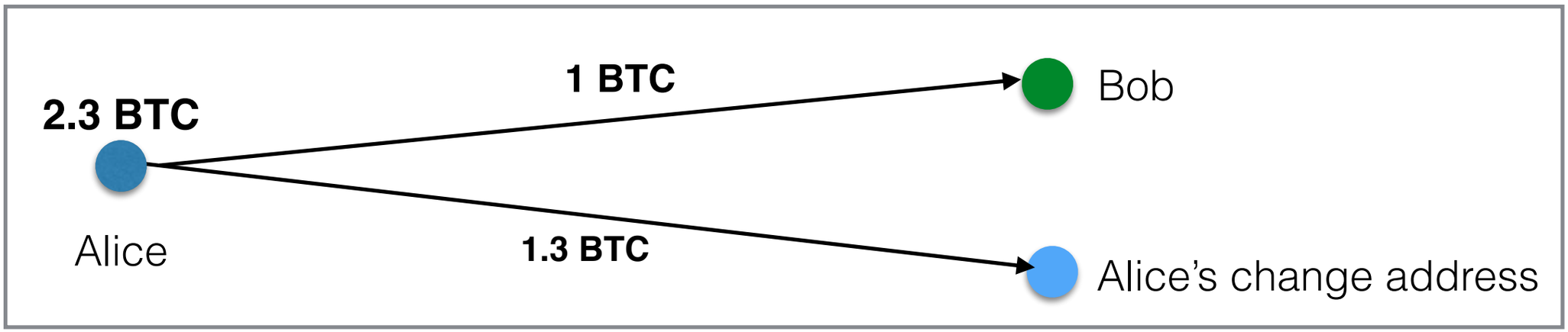
- USB Thumbdrive in a vault

- 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



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 Framework[1]

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

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

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

bitaddress.org

https www.bitaddress.org/bitaddress.org-v2.9.8-SHA256-2c5d16dbcde600147162172090d940fd9646981b7d751d9bddfc5ef383f89308.html

Reader

English | Español | Français | ελληνικά | italiano | Deutsch | Česky | Magyar | 日本語 | 简体中文 | Русский

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

```
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness...
OR type some random characters into this textbox
```

Donations: **1NiNja**1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)

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

bitaddress.org

https www.bitaddress.org/bitaddress.org-v2.9.8-SHA256-2c5d16dbcde600147162172090d940fd9646981b7d751d9bddfc5ef383f89308.html

Reader

English | Español | Français | ελληνικά | italiano | Deutsch | Česky | Magyar | 日本語 | 简体中文 | Русский

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

```
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness...  233
OR type some random characters into this textbox

617091f9e314ba6c31897c18ed6fd484e9774008480178a6f95fca3b62321dc845
ff8ad0c5d6afc084b01140054461c0072e9d47edfbcb481b93dc67afd79a7cb77c
6ffc542b0dd90efef5bced70b3edd65a3b64326a876c8c0ace83babd305deab51c
bc64f294b04ee5f5080c6ccca221a7aac0d6559ad8f84af93238464c5879225633
a70e6640d411f0899c64c0aba0cff05eac87924ebbfcd687ae88a52b404342034b
f442f7ac677ae6d13b3d82921b4f1f46a24eae59714bbb9a5e4abe52dc624cac5d
5514a662d91a8301f9f570218cec5aa8f2b349d3b793b27a5086bc148972a05fdd
415055d2690c32b322c886a622ef8e08ed3213d4ef5c696b18
```

Donations: **1NiNja**1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)

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

bitaddress.org

https www.bitaddress.org/bitaddress.org-v2.9.8-SHA256-2c5d16dbcde600147162172090d940fd9646981b7d751d9bddfc5ef383f89308.html

Reader

English | Español | Français | ελληνικά | italiano | Deutsch | Česky | Magyar | 日本語 | 简体中文 | Русский

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Generating Bitcoin Address...
MOVE your mouse around to add some extra [redacted] ... 60
OR type some random characters into this textbox USEC15 aaaaaaaaaaa

```
bc85ffede301575c5d4b7e1d3c92ba5fef4d7ffaa50d0c909ee71d0c30d288a894
0e87b00a1f7366b1051da2c238eab034295c8c3548a57bd2b1a48321302a196792
cdabfe9d1646f3c6564efeb7520c4efd938bc8eb1ca09b693cf526c57996749881
8859ff2095e103f4a056167e37778fc1ea691ebec49794472818a514c9c113775d
fa40de065d9a468c58741bd7388f32bd761a36dc724101cf357e75abeebcd3c199
a391d8299fa4f90655bea24a8b9fe9c147ac59f4e2c9707e9d92ae1f23d5266d52
64551742ca32b125543c344254e9a99443d31b0444da24fa1c204b83742dec7825
09ace58f13f5787858ad375dc5d2dd6683cc0000a532729405
```

Donations: **1NiNja**1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)

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

bitaddress.org

https www.bitaddress.org/bitaddress.org-v2.9.8-SHA256-2c5d16dbcde600147162172090d940fd9646981b7d751d9bddfc5ef383f89308.html

Reader

English | Español | Français | ελληνικά | italiano | Deutsch | Česky | Magyar | 日本語 | 简体中文 | Русский

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address

SHARE

1JCMTL8wPLPWBivCZckvvhVYKW5Ja9MgkN

Private Key (Wallet Import Format)

SECRET

5KdpwAtxnDtCBC9gnt63Epw94iFGMTTw2ykh8NqMuk3sbVx4mxf

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.

bitaddress.org

https www.bitaddress.org/bitaddress.org-v2.9.8-SHA256-2c5d16dbcde600147162172090d940fd9646981b7d751d9bddfc5ef383f89308.html

Reader

Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address

SHARE

1JCMTL8wPLPWBivCZckvvhVYKW5Ja9MgkN

Private Key (Wallet Import Format)

SECRET

5KdpwAtxnDtCBC9gnt63Epw94iFGMTTw2ykh8NqMuk3sbVx4mxf

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.

Bitcoin Block Explorer - Blockchain.info

Blockchain Luxembourg S.A.R.L blockchain.info

Reader

BLOCKCHAIN info

Home | Charts | Stats | Markets | API | Wallet

Search

Home Welcome to Blockchain

More...

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
342317	5 minutes	1	25.00 BTC	F2Pool	0.25
342316	6 minutes	1867	9,771.76 BTC	121.40.205.76	967.22
342315	29 minutes	1972	15,013.72 BTC	Eligius	881.2
342314	1 hour 5 minutes	328	1,852.91 BTC	F2Pool	248.03
342313	1 hour 9 minutes	483	2,834.88 BTC	123.56.40.59	273.22
342312	1 hour 16 minutes	339	1,410.93 BTC	KnCMiner	169.01

Latest Transactions

3a23ce75a7... (LuckyBit hot wallet)	< 1 minute	0.00436528 BTC
e6cb41d413a471c5b25fb77c0...	< 1 minute	0.36828973 BTC
9fd7d2732186795ffd50f460f...	< 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

Search

NEWS

The Next Big Boost for Bitcoin Mining: Oil Immersion Cooling

GRC Cooling ← 1 minute ago

Bitcoin Panel Seeks Regulation Redo at New Jersey Hearing

CoinDesk 19 minutes ago

Ok (1656 Nodes Connected)

About Us & Contact - Privacy Policy - Terms of Service - - Advanced: Enable - Bitcoin

Bitcoin Address 1JCMTL8wPLPWBivCZckvvhVYKW5Ja9MgkN

Blockchain Luxembourg S.A.R.L blockchain.info/address/1JCMTL8wPLPWBivCZckvvhVYKW5Ja9MgkN

Reader

BLOCKCHAIN info

Home Charts Stats Markets API Wallet

Search

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1JCMTL8wPLPWBivCZckvvhVYKW5Ja9MgkN
Hash 160	bc9fc9bb43df3f93bde77fd4597f93068f9f9100
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

Filter

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

Ok (1661 Nodes Connected)

About Us & Contact - Privacy Policy - Terms of Service - - Advanced: Enable - Bitcoin

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