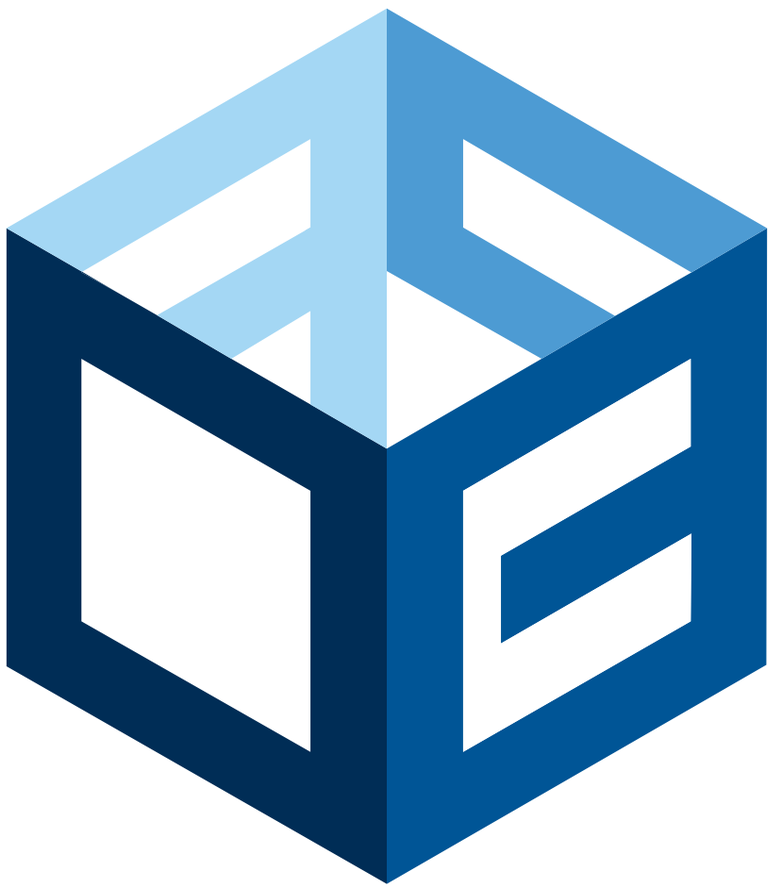


open bitcoin privacy project

Bitcoin Wallet Privacy Rating Report

Spring 2015

Table of Contents

Introduction

Any technology as revolutionary as Bitcoin is bound to come with surprises. In fact, if you've been following the technology for any appreciable amount of time, you will often find yourself in awe of some unconsidered and new angle, some formerly inconceivable subtlety that challenges your assumptions about finance and commerce. This is the age of uncensored and programmable money. We don't know exactly what the future holds for Bitcoin, but we do know for sure that the world will never be the same.

The privacy implications of Bitcoin are one such surprise for many of its students. We are emerging from a banking system that takes for granted not only financial control by trusted third parties, but also total information awareness for those same organizations. The details of Main Street's transactions have, until today, been stored in esteemed and marbled halls occupied by men in fine suits. We have carried around plastic cards with our names and numbers, swiped and authenticated with each purchase; we have emailed dollars, francs, and yen to our friends and eBay sellers -- except for those of us excluded by border or notoriety. Bitcoin flips the script by placing these details not in the hands of banks, but the world. The future will transact on a global and public ledger. This opens up many wonderful opportunities, and just as many pitfalls.

Financial privacy is enforced lightly by the Bitcoin protocol. The short section on the matter dedicated by Satoshi in his whitepaper contains helpful suggestions, but no rules. Protections are pushed to the edges of the network, to the services we use and the wallet software we execute on our computing devices. Our services and software have long ignored Satoshi's suggestions, however, relying on a prevailing and dubious notion of Bitcoin as inherently anonymous.

The Open Bitcoin Privacy Project publishes rating reports to highlight where software is succeeding at protecting our privacy, and where it is failing. We have selected key behavioral patterns and features of Bitcoin software that measures its effectiveness at protecting the financial details of its users. Technically-minded readers will find our Threat Model on page 26, explaining the motivation for the metrics we developed.

Each wallet rated in this report was analyzed in terms of the usability of its privacy projections, the effectiveness of those protections, and the level of guidance provided to users to guard their own data. We have provided scores broken down by category for each wallet. Casual readers of the report can simply skip to our rankings by total score on page 5.

We carefully designed our testing methodology, detailed on page 3, to be as objective and independently verifiable as possible to reduce bias. Additionally, we reached out to each of the organizations that produce the software we've rated to provide clarifications; their responses to our questionnaire are contained in this report. Still, the ratings rely on our expertise, and the wisdom of the Bitcoin community members who provided feedback. We welcome your input to improve future reports.

It is our hope that this report will inform your selections when choosing wallets, and when communicating desired features to developers. Thank you for taking the time to read our Spring 2015 report. We look forward to your feedback.

Sincerely,

Kristov Atlas
OBPP Contributor

Privacy Ratings Methodology

Each wallet is subject to 38 privacy tests organized into five categories and 14 sub-categories with variable weights representing the relative importance of each measure. The result of each test is converted to a raw numeric score between 0 and 100 via the methods described below and multiplied by the test's weighting factor.

The criteria are designed such that a higher score is always better than a lower score. By adding up the individual weighted test scores, an overall wallet privacy score is determined with a maximum possible score of 100 points.

Most of the criteria in the wallet ratings generate results in one of the following standard forms:

BOOLEAN

When the result of a test is true, that item is assigned a score of 100.
When the result of a test is false, the item is assigned a score of 0.

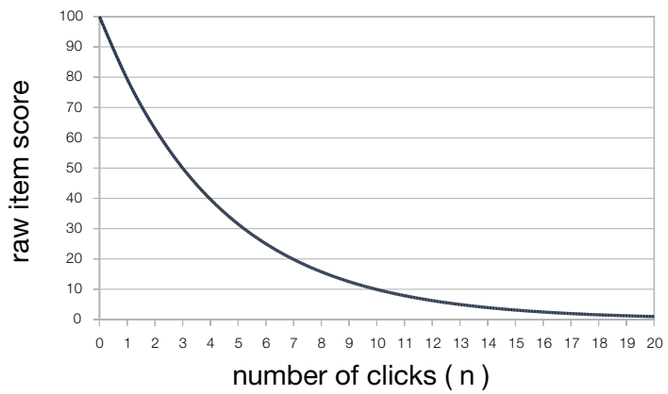
NUMBER OF CLICKS

The number of clicks needed to perform an action is converted to a score according to the following formula:

$100 \times 2^{-n/3}$ where n is the number of clicks

Zero clicks means the wallet achieves the desired behavior without any additional user action, which results in an item score of 100. Every three clicks drops the score by half. When the desired behavior can not be achieved in a particular wallet, the score is zero.

If a particular action requires the user to type a command, each press of the space bar and return key counts as a click.



TIERED

Two specific privacy tests are evaluated on an individualized basis according to the following tiered assessments:

IV.A.2 Balance information is obtained in a manner which avoids leaking the addresses in a wallet to network peers

- 100: Full node - The wallet is part of, or works with, a full node under the user's exclusive control
- 75: Carefully filtered - Address filters are used, but filters are never updated and when a new one is required it is registered with a brand new peer
- 50: Unsafely filtered - Address filters are used, and they are updated or reuse peers.
- 0: Unfiltered - Balance is obtained from a peer which can easily connect wallet addresses to a specific connection/wallet

IV.C.5 Compatible with latest version of Tails

- 100: Actually included in the Tails live CD
- 75: Program and any dependencies are packaged into a single file which can be easily installed
- 50: Installation is possible, but requires multiple complex steps
- 0: Will not run on Tails

When a test is not clearly applicable to a particular wallet because the wallet does not include the criteria tests, a score of either 0 or 100 is applied according to the following guidelines:

- If the test checks for the absence of undesirable behavior, and the wallet avoids the undesirable behavior for reasons unanticipated by the authors of the criteria, the item is scored at 100.
- If the test checks for the presence of desirable behavior, and the wallet achieves the same benefit of the desired behavior in methods unanticipated by the authors of the criteria, the item is scored at 100.
- In all other cases, the item is scored at 0.

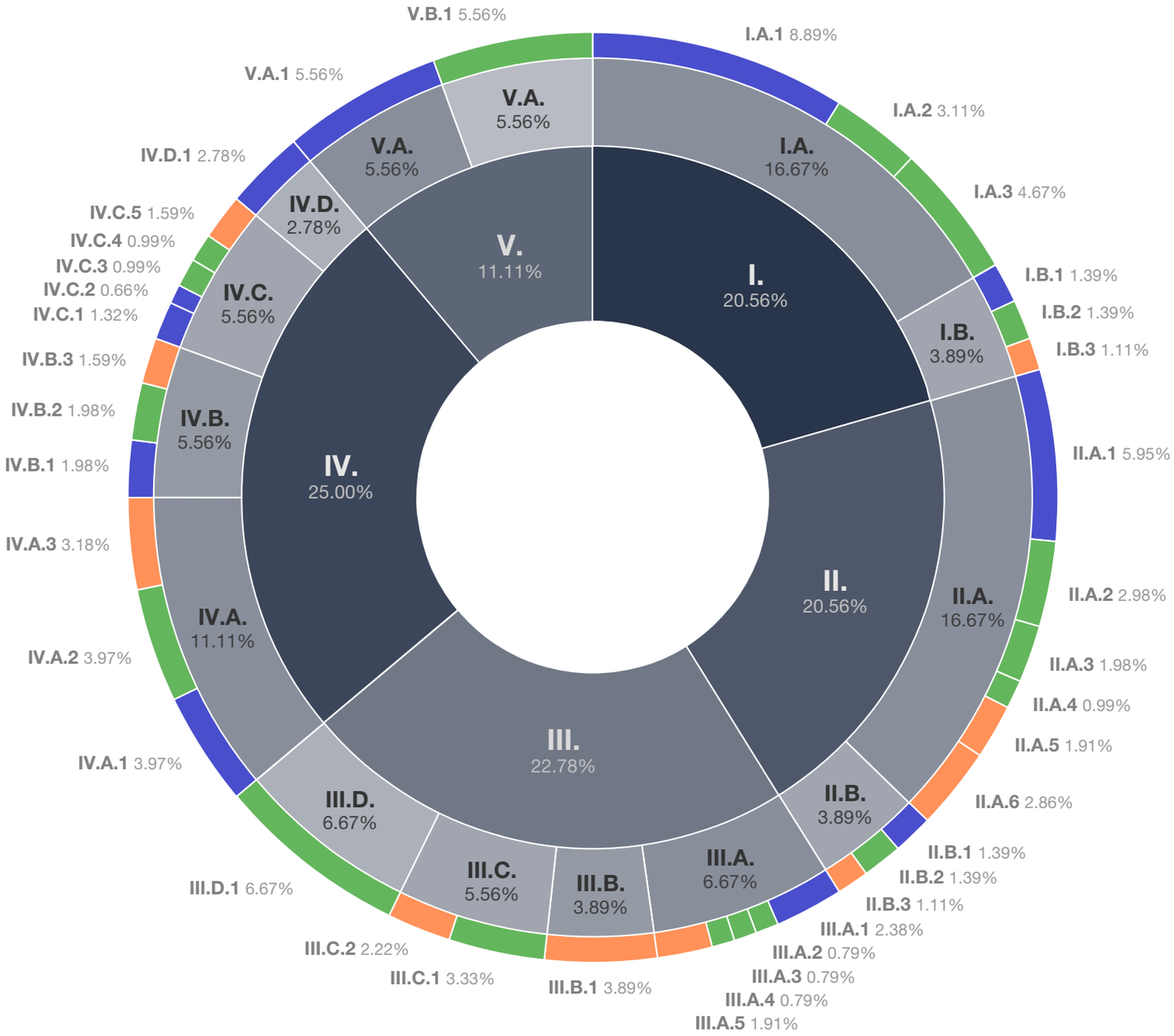
Detailed scoring data for each wallet and a full description of each test is included in Appendix B beginning on page 27.

Privacy Criteria Weighting

The weighting factors for the five categories and 14 sub-categories are shown in the following outline with individual test weighting factors shown around the perimeter of the circle chart.

Detailed scoring data for each wallet and a full description of each test is provided in Appendix B beginning on page 27.

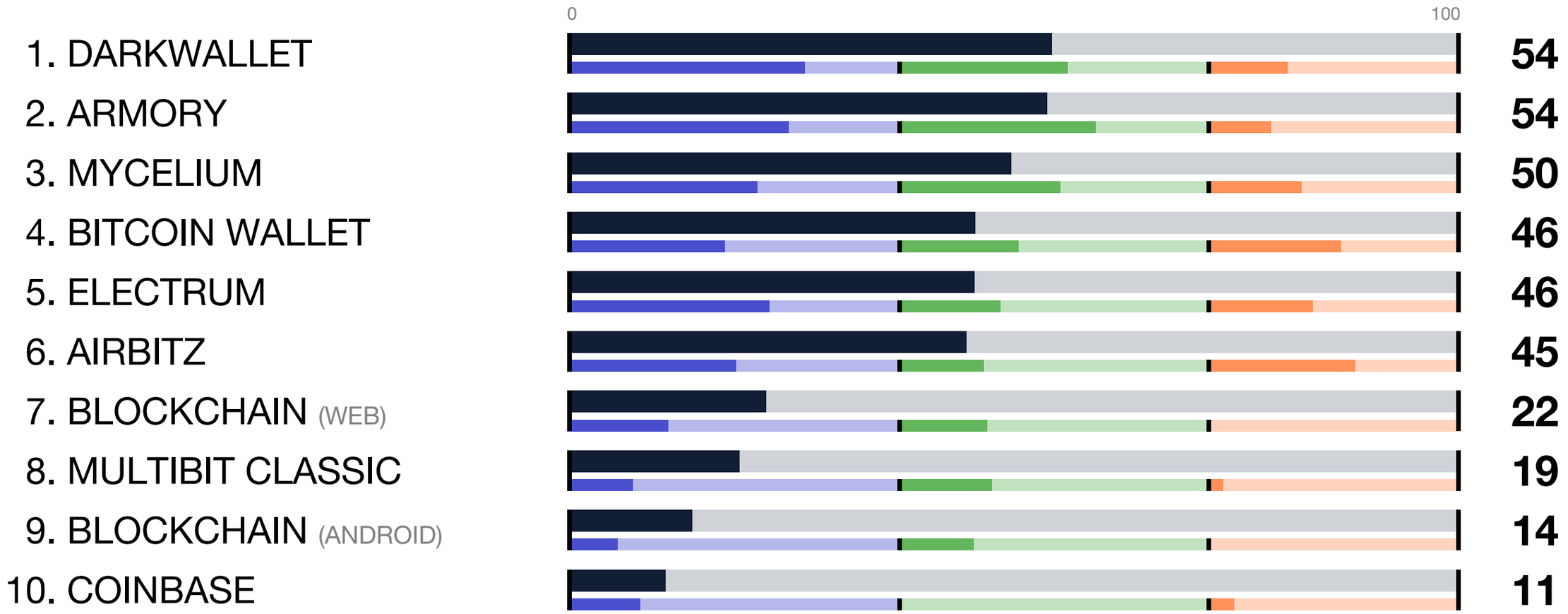
I.	**Receiving Address Generation and Backup**		**20.56%**
	I.A.	Generation	16.67%
	I.B.	Backup	3.89%
II.	**Change Address Generation and Backup**		**20.56%**
	II.A.	Generation	16.67%
	II.B.	Backup	3.89%
III.	**Privacy from Blockchain Observers**		**22.78%**
	III.A.	Mixing	6.67%
	III.B.	Address Reuse	3.89%
	III.C.	Input Merging	5.56%
	III.D.	Identity Separation	6.67%
IV.	**Privacy from Network Observers**		**25.00%**
	IV.A.	Balance Information	11.11%
	IV.B.	Outgoing Transactions	5.56%
	IV.C.	Identity Separation	5.56%
	IV.D.	Operating System Support	2.78%
V.	**Receiver Privacy**		**11.11%**
	V.A	ECDH Address Support	5.56%
	V.A.	Receiver Identity	5.56%



Each individual privacy test is also assigned one of three classifications:

- Usability
- Quality
- Feedback

Overall Wallet Privacy Rankings



USABILITY RANKINGS

1. Darkwallet
2. Armory
3. Electrum
4. Mycelium
5. AirBitz
6. Bitcoin Wallet
7. Blockchain (Web)
8. Coinbase
9. Multibit Classic
10. Blockchain (Android)

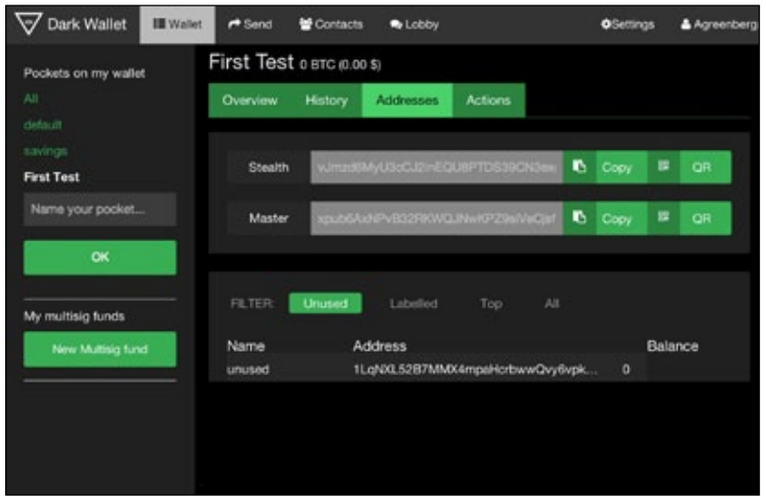
QUALITY RANKINGS

1. Armory
2. Darkwallet
3. Mycelium
4. Bitcoin Wallet
5. Multibit Classic
6. Blockchain (Web)
7. Electrum
8. AirBitz
9. Blockchain (Android)
10. Coinbase

FEEDBACK RANKINGS

1. AirBitz
2. Bitcoin Wallet
3. Electrum
4. Mycelium
5. Darkwallet
6. Armory
7. Coinbase
8. Multibit Classic
9. Blockchain (Web)
10. Blockchain (Android)

Darkwallet



Version Reviewed: 0.8.0 (chrome plugin)

Supported Platforms: Google Chrome Browser

Darkwallet is the first Bitcoin wallet explicitly devoted to privacy as a primary design goal, created by Amir Taaki and Cody Wilson. Darkwallet in the only wallet we've considered so far which includes automatic CoinJoin mixing and ECDH Stealth Addresses. Another notable feature in Darkwallet is an automatic P2P network for messaging between users.

As demonstrated by its score, Darkwallet is generally successful in its attempts to avoid privacy pitfalls. Some of the weaknesses include a reliance on third party Obelisk servers which have the ability to de-anonymize users; theoretically users could run their own Obelisk server, but this is beyond the capabilities of most potential Darkwallet users. Another factor that makes Darkwallet weaker than it could be is its relatively small user base, which makes CoinJoin unlikely to find a partner for on-demand mixing.

The future of Darkwallet is currently uncertain, as it has not yet reached its release milestone and no development activity has occurred since February 20th.

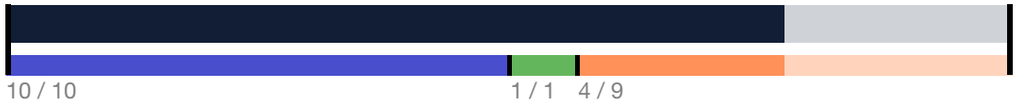
OVERALL WALLET PRIVACY

TOTAL SCORE

54 / 100

USABILITY	QUALITY	FEEDBACK
27 / 36	**19** / 35	**9** / 29

RECEIVING ADDRESS GENERATION & BACKUP



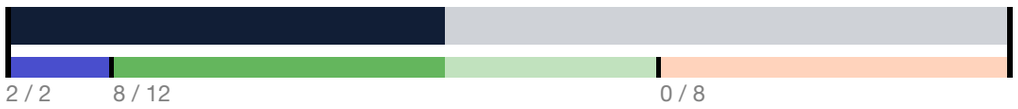
CATEGORY SCORE

16 / 21

CHANGE ADDRESS GENERATION & BACKUP

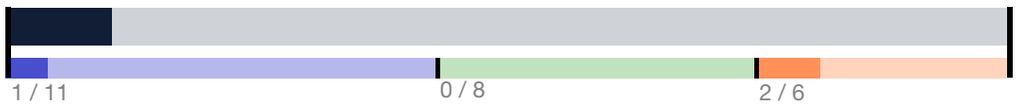
15 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS



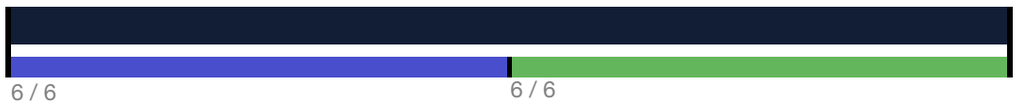
10 / 23

PRIVACY FROM NETWORK OBSERVERS



3 / 25

PRIVACY FOR TRANSACTION RECIPIENTS



11 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Darkwallet

**The developers of Darkwallet did not respond to the OBPP questionnaire.*

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   Backups have been invalidated by new receiving or change address creation

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   An outgoing transaction sends funds to a previously-used address

   An outgoing transaction links inputs from multiple addresses

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   An outgoing transaction links inputs from multiple accounts/identities

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   Randomizing the position of the change output(s)

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   Intentionally creating "decoy" change outputs that have a low number of significant digits

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Any of the above with a public IP address

   Any of the above with a registered account

   Any of the above with a persistent software or hardware fingerprint

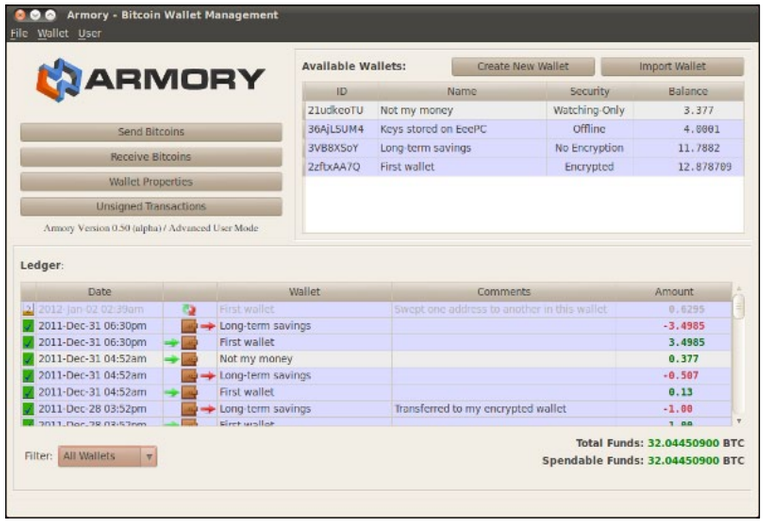
7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

Armory

OVERALL RANK
2ND



Version Reviewed: 0.93.1 (Linux)

Supported Platforms: Linux, OSX, Windows

Armory is a security-focused desktop wallet geared toward intermediate and advanced Bitcoin users. The open-source consumer wallet was first announced in early 2012. In recent months, the company has pivoted to focus their efforts primarily on enterprise customers. In addition to support for advanced security features such as offline signing and fragmented backups, Armory compares favorably to competing wallets in terms of privacy. Armory utilizes Bitcoin Core (bitcoind) to connect to the Bitcoin network. Consequently, Armory users enjoy the network privacy benefits of using a full node. The software is compatible with deterministic address generation and does not reuse addresses by default. Armory transactions broadcast through Bitcoin Core can often be routed through Tor with minor configuration in order to bolster network privacy.

Armory can improve privacy protections for users on the blockchain by supporting a mixing protocol such as CoinJoin. More careful handling of change outputs would also bolster Armory's protections on the blockchain. Additionally, Armory can provide users more feedback through the GUI about potential privacy degradations that may occur — before the transactions are broadcast — and help steer the user through avoiding those pitfalls.

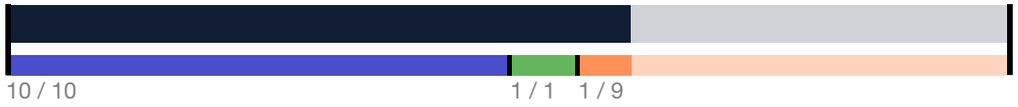
OVERALL WALLET PRIVACY

TOTAL SCORE

54 / 100

USABILITY	QUALITY	FEEDBACK
25 / 36	**22** / 35	**7** / 29

RECEIVING ADDRESS GENERATION & BACKUP



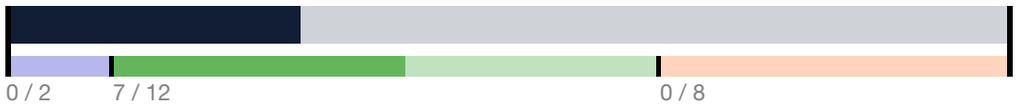
CATEGORY SCORE

13 / 21

CHANGE ADDRESS GENERATION & BACKUP

10 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS

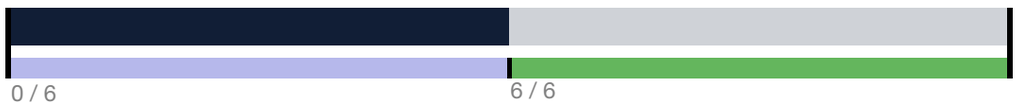


7 / 23

PRIVACY FROM NETWORK OBSERVERS

19 / 25

PRIVACY FOR TRANSACTION RECIPIENTS



6 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Armory

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

   Wallet.

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   No, Could be implemented with ArmoryD.

   Backups have been invalidated by new receiving or change address creation

   Not applicable because Armory wallets use deterministic address generation.

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   No, Could be implemented with ArmoryD.

   An outgoing transaction sends funds to a previously-used address

   No, Could be implemented with ArmoryD.

   An outgoing transaction links inputs from multiple addresses

   No, Could be implemented with ArmoryD.

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   No.

   An outgoing transaction links inputs from multiple accounts/identities

   Not applicable.

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

   Not necessarily, We have the ability "secure" print your backup from an offline computer. With secure print the user writes a code on the backup page. The written code would be necessary during restoration.

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   Randomizing the position of the change output(s)

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   Intentionally creating "decoy" change outputs that have a low number of significant digits

   None of those

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

   Depends on how it's implemented with ArmoryD.

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Any of the above with a public IP address

   Any of the above with a registered account

   Any of the above with a persistent software or hardware fingerprint

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

   Not applicable.

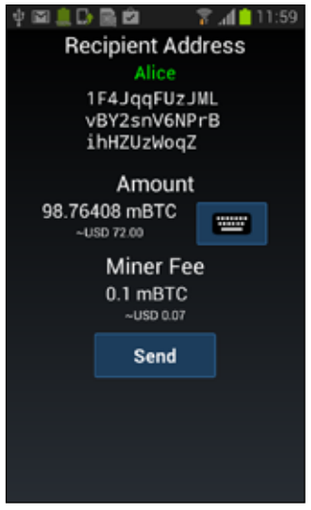
8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

   No.

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

   No.

Mycelium



Version Reviewed: 2.2.0 (Android)

Supported Platforms: Android, iOS

Many long-time Bitcoin users have regarded Mycelium Bitcoin Wallet as the leading Android wallet throughout 2014 and in to 2015. In terms of privacy features, Mycelium implements HD wallets based on BIP44, including multiple account support, and does not encourage address reuse by default. Mycelium is notable for including Local Trader, a built-in P2P system for finding traders to exchange between local currencies and Bitcoin.

Mycelium is the best performer of all mobile wallets in this round of rating by OBPP, but its score suffers from the method via which the wallet obtains balance information. Mycelium wallets obtain their balance information from dedicated Mycelium servers instead of connecting to Bitcoin network peers. While this does provide substantial benefits in terms of performance and battery life, this practice places Mycelium in a position to collect identifying information about their users. While Mycelium has very good support for Tor in their wallet, connecting to Mycelium servers via Tor only partially mitigates this privacy weakness.

OVERALL WALLET PRIVACY

TOTAL SCORE

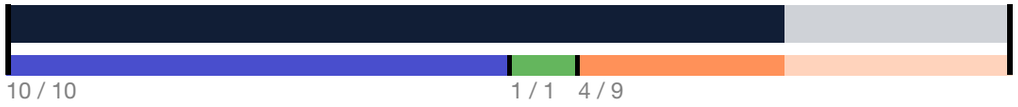
50 / 100

USABILITY **21** / 36

QUALITY **18** / 35

FEEDBACK **10** / 29

RECEIVING ADDRESS GENERATION & BACKUP



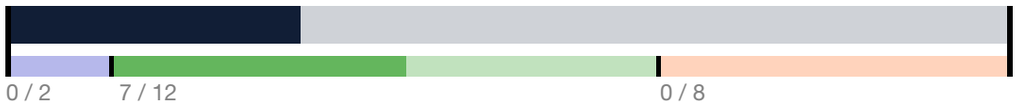
CATEGORY SCORE

16 / 21

CHANGE ADDRESS GENERATION & BACKUP

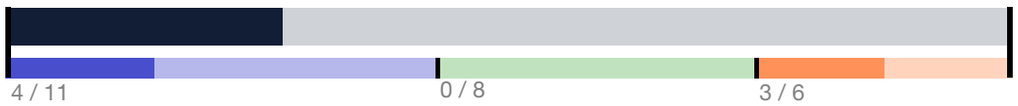
15 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS



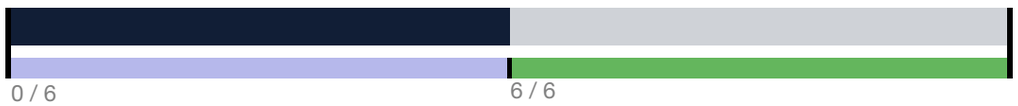
7 / 23

PRIVACY FROM NETWORK OBSERVERS



7 / 25

PRIVACY FOR TRANSACTION RECIPIENTS



6 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Mycelium

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

   Wallet. All of the private keys needed to create a blockchain transaction are under the exclusive control of the user.

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   No.

   Backups have been invalidated by new receiving or change address creation

   No (we use HD wallets, so this isn't an issue, but we warn if single address accounts have not been backed up).

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   Wallet does not support mixing yet.

   An outgoing transaction sends funds to a previously-used address

   No, but previous addresses are not displayed, or available to send to from within the wallet. A new address is always used.

   An outgoing transaction links inputs from multiple addresses

   No.

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   Our wallet does not currently provide any warning to users concerning their connection to the website through an anonymous channel, such as Tor.

   An outgoing transaction links inputs from multiple accounts/identities

   Yes. If Tor is selected as a connection method, the connection either goes through to our .onion address, or fails completely.

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

   No. Backup is done by displaying a 12 word seed, on a protected (can't screenshot) display, one word at a time.

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   We have only one change output, but always to a new address.

   Randomizing the position of the change output(s)

   If you mean randomizing the position of the two addresses, change and sent, then yes

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   No.

   Intentionally creating "decoy" change outputs that have a low number of significant digits

   No.

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

   Not applicable, but CoinShuffle will be implemented, so use that for reference when done.

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Not for spending, since all signing is done on the wallet, and address information is not tracked. We can only correlate addresses where more than one is used for inputs, same as anyone else can by looking at transactions on the blockchain. However, for balance lookups yes, since we don't have a good way to anonymize that yet (bloom filters aren't a good solution either), but we don't keep logs of balance lookups.

   Any of the above with a public IP address

   If connecting through clearweb, it's possible, but we don't log IP addresses either. And since we also added full support for Tor, users can completely hide their IP addresses if they want to.

   Any of the above with a registered account

   There are no registered accounts in our app, or any identifiable information besides addresses.

   Any of the above with a persistent software or hardware fingerprint

   No.

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

   Not applicable.

8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

   No, all incoming and outgoing transaction information is broadcast through our servers, though that limits such tracking to just knowing that the user is a Mycelium user.

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

   No, all balance information and signed transactions go through our server.

Bitcoin Wallet

Version Reviewed: 4.19 (Android)

Supported Platforms: Android

Andreas Schildbach's Bitcoin Wallet is the oldest mobile Bitcoin wallet in use. Development for the Android-based wallet began in March of 2011. As the first mobile wallet to gain widespread use, it has served as a de facto reference implementation for Android bitcoin wallets.

Bitcoin Wallet holds up well in terms of privacy features compared to more feature-rich wallets due to its simple interface. Bitcoin Wallet provides a simple interface that doesn't allow users to perform privacy-reducing actions like reusing addresses for receiving funds. Multiple account support is Bitcoin Wallet's single largest missing feature compared to its mobile competition. As with other mobile wallets, the software could improve user privacy protection by adopting practices such as mixing, use of shared secret addresses schemes like those based on Elliptic-Curve Diffie Hellman, and better handling of privacy when obtaining balance information or broadcasting transactions.

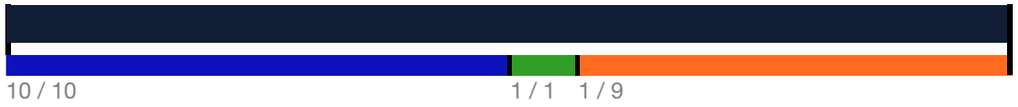
OVERALL WALLET PRIVACY

TOTAL SCORE

46 / 100

USABILITY	QUALITY	FEEDBACK
18 / 36	**13** / 35	**15** / 29

RECEIVING ADDRESS GENERATION & BACKUP



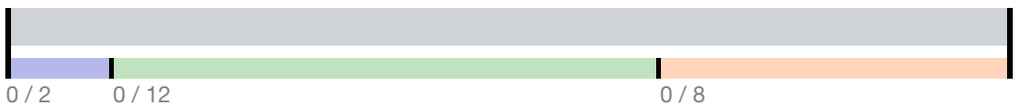
CATEGORY SCORE

21 / 21

CHANGE ADDRESS GENERATION & BACKUP

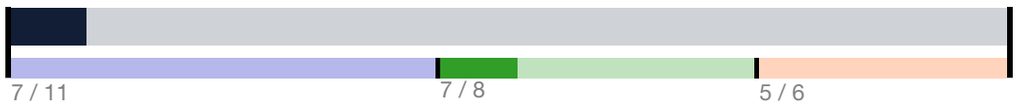
18 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS



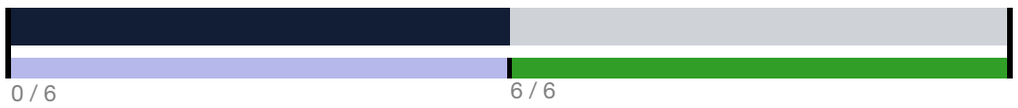
0 / 23

PRIVACY FROM NETWORK OBSERVERS



2 / 25

PRIVACY FOR TRANSACTION RECIPIENTS



6 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Bitcoin Wallet

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   Backups have been invalidated by new receiving or change address creation

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   An outgoing transaction sends funds to a previously-used address

   An outgoing transaction links inputs from multiple addresses

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   An outgoing transaction links inputs from multiple accounts/identities

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   Randomizing the position of the change output(s)

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   Intentionally creating "decoy" change outputs that have a low number of significant digits

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Any of the above with a public IP address

   Any of the above with a registered account

   Any of the above with a persistent software or hardware fingerprint

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

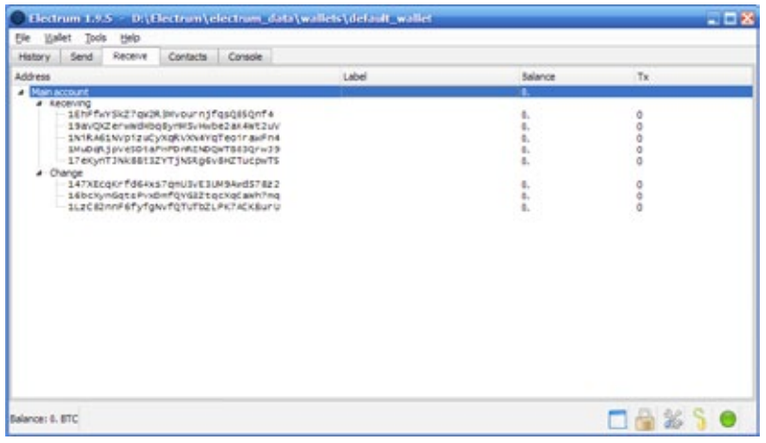
9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

**The developers of Bitcoin Wallet did not respond to the OBPP questionnaire.*

OVERALL RANK

5TH

Electrum



Version Reviewed: 2.0.3 (Linux)

Supported Platforms: Android, Linux, OSX, Windows

Electrum is a cross-platform lightweight desktop wallet that has been under active development since November 2011. This wallet uses a deterministic seed to generate all keys, backed up by a 12-word string. Electrum 2.0 now implements BIP32 for this. Instead of downloading the entire blockchain, it connects to federated Electrum servers for transaction and balance data. These connections can easily be made through Tor; Electrum is the only Bitcoin wallet to be included by default with the privacy-focused Linux distro Tails. Electrum can also do two-factor authentication, and provides compatibility with hardware wallets such as Trezor.

Because the Electrum client connects to servers for data, users sacrifice privacy and must rely on trust in the blockchain information received. Because of the networking model, Electrum servers can identify relationships between addresses through observing requests for balance information and transaction broadcasts. Electrum could be improved through the implementation of features also lacking in many other wallets, including ECDH address and mixing support, and by providing more detailed warnings to users before privacy violations take place.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE **46** / 100

USABILITY	QUALITY	FEEDBACK
23 / 36	**11** / 35	**12** / 29

RECEIVING ADDRESS GENERATION & BACKUP

CATEGORY SCORE **16** / 21

10 / 10 — 1 / 1 — 4 / 9

CHANGE ADDRESS GENERATION & BACKUP

18 / 21

7 / 7 — 4 / 7 — 6 / 6

PRIVACY FROM BLOCKCHAIN OBSERVERS

0 / 23

0 / 2 — 0 / 12 — 0 / 8

PRIVACY FROM NETWORK OBSERVERS

7 / 25

5 / 11 — 0 / 8 — 2 / 6

PRIVACY FOR TRANSACTION RECIPIENTS

6 / 11

0 / 6 — 6 / 6

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Electrum

**The developers of Electrum did not respond to the OBPP questionnaire.*

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   Backups have been invalidated by new receiving or change address creation

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   An outgoing transaction sends funds to a previously-used address

   An outgoing transaction links inputs from multiple addresses

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   An outgoing transaction links inputs from multiple accounts/identities

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   Randomizing the position of the change output(s)

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   Intentionally creating "decoy" change outputs that have a low number of significant digits

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Any of the above with a public IP address

   Any of the above with a registered account

   Any of the above with a persistent software or hardware fingerprint

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

OVERALL RANK
6TH

AirBitz

Version Reviewed: 1.4.6 (Android)

Supported Platforms: Android, iOS

The AirBitz Bitcoin Wallet, first released in early 2014, is a light client available for Android and iOS mobile devices. The mobile app features sending and receiving functionality, as well as a bitcoin merchant directory that allows users to search for nearby bitcoin-accepting businesses. Much of the Bitcoin-specific code is based on the Libbitcoin library.

AirBitz was one of the first mobile wallets to use an HD architecture, which permits it to easily protect user privacy by automatically generating new addresses for receipt of funds and change. The HD architecture also allows AirBitz more advanced support for multiple accounts than many of its competitors. Additional controls are needed for AirBitz to thoroughly protect blockchain privacy, including randomizing output indexes and mixing funds. Balance information and transaction broadcasting are conducted through one or more trusted Obelisk servers, which can lead to a degradation in privacy. Since access to privacy networks such as Tor are limited on mobile devices, AirBitz users have limited capacity to take advantage of network-based protections, and the wallet does not integrate support for such proxies.

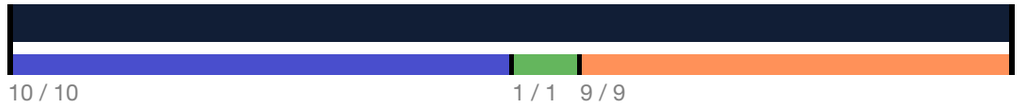
OVERALL WALLET PRIVACY

TOTAL SCORE

45 / 100

USABILITY	QUALITY	FEEDBACK
19 / 36	**9** / 35	**16** / 29

RECEIVING ADDRESS GENERATION & BACKUP



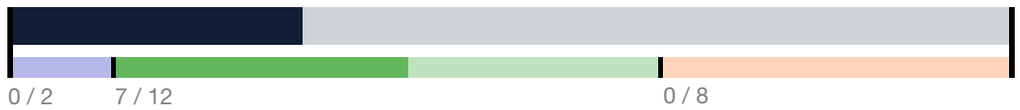
CATEGORY SCORE

21 / 21

CHANGE ADDRESS GENERATION & BACKUP

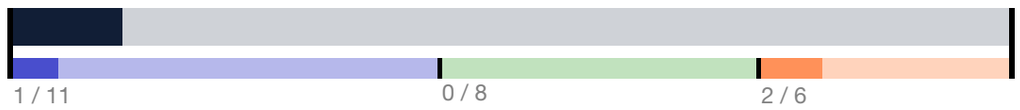
15 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS



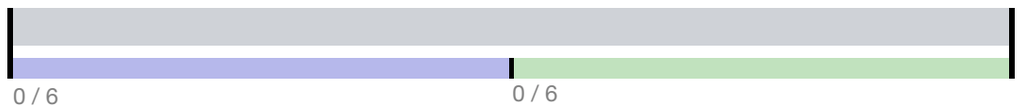
7 / 23

PRIVACY FROM NETWORK OBSERVERS



3 / 25

PRIVACY FOR TRANSACTION RECIPIENTS



0 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - AirBitz

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

   Wallet.

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   Backups have been invalidated by new receiving or change address creation

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   An outgoing transaction sends funds to a previously-used address

   An outgoing transaction links inputs from multiple addresses

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   An outgoing transaction links inputs from multiple accounts/identities

   None of the above.

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

   Not sure what is meant by this. Network observer can see transmission of fully encrypted data

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   No, but in pipeline.

   Randomizing the position of the change output(s)

   No, but in pipeline.

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   No, but in pipeline.

   Intentionally creating "decoy" change outputs that have a low number of significant digits

   No.

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

   Not applicable.

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   No.

   Any of the above with a public IP address

   Yes.

   Any of the above with a registered account

   No.

   Any of the above with a persistent software or hardware fingerprint

   No.

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

   It does not. In pipeline via prefix queries.

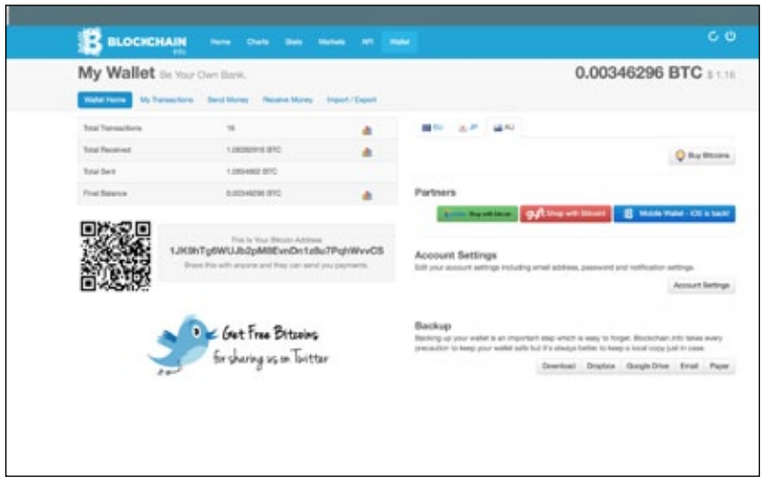
8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

   Yes, sends and receives have different paths.

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

   Accounts have no links at all to balance and incoming/outgoing transactions.

Blockchain (web)



Version Reviewed: March 2015 Production Website

Supported Platforms: Android, iOS, Web

Blockchain.info helped early adoption of Bitcoin by providing one of the first web wallets to new users. Blockchain.info also served as early advocates for users to maintain control over their own private keys, decreasing their security and privacy risk against third parties. The service maintains a large share of the Bitcoin user base, with nearly 3.4 million wallet accounts currently in existence. The service has sometimes lead in protecting user privacy, the chief example of which was the early implementation of an optional CoinJoin-based, peer-to-peer mixing service called SharedCoin.

However, Blockchain.info's web wallet has recently fallen behind competitors. Users must perform additional actions outside of the normal sending and receiving workflows to avoid simple privacy pitfalls such as address reuse. Due to the lack of an HD architecture, fixing these blockchain privacy issues is a challenge, as is simplifying the steps required for users to backup wallets completely. While it is trivial for users to connect to the web wallet via Tor using an operating system such as Tails, all balance information is obtained from the same centralized server that transactions are sent to, maintained by Blockchain.info. This can potentially protect the privacy of users of their wallet or wallet API from the larger Bitcoin network, but requires users to trust Blockchain.info with this privacy-sensitive data. The centralized server model is inherently more limited than a Bitcoin light client model that connects to other peers in the Bitcoin network.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

22 / 100

USABILITY	QUALITY	FEEDBACK
11 / 36	**10** / 35	**0** / 29

RECEIVING ADDRESS GENERATION & BACKUP

CATEGORY SCORE

8 / 21

6 / 10 — 1 / 1 — 0 / 9

CHANGE ADDRESS GENERATION & BACKUP

4 / 21

3 / 7 — 1 / 7 — 0 / 6

PRIVACY FROM BLOCKCHAIN OBSERVERS

3 / 23

1 / 2 — 1 / 12 — 0 / 8

PRIVACY FROM NETWORK OBSERVERS

2 / 25

2 / 11 — 0 / 8 — 0 / 6

PRIVACY FOR TRANSACTION RECIPIENTS

6 / 11

0 / 6 — 6 / 6

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Blockchain (Web)

1. Please classify your application as one of the three categories:

Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

Blockchain.info is a wallet. All private keys are generated by the user's machine, and we do not store any decryptable version of the keys.

2. Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:

Receiving funds to an address which has previously received incoming transactions

Not currently.

Backups have been invalidated by new receiving or change address creation

Not currently. Users can enable automatic wallet backups via email if they want the wallet to be automatically backed up each time a modification takes place, but this is disabled by default. A new version of the wallet will be released soon which will obviate the need for backups after initial setup.

If the wallet supports mixing, a proposed mixing transaction is easily reversible

The web version of our wallet includes the SharedCoin feature, which is based on the CoinJoin protocol. Though not a perfect CoinJoin implementation, this feature was made resistant to sudoku analysis in early 2015. Users are alerted to the limitations of SharedCoin before using the service here: https://sharedcoin.com/ There are no specific visual indications that vary during use of SharedCoin to indicate the degree of privacy afforded.

An outgoing transaction sends funds to a previously-used address

Not currently

An outgoing transaction links inputs from multiple addresses

Not currently. When a user performs a custom send, they have an opportunity to review the transaction before it is signed and broadcast to the network. If they click on "Advanced" in the review screen, the Blockchain.info wallet will list all of the inputs that will be included in the transaction, whether they have been selected manually by the user or automatically selected by the application to constitute the desired amount of funds. However, the user interface does not explicitly warn the user about the privacy consequences of merging inputs.

Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

Our wallet does not currently provide any warning to users concerning their connection to the website through an anonymous channel, such as Tor.

An outgoing transaction links inputs from multiple accounts/identities

Our current wallet does not support accounts or identities.

3. Does your application's backup process involve any activity which may be visible to an external network observer?

We do not currently perform any automatic backups of wallets. Upon account creation, users are instructed to backup their mnemonic, which encodes their wallet identifier and password. No wallet backup requires automatically, aside from caching in the browser of the encrypted wallet payload. We provide a number of ways to manually backup wallets, some of which can be visible to an external network observer (see chart below):

Backup Option	*Visible to external network observer?*
Browser caching	*No*
Download	*No, using JavaScript the wallet data is turned into a "blob" and the user is presented with a download dialogue for wallet.aes.json.*
Dropbox	*Yes. Users will connect to DropBox to authenticate with the OAuth API. Wallet identifiers are not disclosed in URLs, and all communications with DropBox are encrypted with SSL/TLS.*
Google Drive	*Yes. Users will connect to Google Drive to authenticate with the OAuth API. Wallet identifiers are not disclosed in URLs, and all communications with DropBox are encrypted with SSL/TLS.*
Email	*Yes. Email is not encrypted. The email will be sent to the address that the user configures for their wallet account.*
Paper	*No, uses data: uri.*

All forms of wallet backup are AES encrypted so that the user's wallet identifier is not in plaintext in the backup file, and the user's password is required to decrypt the backup file.

4. Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:

Randomizing the number of change outputs

No, our wallet currently only generates a single change output

Randomizing the position of the change output(s)

When using Custom Send to a single recipient and a single change address, the change address is always listed second in the transaction and not randomized. When using SharedCoin, all inputs and outputs are randomly shuffled by the SharedCoin server, and so change outputs are necessarily randomized:

https://github.com/blockchain/Sharedcoin/blob/master/website/src/piuk/website/SharedCoin.java#L1979

Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

No, our wallet does not currently try to match change outputs with the size of a desired spend.

Intentionally creating "decoy" change outputs that have a low number of significant digits

No, our wallet does not create decoy change outputs.

5. If your application includes mixing functionality:

Is it possible for a malicious participant in the mix to steal funds?

No. All private keys are held by the users in browser and cannot be stolen by the server. Participants are unable to steal each other's mixing funds due to the properties of the CoinJoin protocol that SharedCoin is based on.

Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

Mixing peers only retain information about their own inputs and outputs. The SharedCoin server has visibility over all inputs and outputs, and which peers they belong to. Future versions of SharedCoin may be cryptographically "blinded" to this information.

6. If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:

A user's receiving or change address to another receiving or change address in the same wallet

All transactions are pushed through a single server. The server would be able to identify recurring addresses between several transactions. We avoid logging such data as much as possible.

Any of the above with a public IP address

Our web server is required by design to see the user's IP address. We avoid logging such data as much as possible, except for authorization purposes (See response to software fingerprinting below). We maintain an .onion address for Tor users who wish to keep their accounts dissociated from their public IP addresses.

Any of the above with a registered account

Lookups of the balance information for specific addresses come through the same server as the one used for logging into accounts. We avoid logging such data as much as possible.

Any of the above with a persistent software or hardware fingerprint

Our web wallet server is capable of identifying browser fingerprints unless users take steps to randomize or standardize their fingerprint. We avoid logging such data as much as possible, though some fingerprint information is collected in order to prompt users for email authorization when they attempt to download their encrypted wallet file (login) on a new machine.

7. If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?

Our wallet does not connect directly to network peers.

8. Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?

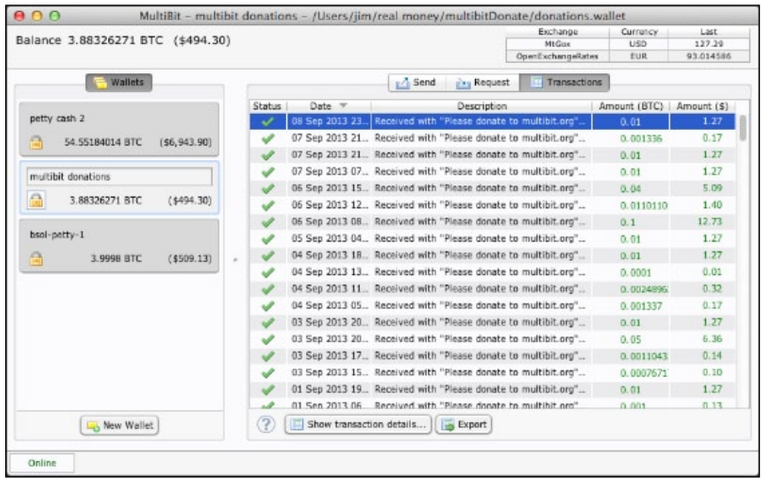
No, all data is sent through the same server.

9. If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?

Our wallet does not currently support accounts or identities.

OVERALL RANK
8TH

Multibit Classic



Version Reviewed: 0.5.18 (Linux)

Supported Platforms: Linux, OSX, Windows

Multibit is an open-source, light client Bitcoin wallet written in Java for execution on desktop and laptop computers. The Java architecture of the code allows for it to be easily ported to Windows, OS X, and Linux. The Classic edition of the wallet was first announced as a project in late 2011. Multibit Classic has been a popular desktop client that competes with Electrum as light client alternatives to the reference full node Bitcoin Core wallet, sparing users from downloading the entire Bitcoin blockchain.

Balance information is obtained from peers on the Bitcoin network through an SPV extension to the Bitcoin protocol using Bloom filters. In recent years, development focus has shifted from Multibit Classic to an HD reboot of the software that is currently in beta testing. The Classic edition of the application lacks basic controls to protect user privacy on the blockchain. Private keys are generated and held in a key pool, making backups more complicated and incentivizing address reuse. Multibit relies on weak privacy guarantees when obtaining balance information and broadcasting transactions. The software provides primitive support for maintaining multiple financial identities by allowing the user to load multiple wallet files simultaneously and quickly switch between them.

OVERALL WALLET PRIVACY

0 — 100

USABILITY **7** / 36

QUALITY **10** / 35

FEEDBACK **2** / 29

TOTAL SCORE

19 / 100

RECEIVING ADDRESS GENERATION & BACKUP

4 / 10 — 1 / 1 — 0 / 9

CATEGORY SCORE

5 / 21

CHANGE ADDRESS GENERATION & BACKUP

2 / 7 — 1 / 7 — 0 / 6

4 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS

0 / 2 — 0 / 12 — 0 / 8

0 / 23

PRIVACY FROM NETWORK OBSERVERS

1 / 11 — 2 / 8 — 2 / 6

5 / 25

PRIVACY FOR TRANSACTION RECIPIENTS

0 / 6 — 6 / 6

6 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Multibit Classic

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

   Wallet. All private keys are under exclusive control of the user.

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   Backups have been invalidated by new receiving or change address creation

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   An outgoing transaction sends funds to a previously-used address

   An outgoing transaction links inputs from multiple addresses

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   An outgoing transaction links inputs from multiple accounts/identities

   No.

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

   No - backups are performed by the user.

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   Randomizing the position of the change output(s)

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   Intentionally creating "decoy" change outputs that have a low number of significant digits

   No.

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

   There is no mixing in MultiBit Classic.

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Any of the above with a public IP address

   Any of the above with a registered account

   Any of the above with a persistent software or hardware fingerprint

   MultiBit Classic does not obtain balance info from other servers. It gets (bloom-filtered) tx information from Bitcoin Core nodes.

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

   The bloom filters used by MultiBit (and other bitcoinj based wallets) are susceptible to reverse engineering if an attacker can monitor all the user's network traffic unfortunately.

8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

   It broadcasts on one Bitcoin Core node and listens on others yes.

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

   MultiBit Classic does not support multiple identities.

Blockchain (Android)

Version Reviewed: 4.0.20 (Android)

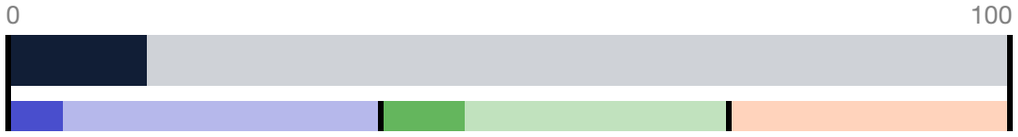
Supported Platforms: Android, iOS, Web

As an offshoot of the Blockchain.info web wallet, the company was also quick amongst competitors to produce companion mobile versions of their wallet service. The Open Bitcoin Privacy Project considered ratings for both the android and web wallets provided by Blockchain.info, as they differ substantially in their functionality.

Like the Blockchain.info web wallet, users must click through additional steps to achieve basic blockchain privacy protections such as avoiding address reuse. The SharedCoin service that makes it possible for web wallet users to bolster their blockchain privacy is unfortunately not available in Blockchain.info's mobile wallets. Because the wallet's private keys are not determined deterministically from a seed, backups can become invalided quickly when a user opts to generate a new receiving or change address. So long as Blockchain.info continues to provide service to a given customer, however, she can recover funds from a single wallet mnemonic passphrase provided to her when she creates the account.

Blockchain.info's Android wallet relies on trusted servers to obtain balance information and broadcast new transactions to the Bitcoin network. Limiting this privacy degradation with anonymity networks such as Tor is difficult on an Android device, and requires preparations such as rooting the device and configuring traffic to route through an Orbot proxy.

OVERALL WALLET PRIVACY

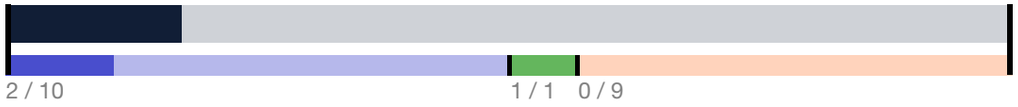


TOTAL SCORE

14 / 100

USABILITY	QUALITY	FEEDBACK
6 / 36	**8** / 35	**0** / 29

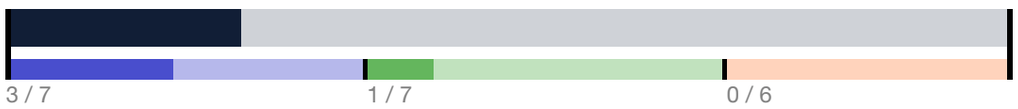
RECEIVING ADDRESS GENERATION & BACKUP



CATEGORY SCORE

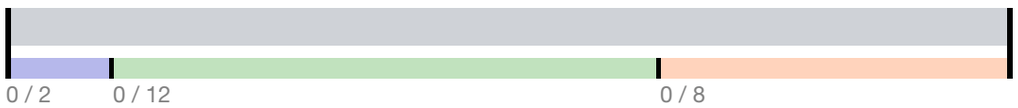
4 / 21

CHANGE ADDRESS GENERATION & BACKUP



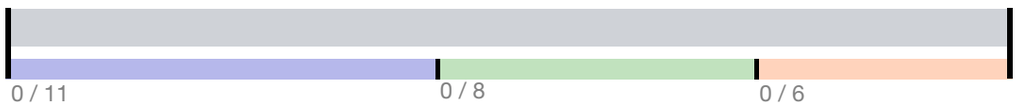
5 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS



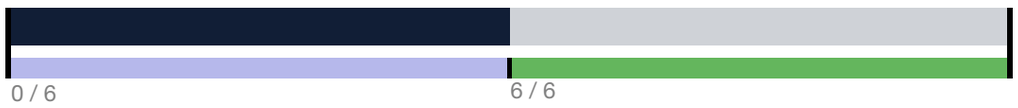
0 / 23

PRIVACY FROM NETWORK OBSERVERS



0 / 25

PRIVACY FOR TRANSACTION RECIPIENTS



6 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Blockchain (Android)

1. Please classify your application as one of the three categories:

Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

Blockchain.info is a wallet. All private keys are generated by the user's machine, and we do not store any decryptable version of the keys.

2. Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:

Receiving funds to an address which has previously received incoming transactions

Not currently.

Backups have been invalidated by new receiving or change address creation

Not currently. Users can enable automatic wallet backups via email if they want the wallet to be automatically backed up each time a modification takes place, but this is disabled by default. A new version of the wallet will be released soon which will obviate the need for backups after initial setup.

If the wallet supports mixing, a proposed mixing transaction is easily reversible

The web version of our wallet includes the SharedCoin feature, which is based on the CoinJoin protocol. Though not a perfect CoinJoin implementation, this feature was made resistant to sudoku analysis in early 2015. Users are alerted to the limitations of SharedCoin before using the service here: https://sharedcoin.com/ There are no specific visual indications that vary during use of SharedCoin to indicate the degree of privacy afforded.

An outgoing transaction sends funds to a previously-used address

Not currently

An outgoing transaction links inputs from multiple addresses

Not currently. When a user performs a custom send, they have an opportunity to review the transaction before it is signed and broadcast to the network. If they click on "Advanced" in the review screen, the Blockchain.info wallet will list all of the inputs that will be included in the transaction, whether they have been selected manually by the user or automatically selected by the application to constitute the desired amount of funds. However, the user interface does not explicitly warn the user about the privacy consequences of merging inputs.

Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

Our wallet does not currently provide any warning to users concerning their connection to the website through an anonymous channel, such as Tor.

An outgoing transaction links inputs from multiple accounts/identities

Our current wallet does not support accounts or identities.

3. Does your application's backup process involve any activity which may be visible to an external network observer?

We do not currently perform any automatic backups of wallets. Upon account creation, users are instructed to backup their mnemonic, which encodes their wallet identifier and password. No wallet backup requires automatically, aside from caching in the browser of the encrypted wallet payload. We provide a number of ways to manually backup wallets, some of which can be visible to an external network observer (see chart below):

Backup Option	*Visible to external network observer?*
Browser caching	*No*
Download	*No, using JavaScript the wallet data is turned into a "blob" and the user is presented with a download dialogue for wallet.aes.json.*
Dropbox	*Yes. Users will connect to Dropbox to authenticate with the OAuth API. Wallet identifiers are not disclosed in URLs, and all communications with Dropbox are encrypted with SSL/TLS.*
Google Drive	*Yes. Users will connect to Google Drive to authenticate with the OAuth API. Wallet identifiers are not disclosed in URLs, and all communications with DropBox are encrypted with SSL/TLS.*
Email	*Yes. Email is not encrypted. The email will be sent to the address that the user configures for their wallet account.*
Paper	*No, uses data: uri.*

All forms of wallet backup are AES encrypted so that the user's wallet identifier is not in plaintext in the backup file, and the user's password is required to decrypt the backup file.

4. Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:

Randomizing the number of change outputs

No, our wallet currently only generates a single change output

Randomizing the position of the change output(s)

When using Custom Send to a single recipient and a single change address, the change address is always listed second in the transaction and not randomized. When using SharedCoin, all inputs and outputs are randomly shuffled by the SharedCoin server, and so change outputs are necessarily randomized:

https://github.com/blockchain/Sharedcoin/blob/master/website/src/piuk/website/SharedCoin.java#L1979

Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

No, our wallet does not currently try to match change outputs with the size of a desired spend.

Intentionally creating "decoy" change outputs that have a low number of significant digits

No, our wallet does not create decoy change outputs.

5. If your application includes mixing functionality:

Is it possible for a malicious participant in the mix to steal funds?

No. All private keys are held by the users in browser and cannot be stolen by the server. Participants are unable to steal each other's mixing funds due to the properties of the CoinJoin protocol that SharedCoin is based on.

Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

Mixing peers only retain information about their own inputs and outputs. The SharedCoin server has visibility over all inputs and outputs, and which peers they belong to. Future versions of SharedCoin may be cryptographically "blinded" to this information.

6. If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:

A user's receiving or change address to another receiving or change address in the same wallet

All transactions are pushed through a single server. The server would be able to identify recurring addresses between several transactions. We avoid logging such data as much as possible.

Any of the above with a public IP address

Our web server is required by design to see the user's IP address. We avoid logging such data as much as possible, except for authorization purposes (See response to software fingerprinting below). We maintain an .onion address for Tor users who wish to keep their accounts dissociated from their public IP addresses.

Any of the above with a registered account

Lookups of the balance information for specific addresses come through the same server as the one used for logging into accounts. We avoid logging such data as much as possible.

Any of the above with a persistent software or hardware fingerprint

Our web wallet server is capable of identifying browser fingerprints unless users take steps to randomize or standardize their fingerprint. We avoid logging such data as much as possible, though some fingerprint information is collected in order to prompt users for email authorization when they attempt to download their encrypted wallet file (login) on a new machine.

7. If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?

Our wallet does not connect directly to network peers.

8. Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?

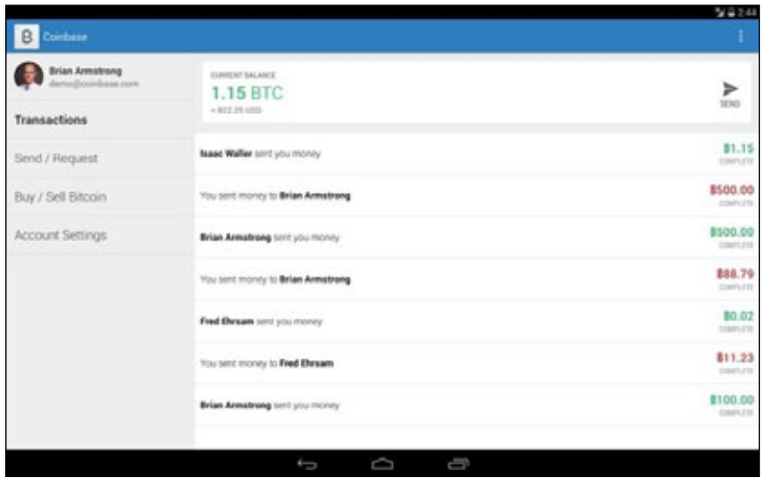
No, all data is sent through the same server.

9. If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?

Our wallet does not currently support accounts or identities.

Coinbase

OVERALL RANK
10TH



Version Reviewed: March 2015 Production Website

Supported Platforms: Android, Web

Coinbase is a prominent company in the Bitcoin space that provides Bitcoin exchange, payment processor, and wallet services on the web. Their wallet can be subdivided into two components: a classic version, and Coinbase Vault. Both versions of their wallet functionality are pseudo-wallets in that Coinbase acts as a custodian of private keys, with the exception that Coinbase Vault allows users to retain some of the signing keys required for a transaction. For this assessment of Coinbase, we focused on the class version of the wallet functionality.

Because of the custodial nature of Coinbase's wallet, users are afforded low privacy. Private keys are generated and held server-side, and the service retains detailed information about incoming and outgoing transactions. Customers must undergo a stringent identification process in order to use the service. The wallet generates new Bitcoin addresses for change, but employs few other basic controls to protect privacy on the blockchain. There are a number of basic improvements that can be made to the classic Coinbase wallet to protect customer privacy without violating Know-Your-Customer guidelines, including discouraging address reuse and randomizing output indexes on the blockchain. In the future, Coinbase can also provide better feedback to users about actions that will degrade their privacy, such as merging inputs when sending bitcoins from their Coinbase wallet.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

11 / 100

USABILITY	QUALITY	FEEDBACK
8 / 36	**0** / 35	**3** / 29

RECEIVING ADDRESS GENERATION & BACKUP

2 / 10 — 0 / 1 — 0 / 9

CATEGORY SCORE

2 / 21

CHANGE ADDRESS GENERATION & BACKUP

6 / 7 — 0 / 7 — 3 / 6

9 / 21

PRIVACY FROM BLOCKCHAIN OBSERVERS

0 / 2 — 0 / 12 — 0 / 8

0 / 23

PRIVACY FROM NETWORK OBSERVERS

0 / 11 — 0 / 8 — 0 / 6

0 / 25

PRIVACY FOR TRANSACTION RECIPIENTS

0 / 6 — 0 / 6

0 / 11

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Questionnaire Response - Coinbase

1. **Please classify your application as one of the three categories:**

   Wallet: All of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Pseudo-wallet: None of the private keys needed to create a blockchain transaction are under the exclusive control of the user
   Hybrid wallet: Some portion of the private keys needed to create a blockchain transaction are under the exclusive control of the user

2. **Does your application provide any type of visual warning to the user when events which may reduce their privacy or safety occur, such as:**

   Receiving funds to an address which has previously received incoming transactions

   Backups have been invalidated by new receiving or change address creation

   If the wallet supports mixing, a proposed mixing transaction is easily reversible

   An outgoing transaction sends funds to a previously-used address

   An outgoing transaction links inputs from multiple addresses

   Network connectivity to peers or dedicated balance servers is not routed through an anonymous channel

   An outgoing transaction links inputs from multiple accounts/identities

3. **Does your application's backup process involve any activity which may be visible to an external network observer?**

4. **Does your application take positive steps to make change outputs indistinguishable from spending outputs, such as:**

   Randomizing the number of change outputs

   Randomizing the position of the change output(s)

   Selecting sufficient input value such that the change output(s) closely resemble the size of the desired spend

   Intentionally creating "decoy" change outputs that have a low number of significant digits

5. **If your application includes mixing functionality:**

   Is it possible for a malicious participant in the mix to steal funds?

   Is it possible for any participant in the mix to retain information which correlates outputs to their corresponding inputs?

6. **If your application obtains balance information from dedicated servers, is it possible to operate the dedicated servers in a manner which correlates:**

   A user's receiving or change address to another receiving or change address in the same wallet

   Any of the above with a public IP address

   Any of the above with a registered account

   Any of the above with a persistent software or hardware fingerprint

7. **If your application obtains balance information by uploading a filter to network peers, are filters ever updated in a manner that allows the peer to correlate the old and new filter with the same connection?**

8. **Does your application take positive steps to route outgoing transactions through different path to the network than the path via which it receives balance and incoming transaction information?**

9. **If your application supports multiple accounts/identities, does your application take positive steps to route balance, incoming and outgoing transaction information through different network paths for each account/identity?**

Coinbase declined to answer the questionnaire.

Appendix A - Privacy Threat Model

The following threat model was used to develop criteria for measuring the privacy strength of Bitcoin wallets.

Attackers	Attack	Counter Measure	Relevant Tests
Blockchain Observer	Link transactions to a single entity based on all of them containing inputs with a common address	Avoid address reuse	I.A.1, I.A.2, I.A.3, I.B.1, II.A.1, II.A.5, III.B.1, IV.A.1
		Randomize the position of the change output(s) in the output list	II.A.2
	Link outputs in a transaction to a single entity by detecting which output is a change output	Select inputs such that the amount of change in the transaction is close to the size of the desired spend	II.A.3
		Use multiple change outputs, and intentionally set the value of some outputs to values that resemble plausible spends	II.A.4
	Link outputs to a single entity based on them all being included as inputs in the same transaction	Avoid using inputs from different addresses in the same transaction	III.C.2
		Use mixing when sending transactions, and make non-mixed transactions resemble mixed transactions	III.A.1, III.A.2, III.A.5, III.C.1
Network Peer	Link identities by observing that addresses associated with both identities are used as inputs in the same transaction	Avoid constructing transactions that contain inputs from more than one identity/account	IV.C.5
	Temporally link transactions to a known IP address via side channel attacks based on wallet behavior	Avoid leaking information about user behavior via observable network traffic	I.B.2
		Avoid leaking information about recipients in transaction via an external network lookup	V.B.1
	Link addresses to a user by observing their backup files	Use strictly local wallet backups, or encrypt remote wallet backups	II.B.2
	Link addresses belonging to a single user by observing the pattern of their balance lookup requests (bloom/prefix filters or direct query)	Connect to the source of balance information in a manner that does not leak the IP address of the requestor	IV.A.1, IV.A.5
	Reduce the false positive rate of filters by comparing how the filters received from a single client change over time	If a filter requires an update, send the new filter to a different peer than the peer which has the old filter	IV.A.2
	Reduce the false positive rate of filters by comparing the transactions sent by a client with the filter they have sent	Route outgoing transactions through a different route than through the peer which is providing balance information	IV.B.2
	Link addresses to an IP address by observing the inputs of outgoing transactions sent by a client	Route outgoing transactions via a method that does not reveal the IP address of the sender	IV.B.1, IV.B.3
	Link different identities based on a bloom/prefix filter that matches addresses associated with multiple identities	Use separate filters, provided to different peers, for each identity	IV.C.3
	Link different identities by observing that the same IP address is sending outgoing transactions associated with multiple identities	Use separate routes for outgoing transactions associated with each identity	IV.C.4
Transaction Participant	Collude with other transaction participants to infer a bitcoin user's behavior based on the flow of funds from one colluding entity, to the targeted user, to another colluding entity	Use multiple identities/accounts to allow funds associated with one transaction participant to be kept apart from funds associated with a different transaction participant	III.D.1, IV.C.1, IV.C.2
	Defeat attempts by users to mix their coins by participating in mixing transactions and collecting information which can be used to map inputs to outputs in the mixing transaction.	Use mixing protocols which are secure against misbehavior by any participant	III.A.3
Meta Attack	Concern that wallet backups may become unexpectedly invalid may give users an incentive to reuse addresses due to fear of losing funds	Use eternal backups	I.B.3, II.B.1, II.B.3
		Proactively inform users when backups require an update	I.B.3, II.B.1, II.B.3
	Concern that mixing services can steal funds may give users an incentive to avoid mixing	Use mixing methods that do not allow for theft of funds	III.A.4
	Overhead involved with communicating unique deposit addresses to senders may give users an incentive to reuse one address	Use deposit addresses derived from a constant seed using ECDH (e.g. stealth addresses)	V.A.1
	The difficulty of setting up Tor on different operating systems may be a barrier to using wallet privacy features	Create wallets that are easily usable on operating systems with built-in Tor support	IV.D.1

Appendix B - Detailed Scoring Data

	Test Description	Classification	Potential Score	Airbitz	Armory	Bitcoin Wallet	Blockchain (Android)	Blockchain (Web)	Coinbase	Darkwallet	Electrum	Multibit Classic	Mycelium
	Receiving Address Generation & Backup												
	Generation												
I.A.1	*Number of clicks required to deviate from the default receiving functionality and generate a new receiving address for an existing wallet*	Usability	8.89	8.89	8.89	8.89	1.76	5.60	2.22	8.89	8.89	3.53	8.89
I.A.2	*Receiving addresses are hidden from the default view once they have been used*	Feedback	3.11	3.11	-	3.11	-	-	-	3.11	3.11	-	3.11
I.A.3	*Preemptively indicates a loss of privacy when user elects to receive funds at a previously-used addresses*	Feedback	4.67	4.67	-	4.67	-	-	-	-	-	-	-
	Backup												
I.B.1	*Number of clicks to backup a newly-generated receiving address from an existing wallet (worst case), from the default window/authenticated home page*	Usability	1.39	1.39	1.39	1.39	0.44	0.69	-	1.39	1.39	0.35	1.39
I.B.2	*The backup process leaks information about wallet addresses (e.g. each time a new change address is created on-demand, an email backup is triggered immediately)*	Quality	1.39	1.39	1.39	1.39	1.39	1.39	-	1.39	1.39	1.39	1.39
I.B.3	*Indicates a reduction in wallet safety when receiving address backups are stale, or uses eternal backups*	Feedback	1.11	1.11	1.11	1.11	-	-	-	1.11	1.11	-	1.11
	Change Address Generation & Backup												
	Generation												
II.A.1	*Number of clicks required to deviate from the default change functionality and receive change at a newly generated address*	Usability	5.95	5.95	5.95	5.95	2.98	2.36	5.95	5.95	5.95	1.88	5.95
II.A.2	*The position of the change output(s) in the transaction is random*	Quality	2.98	-	-	2.98	-	-	-	2.98	2.98	-	2.98
II.A.3	*One or more change outputs are created which are close to the value of the desired spend*	Quality	1.98	-	-	-	-	-	-	-	-	-	-
II.A.4	*Some change output values are intentionally set to "round numbers" (a.k.a low number of significant digits)*	Quality	0.99	-	-	-	-	-	-	-	-	-	-
II.A.5	*Change addresses are hidden from the normal receiving workflow by default to discourage using them as receiving addresses*	Feedback	1.90	1.91	-	1.91	-	-	-	1.91	1.91	-	1.91
II.A.6	*Preemptively indicates a loss of privacy when user elects to reuse change addresses as receiving addresses*	Feedback	2.86	2.86	-	2.86	-	-	2.86	-	2.86	-	-
	Backup												
II.B.1	*Number of clicks to backup a newly-generated change address from an existing wallet (worst case), apart from the sending workflow*	Usability	1.39	1.39	1.39	1.39	0.44	0.55	-	1.39	1.39	0.44	1.39
II.B.2	*Backups can occur offline, or are encrypted client-side with data that only the user controls e.g. password*	Quality	1.39	1.39	1.39	1.39	1.39	1.39	-	1.39	1.39	1.39	1.39
II.B.3	*Indicates a reduction in wallet safety when change address backups are stale, or uses eternal backups*	Feedback	1.11	1.11	1.11	1.11	-	-	-	1.11	1.11	-	1.11
	Privacy from Blockchain Observers												
	Mixing												
III.A.1	*Number of clicks required by user for inputs/outputs to be mixed with one or more other users*	Usability	2.38	-	-	-	-	1.19	-	2.38	-	-	-
III.A.2	*Average number of other users whose funds are mixed with yours when sending through a mixing process*	Quality	0.79	-	-	-	-	0.65	-	0.08	-	-	-
III.A.3	*Mixing is secure against correlation attacks by the facilitator*	Quality	0.79	-	-	-	-	-	-	-	-	-	-
III.A.4	*Mixing is secure against theft of funds*	Quality	0.79	-	-	-	-	0.79	-	0.79	-	-	-
III.A.5	*Warns the user when a proposed mix is easy to reverse*	Feedback	1.90	-	-	-	-	-	-	-	-	-	-
	Address Reuse												
III.B.1	*Warns user when sending to an address that the user has sent to before*	Feedback	3.89	-	-	-	-	-	-	-	-	-	-
	Input Merging												
III.C.1	*When an outgoing transaction must merge inputs, and when mixing is not being used, is the transaction constructed in a way that plausibly resembles a mixing transaction*	Quality	3.33	-	-	-	-	-	-	-	-	-	-
III.C.2	*Outside of a mixing transaction, preemptively indicates a loss of privacy when merging inputs from different addresses in the same transaction*	Feedback	2.22	-	-	-	-	-	-	-	-	-	-
	Identity Separation												
III.D.1	*Avoids creating transactions which contain inputs from different identity containers, except optionally if the user has intentionally overridden this behavior*	Quality	6.67	6.67	6.67	-	-	-	-	6.67	-	-	6.67

Appendix B - Detailed Scoring Data (continued)

	Test Description	Classification	Potential Score	AirBitz	Armory	Bitcoin Wallet	Blockchain (Android)	Blockchain (Web)	Coinbase	Darkwallet	Electrum	Multibit Classic	Mycelium
	Privacy from Network Observers												
	Balance Information												
IV.A.1	*Number of clicks required by user to connect to the source of balance information without leaking their identity over the network*	Usability	3.97	-	3.97	-	-	-	-	-	0.99	-	1.58
IV.A.2	*Balance information is obtained in a manner which avoids leaking the addresses in a wallet to network peers*	Quality	3.97	-	3.97	1.98	-	-	-	-	-	1.98	-
IV.A.3	*Client provides a visual indication if the balance information is not being obtained through an anonymizing network, including IP address information*	Feedback	3.17	-	3.18	-	-	-	-	-	-	-	-
	Outgoing Transactions												
IV.B.1	*Number of clicks required by user to route outgoing transactions through an anonymizing network*	Usability	1.98	-	0.20	-	-	-	-	0.63	0.50	-	0.79
IV.B.2	*Are outgoing transactions routed through a different entry point into the network than the source of balance information*	Quality	1.98	-	1.98	-	-	-	-	-	-	-	-
IV.B.3	*Client provides a visual indication if outgoing transactions are not being routed through an anonymizing network, including IP address information*	Feedback	1.59	-	-	-	-	-	-	-	-	-	1.59
	Identity Separation												
IV.C.1	*Number of clicks to create a new identity container*	Usability	1.32	0.83	0.33	-	-	-	-	0.42	0.13	0.53	0.66
IV.C.2	*Number of clicks to assign an imported address to an identity container*	Usability	0.66	0.42	0.66	-	-	-	-	-	0.66	0.66	0.66
IV.C.3	*Avoids including addresses from multiple identity containers in the same address filter*	Quality	0.99	-	0.99	-	-	-	-	-	-	-	-
IV.C.4	*Avoids broadcasting outgoing transactions from different identity containers via the same network access path*	Quality	0.99	-	-	-	-	-	-	-	-	-	-
IV.C.5	*Visually indicates to user when inputs from different accounts/pockets are merged before the transaction is broadcast, or prohibits this operation entirely*	Feedback	1.59	1.59	1.59	-	-	-	-	1.59	1.59	1.59	1.59
	Operating System Support												
IV.D.1	*Compatible with latest version of Tails*	Usability	2.78	-	2.08	-	-	2.08	-	-	2.78	-	-
	Privacy for Transaction Recipients												
	ECDH Address Support												
V.A.1	*Number of clicks required by user to generate a ECDH receiving address, from the default window/authenticated home page*	Usability	5.56	-	-	-	-	-	-	5.56	-	-	-
	Receiver Identity												
V.A.1	*Wallet avoids leaking information about recipients via an external identity lookup*	Quality	5.56	-	5.56	5.56	5.56	5.56	-	5.56	5.56	5.56	5.56

open bitcoin
privacy project

The Open Bitcoin Privacy Project is an open source, global organization whose mission is to improve financial privacy within the Bitcoin ecosystem. This wallet ratings report is part of our ongoing efforts to educate the public and provide transparency to consumers about their options.

You can follow us on Twitter @obpp_org. You can also visit our website, www.openbitcoinprivacyproject.org to join our mailing list and find out more about our projects.

Data for this report, as well as information related to our other projects can be found at our Github repository: www.github.com/OpenBitcoinPrivacyProject

CONTRIBUTORS

The Open Bitcoin Privacy Project wants to thank everyone who contributed in various ways to make this report possible.

The following individuals participated in the creation of the threat model and associated criteria for the 2015-1 rating exercise:

Chris Pacia
Justus Ranvier
Kristov Atlas
Samuel Patterson

The following individuals participated in the wallet rating process:

Daniel Krawisz
Justus Ranvier
Kristov Atlas
Michael Goldstein

The following individuals provided feedback and suggestions about the initial drafts of our criteria:

Sergio Demian Lerner
Olivier Lalonde
Eric Voskuil
LareuntMT
Whit J
Alon Muroch

Special thanks to BTC Design for the graphic design and production work on this report.