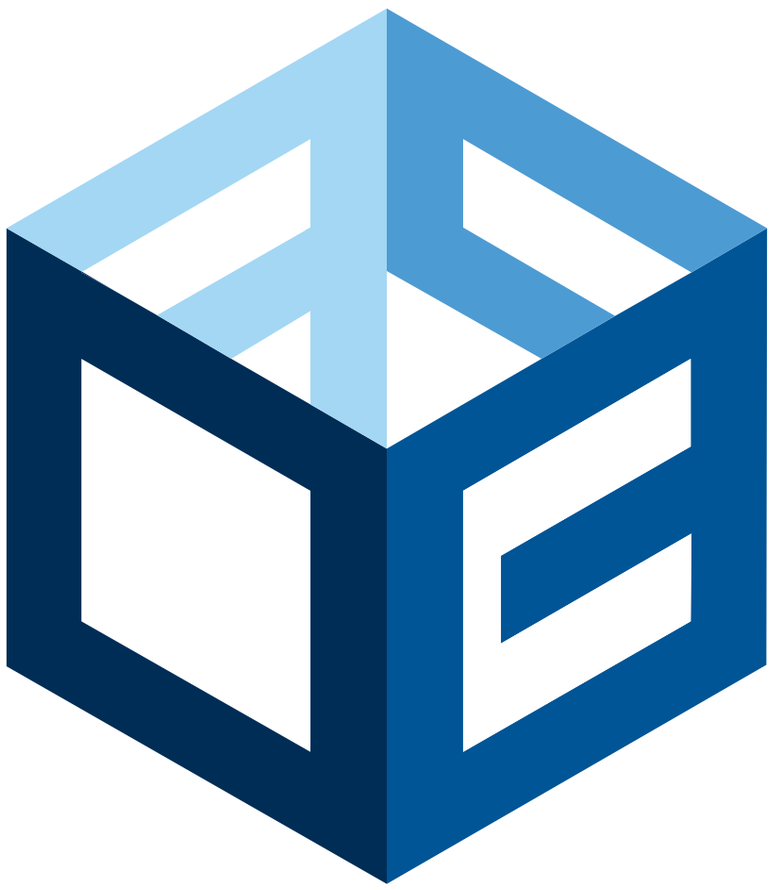


open bitcoin privacy project

Bitcoin Wallet Privacy Rating Report

2nd Edition, March 2016

Table of Contents

Introduction

Since our first report surveying user privacy in Bitcoin wallets, not much has changed for wallet providers. Thankfully, we're seeing newcomers consistently adopt an HD architecture to help users avoid address reuse, but many of the big privacy pushes during 2014 -- such as "stealth" addresses and Tor support -- stalled out during 2015. Wallets seem to be mostly in a holding pattern, waiting for their competitors to take the lead on innovating.

Improvements are desperately needed to keep Bitcoin independent and safe. If you're like me, and you want to see more progress in this area in 2016, it's time to vote with your wallet. Let companies know that you care about privacy, and choose the wallets that respond to this demand.

Although the wallets haven't changed much, the Open Bitcoin Privacy Project has made a lot of improvements to our privacy analysis. Our threat model has matured to take a more systematic approach, considering the many ways that privacy attackers can work, and the corresponding countermeasures that wallet providers can employ to protect their users. We've nearly doubled the number of criteria we look at for each wallet from thirty-eight points to sixty-eight. Also, due to popular demand for more wallets, this edition includes a total of twenty wallet clients, doubled from ten. That's a 250% increase in the amount of data that we've collected this report, made possible thanks to the many volunteers who helped rate wallets.

All wallets were rated by at least two professionally unaffiliated volunteers with cross-checking for consensus to mitigate bias. Along with information solicited from wallet providers, these ratings represent the accumulation of over two thousand data points! ...and we have the spreadsheets to prove it. At the end of this report you'll find acknowledgements for the individuals and companies who generously donated their time and energy to produce the report, as well as instructions on how you can donate bitcoin to the organization; all proceeds go toward the costs of producing the reports and future Bitcoin privacy projects.

We'll be blogging about our findings to paint a clearer picture of the data in the coming weeks following this report's release. However, if you have questions about the details, you can find all of our source data on GitHub. We're always looking for volunteers -- amateur enthusiasts, highly skilled coders, and everywhere between -- so give us a shout if you can help out.

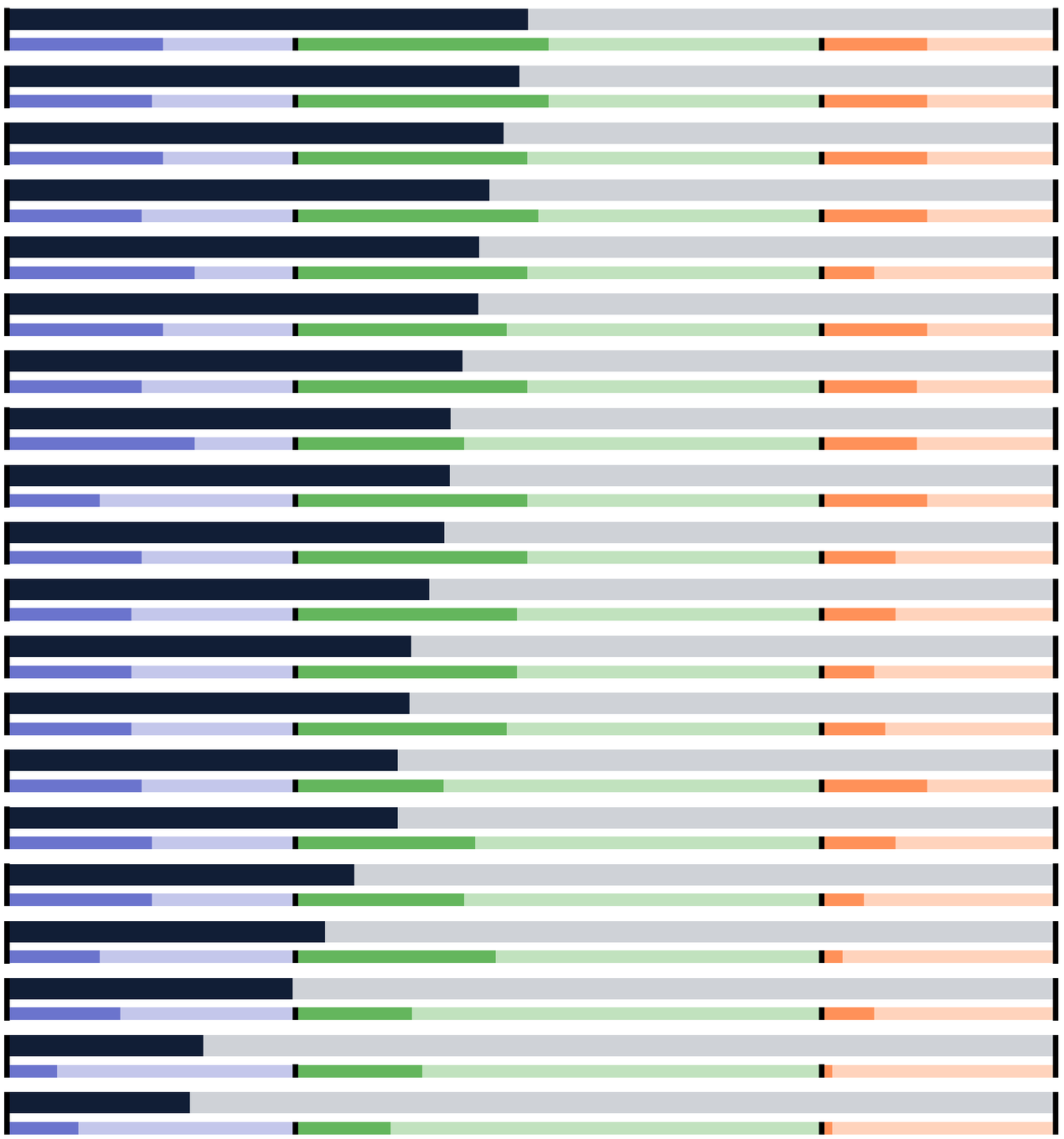
It's been just a little over seven years since the first Bitcoin block was mined. Here's to seven years of the censorship-resistant Bitcoin blockchain, and to many more.

Sincerely,

Kristov Atlas
OBPP Contributor

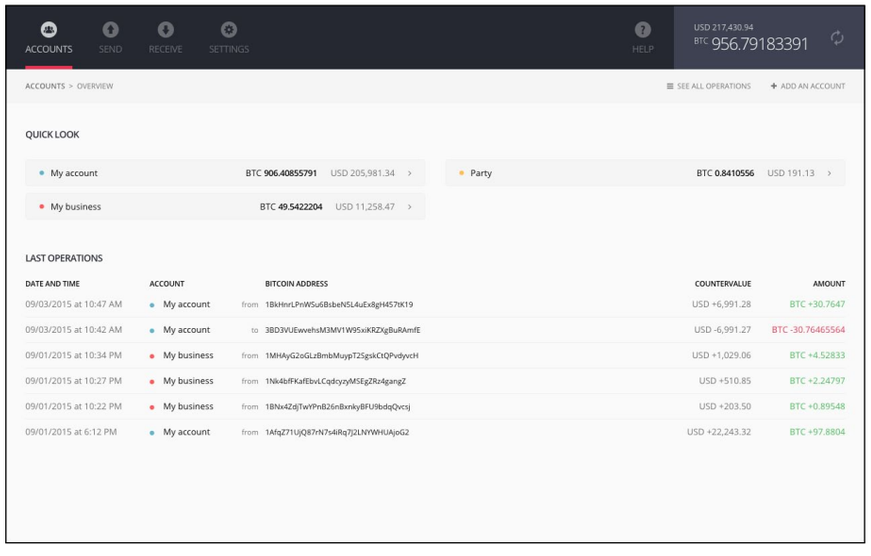
Wallet Privacy Rankings

1.	Ledger	50
2.	Breadwallet	49
3.	Airbitz	47
4.	Bitcoin-Qt	46
5.	Darkwallet	45
6.	ArcBit	45
7.	Samourai	43
8.	Trezor	42
9.	LUXSTACK	42
10.	Bitcoin Wallet	42
11.	MultiBit HD	40
12.	GreenAddress	39
13.	Armory	38
14.	Copay	37
15.	Mycelium	37
16.	Electrum	33
17.	Blockchain	30
18.	BitGo	27
19.	Hive	19
20.	Coinbase	18



OVERALL RANK
1 ST

Ledger



Version Reviewed: 1.4.0 (Browser) & 1.1.0 (Firmware)

Supported Platforms: Google Chrome Browser

Hardware Integrations:
Coinkite, Copay, Electrum, Greenbits, Mycelium

Ledger, a French company founded in early 2015, provides a variety of smartcard-based hardware wallets. These external devices store private keys and have been integrated into a variety of competing Bitcoin wallets, in addition to Ledger's own browser extension-based wallet; we reviewed the latter.

We focused on the Ledger Nano, which is a USB stick that can be inserted into a desktop computer. Once a user's PIN is validated using the computer's keyboard, the user can then send and receive funds to multiple accounts.

While Ledger's Chrome extension does not support advanced privacy features such as mixing, nor maintain a local copy of the blockchain, we found it outperformed its competitors in handling privacy basics. The Chrome extension's interface is designed to help users avoid address reuse, and provides excellent support for managing multiple accounts within a single wallet. Multiple account support is growing increasingly important as users' interact with the world using Bitcoin while assuming many online identities.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE
50 / 100

USABILITY	QUALITY	FEEDBACK
15 / 28	**24** / 50	**10** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
19 / 43

PRIVACY FROM NETWORK OBSERVERS

6 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

2 / 4

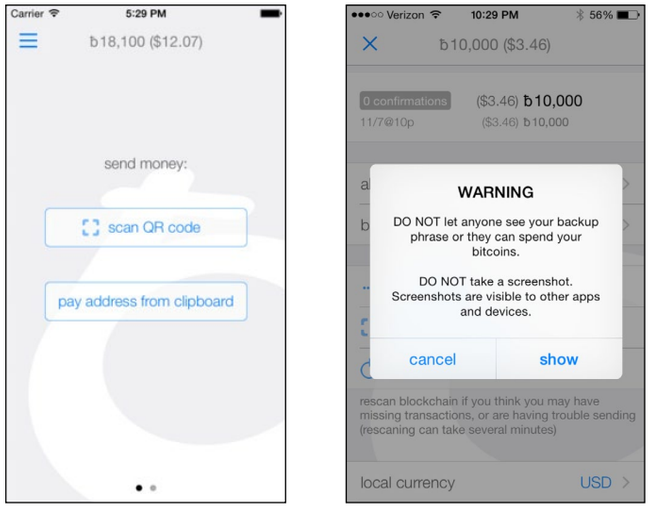
PRIVACY FROM WALLET PROVIDERS

16 / 17

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

OVERALL RANK
2ND

Breadwallet



Version Reviewed: 0.5.2 (iOS)

Supported Platforms: iOS

Breadwallet is a popular iOS wallet. Featuring a simplified user interface, the app provides basic functionality for sending and receiving funds. As a stand-by for Bitcoin users with iPhones for over a year, the wallet has been in active development since early 2013.

Unlike most other mobile wallets, Breadwallet uses a Simplified Payment Verification (SPV) architecture that allows it to obtain balance information directly from nodes in the Bitcoin network. By accessing the Bitcoin network directly, this avoids leaking some of the information commonly transmitted from mobile clients to wallet providers.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE
49 / 100

USABILITY	QUALITY	FEEDBACK
14 / 28	**24** / 50	**10** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
19 / 43

PRIVACY FROM NETWORK OBSERVERS

9 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

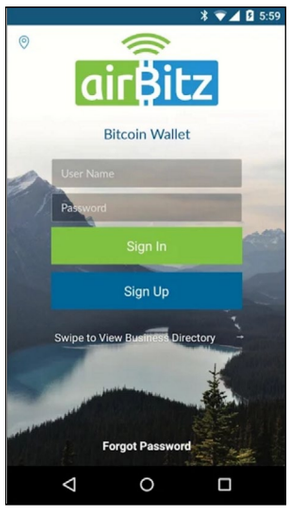
1 / 4

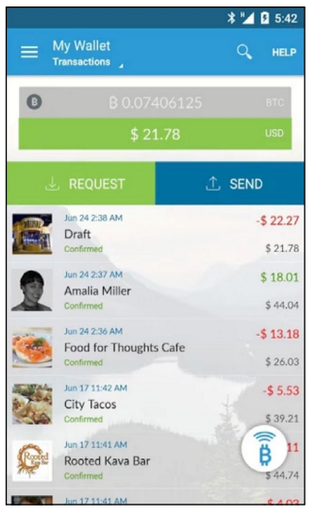
PRIVACY FROM WALLET PROVIDERS

16 / 17

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

Airbitz





Version Reviewed: 1.5.0 (Android)

Supported Platforms: Android, iOS

The Airbitz Bitcoin wallet, first released in early 2014, is a light client available for mobile devices. The mobile app features sending and receiving functionality, the ability to record transaction details, and 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, such as mixing funds. Balance information and transaction broadcasting are conducted through one or more trusted Obelisk servers, affording less network privacy than peer-to-peer wallets, but more than the typical single-server model used by most wallet providers. 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 RANK

3RD

OVERALL WALLET PRIVACY

0 — 100

USABILITY	QUALITY	FEEDBACK
15 / 28	**22** / 50	**10** / 22

TOTAL SCORE

47 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

19 / 43

PRIVACY FROM NETWORK OBSERVERS

6 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

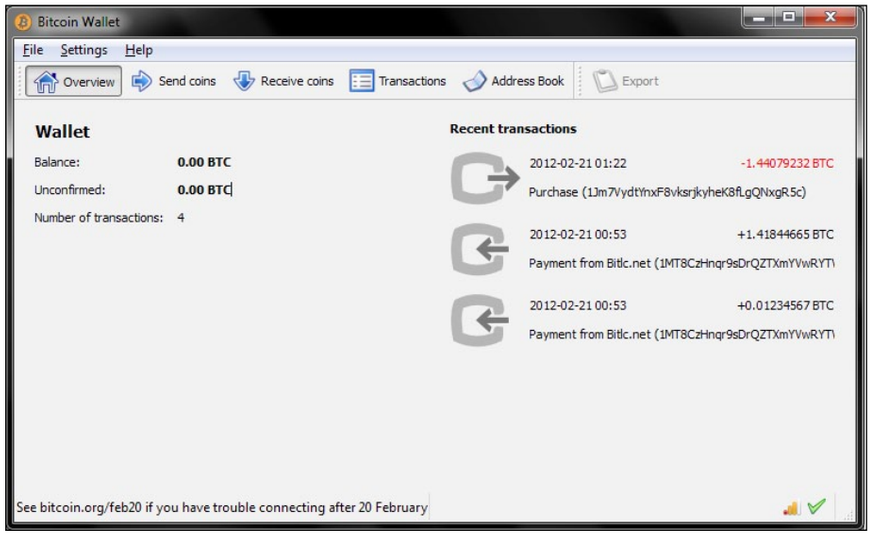
2 / 4

PRIVACY FROM WALLET PROVIDERS

16 / 17

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

Bitcoin-Qt Core



Version Reviewed: 0.11.0

Supported Platforms: Linux, OSX, Windows

Bitcoin-Qt is a graphical interface for the canonical Bitcoin daemon, bitcoind. Although there are now several forks of the Bitcoin project such as Bitcoin Core, Classic, XT, and Unlimited — each with its own very similar version of Bitcoin-Qt — this assessment focused solely on Bitcoin Core's Qt client. Aside from the various versions of Bitcoin-Qt, Armory is currently the only other full node client with a graphical interface. In this assessment, Bitcoin-Qt Core scored about seven points higher than Armory.

Full nodes have strong network privacy protections by virtue of downloading a local copy of the blockchain, avoiding the need to make queries to other parties about specific addresses. Aside from this strength, the official Bitcoin-Qt client has a few basic weaknesses common to most other wallets, such as the lack of built in mixing capability to combat blockchain analysis.

A previous version of this report assigned this wallet client a score of 43.

OVERALL RANK

4TH

OVERALL WALLET PRIVACY

0 — 100

USABILITY	QUALITY	FEEDBACK
13 / 28	**23** / 50	**10** / 22

TOTAL SCORE

46 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

19 / 43

PRIVACY FROM NETWORK OBSERVERS

8 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

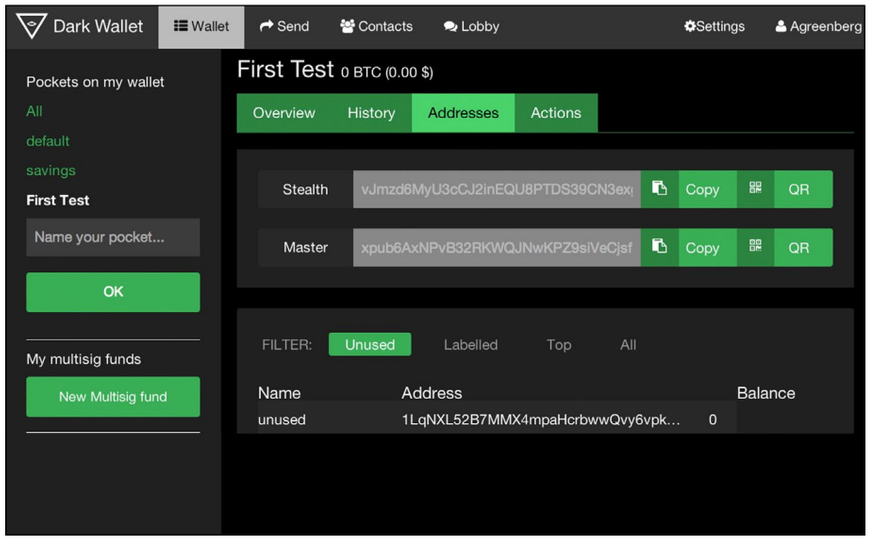
0 / 4

PRIVACY FROM WALLET PROVIDERS

16 / 17

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

Darkwallet



Version Reviewed: 0.8.0 (Google Chrome Browser)

Supported Platforms: Google Chrome Browser

Although Darkwallet's code base remains untouched since our last review, its decline in ranking from first to fourth was caused chiefly by updates to our threat model, rather than a surge in progress by competitors. The once-promising leader of privacy-centric design has been on indefinite hold by its developers since February of 2015.

To date, Darkwallet is still one of only two graphical wallets with CoinJoin support, and one of a handful with ECDHM address support. Darkwallet enables both CoinJoin and ECDHM addresses by default. However, disuse has reduced the available number of Darkwallet partners for CoinJoin transactions, yielding very limited use at present. After a short timeout period, if no other users are available to mix with, the transaction will proceed without the use of CoinJoin.

As part of its privacy-centric design, Darkwallet encourages users to create multiple accounts (referred to as "pockets") within a single wallet, making the segregation of funds between their multiple online identities convenient and easy.

OVERALL RANK

5TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

45 / 100

USABILITY	QUALITY	FEEDBACK
18 / 28	**22** / 50	**5** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

19 / 43

PRIVACY FROM NETWORK OBSERVERS

1 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

8 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

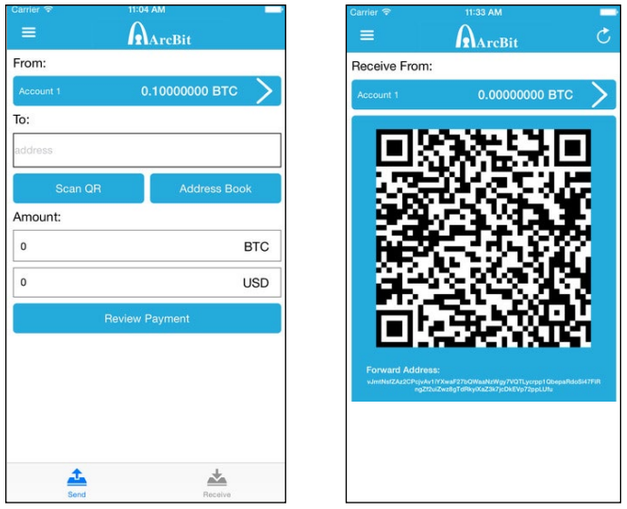
0 / 4

PRIVACY FROM WALLET PROVIDERS

17 / 17

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

ArcBit



Version Reviewed: 1.0.4 (iOS)

Supported Platforms: iOS

ArcBit is a recent contender on the iOS platform that emphasizes a streamlined interface and one novel privacy protection: ECDHM addresses. While adoption of ECDHM addresses has been slow among wallet clients outside of Darkwallet, ArcBit has attempted to reinvigorate the technology with a rebranding they call “forwarding addresses.” Such addresses help users avoid address reuse, and make the sharing of addresses on social networks safe for the first time.

A prominent weakness for ArcBit and many other mobile wallets is protecting users from network observers. While forwarding addresses help protect user privacy on the blockchain, their computationally intensive architecture requires ArcBit users to entrust their privacy to trusted servers, which help to track payments on behalf of the iOS wallet client.

Darkwallet users should take warning that, although ArcBit’s forwarding addresses are extremely similar to Darkwallet’s “stealth” addresses, incompatibilities between the two may render payments sent from ArcBit to Darkwallet stealth addresses invisible to Darkwallet users.

OVERALL RANK

6TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

45 / 100

USABILITY	QUALITY	FEEDBACK
15 / 28	**20** / 50	**10** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

22 / 43

PRIVACY FROM NETWORK OBSERVERS

3 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

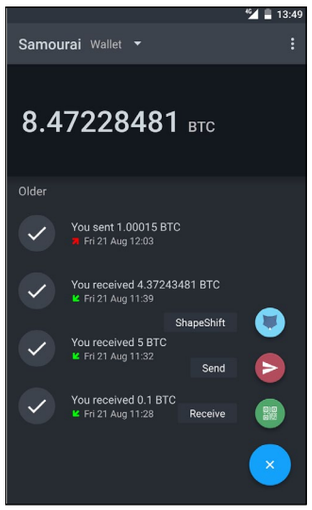
0 / 4

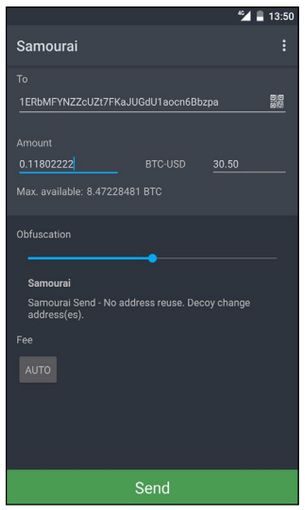
PRIVACY FROM WALLET PROVIDERS

16 / 17

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

Samourai





Version Reviewed: Alpha build A4e9...a911 (Android)

Supported Platforms: Android

Samourai wallet bills itself as “the software that Silicon Valley will never build, the regulators will never allow, and the VC’s will never invest in.” The privacy-centric wallet entered the scene in a closed source alpha release during 2015.

During its early alpha versions, the wallet introduced a series of novel privacy features, including BIP-69 fingerprinting countermeasures, warnings to users for accidental address reuse, and remote wallet wiping via SMS in the case of a stolen or seized device.

Samourai has publicly promised many additional privacy features in future versions including BIP-47 reusable payment codes (a new form of ECDHM address), mixing capabilities, and built-in VPN/Tor support. The developers have also committed to publish their code for scrutiny by other developers and users. The wallet is off to a strong start in 2015, and threatens to usurp Darkwallet for the spotlight in 2016 as the defacto choice for privacy-minded users.

OVERALL WALLET PRIVACY

0 — 100

USABILITY	QUALITY	FEEDBACK
13 / 28	22 / 50	9 / 22

TOTAL SCORE

43 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

19 / 43

PRIVACY FROM NETWORK OBSERVERS

7 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

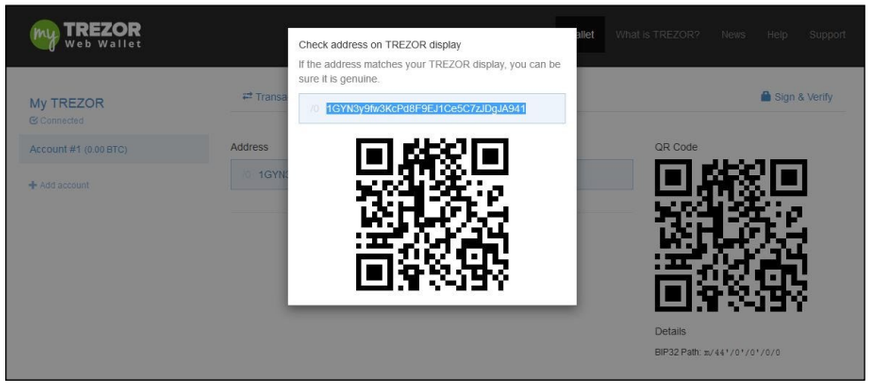
4 / 4

PRIVACY FROM WALLET PROVIDERS

11 / 17

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

Trezor



Supported Platforms: Google Chrome Browser

Trezor, like Ledger and many other hardware wallets, have been successfully integrated into a variety of Bitcoin wallet software products. Someone who purchases the Trezor hardware wallet can choose to link the device with clients such as Electrum, Multibit HD, and Mycelium, and the user's privacy will be chiefly determined by the integrated client rather than their Trezor device. Since there are a variety of wallets applicable to Trezor, we decided to evaluate the myTrezor.com web wallet produced by SatoshiLabs; but users of the hardware wallet should note that this evaluation is not necessarily representative of the device if they choose to link it to a different wallet.

The myTrezor.com web wallet is plain and simple, but its interface steers users away from address reuse, and it offers excellent multi-account support.

The primitive network architecture between the web wallet and the servers it gathers information from causes users to leak information about their wallet over the network when balances are queried or transactions are broadcast. As anonymizing networks like Tor are cumbersome to configure for use with myTrezor.com, this leaves the average user prone to snooping from their Internet Service Provider or eavesdroppers on any unencrypted wireless network.

OVERALL RANK
8TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE
42 / 100

USABILITY	QUALITY	FEEDBACK
18 / 28	**16** / 50	**9** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
18 / 43

PRIVACY FROM NETWORK OBSERVERS

4 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

4 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

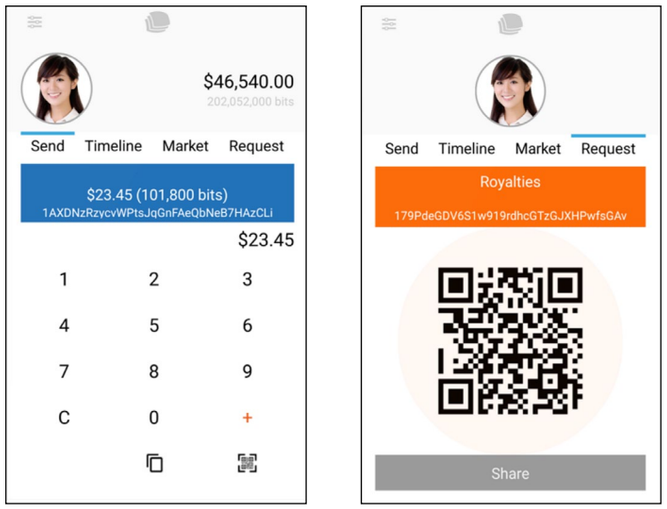
1 / 4

PRIVACY FROM WALLET PROVIDERS

16 / 17

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

LUXSTACK



Version Reviewed: 1.1.40 (Android)

Supported Platforms: Android, iOS

LUXSTACK lands right in the middle of its mobile competitors from a privacy standpoint; not a bad start for a wallet launched within the last year, but not yet exceptional. The interface features basic functionality for sending and receiving funds, and utilizes a single-account HD wallet structure to help avoid address reuse.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

42 / 100

USABILITY	QUALITY	FEEDBACK
9 / 28	**22** / 50	**10** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

19 / 43

PRIVACY FROM NETWORK OBSERVERS

9 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

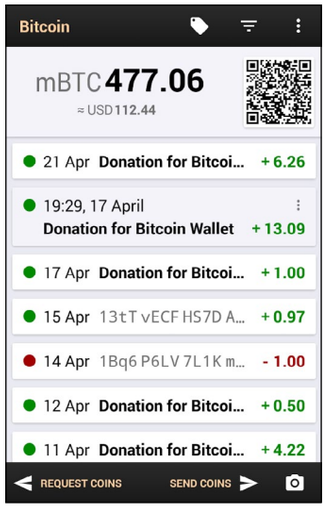
2 / 4

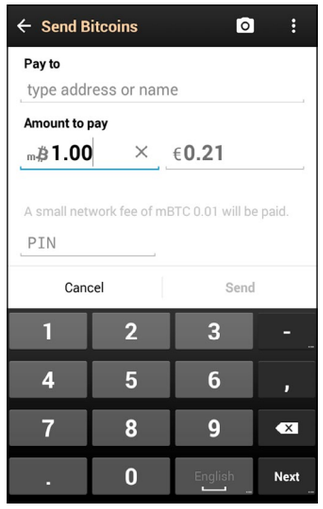
PRIVACY FROM WALLET PROVIDERS

9 / 17

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

Bitcoin Wallet





Version Reviewed: 4.39 (Android)

Supported Platforms: Android

The generically-named “Bitcoin Wallet” was one of the first wallet clients made available for the Android platform. Often referred to as the “Schildbach Wallet” after its venerable creator, Andreas Schildbach, the wallet is one of only a few mobile wallets supporting a Simplified Payment Verification (SPV) architecture, using the BitcoinJ library. SPV wallets are able to connect directly to Bitcoin nodes to obtain balance information and broadcast transactions, rather than relying on a trusted third-party server, as the majority of mobile wallets do.

Network privacy remains an unsolved problem for Bitcoin Wallet and other SPV clients, as they struggle to prevent the leakage of information about user wallets to the Bitcoin network without maintaining their own copy of the blockchain to query locally.

The wallet does not support multiple accounts for users, but rather recommends that users undergo the laborious process of creating multiple Android user accounts and switching between them as needed.

OVERALL RANK
10TH

OVERALL WALLET PRIVACY

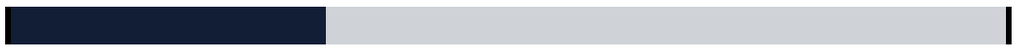
TOTAL SCORE
42 / 100

USABILITY	QUALITY	FEEDBACK
13 / 28	**22** / 50	**7** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

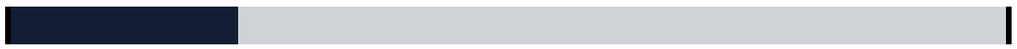
CATEGORY SCORE
16 / 43

PRIVACY FROM NETWORK OBSERVERS



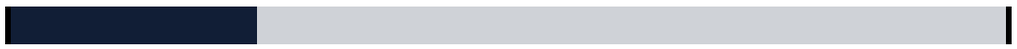
7 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS



3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES



1 / 4

PRIVACY FROM WALLET PROVIDERS

16 / 17

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

MultiBit HD

Version Reviewed: 0.1.2 (Cross-Platform)

Supported Platforms: Linux, OSX, Windows

Hardware Integrations: Trezor, KeepKey

In the previous edition of our report, we examined the MultiBit Classic wallet. Since then, the MultiBit team has formally released a major facelift to the product in the form of MultiBit HD. As the name implies, the new version uses a Hierarchical Deterministic architecture, helping users avoid address reuse and backup their wallet quickly.

Similar to the "Bitcoin Wallet" client for Android, MultiBit HD follows an SPV architecture through the use of the BitcoinJ library. Correspondingly, it suffers the same network privacy challenges as other SPV wallets.

Multibit HD has one unique privacy quirk: By default, one out of every several transactions will include a small donation output to the Multibit developers. While this is a clever business model, it does betray to passive blockchain observers which client was used to author the transactions. This can be disabled by making a more sizeable donation to the development team.

OVERALL WALLET PRIVACY

0 — 100

USABILITY	QUALITY	FEEDBACK
12 / 28	21 / 50	7 / 22

TOTAL SCORE

40 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

15 / 43

PRIVACY FROM NETWORK OBSERVERS

7 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

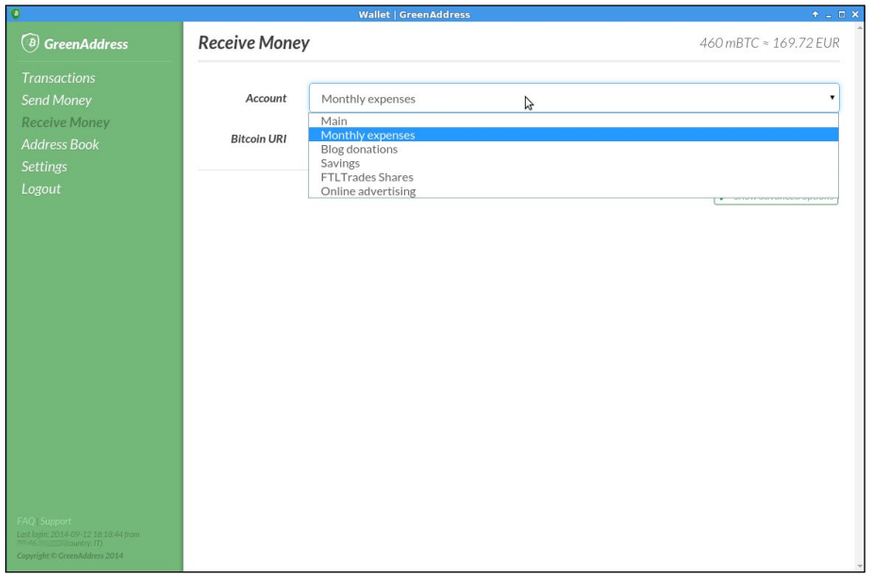
1 / 4

PRIVACY FROM WALLET PROVIDERS

15 / 17

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

GreenAddress



Version Reviewed: 0.0.67 (Google Chrome Browser)

Supported Platforms: Android, iOS, Chrome, Web

The central idea behind GreenAddress is to take custody over one of the two private keys required to move users' multi-signature funds. This allows GreenAddress users to set various security controls such as daily spending limits or requiring a second factor of authentication before sending funds. So long as GreenAddress refuses to sign transactions that attempt to spend the same customer funds twice, they can also use this mechanism to prevent double spends. Prevention of double spending is the origin for the name of the service: a trustworthy address is considered "green" for acceptance without confirmations, assuming you trust the company not to allow double-spends.

The shared custody over funds also gives the service intimate knowledge about the status of user funds.

One quirk of the Chrome plugin user interface is that, in order for a user to generate a new receiving address, he must click on a different category in the menu, such as "Transactions," and then click back to the "Receive Money" section. This may lead users to accidentally reuse addresses if receiving multiple transactions in a row, or if they leave the application open in between uses.

OVERALL RANK

12TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

39 / 100

USABILITY	QUALITY	FEEDBACK
12 / 28	**21** / 50	**5** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

14 / 43

PRIVACY FROM NETWORK OBSERVERS

4 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

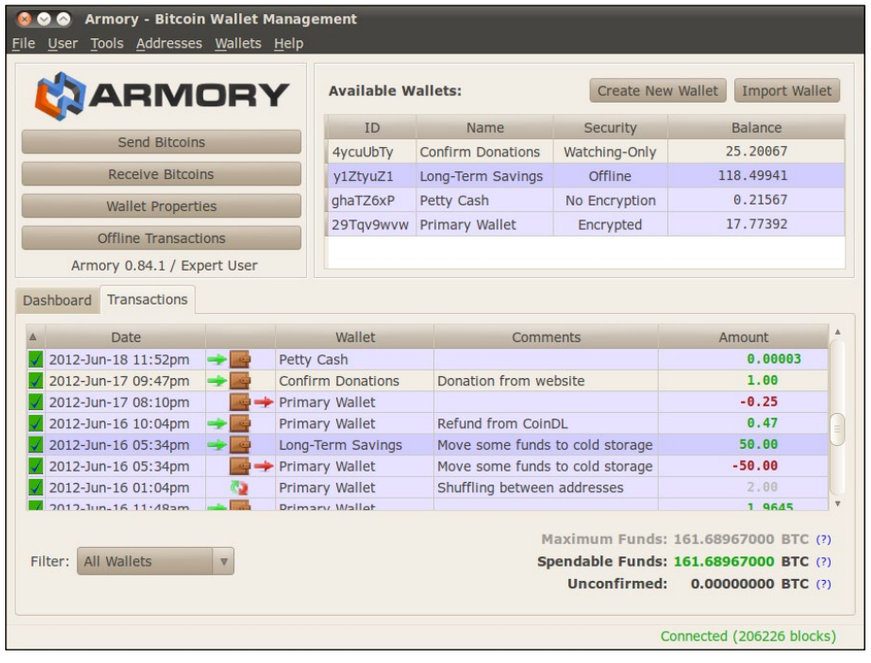
1 / 4

PRIVACY FROM WALLET PROVIDERS

17 / 17

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

Armory



Version Reviewed: 0.93.2 (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 the last year, the company has pivoted to focus their efforts primarily on paying enterprise customers. The existing consumer version of the wallet emphasizes advanced security features such as offline signing and fragmented backups.

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, though users will need to engage in some setup steps first.

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 RANK
13TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE
38 / 100

USABILITY
12 / 28

QUALITY
20 / 50

FEEDBACK
6 / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
14 / 43

PRIVACY FROM NETWORK OBSERVERS

8 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

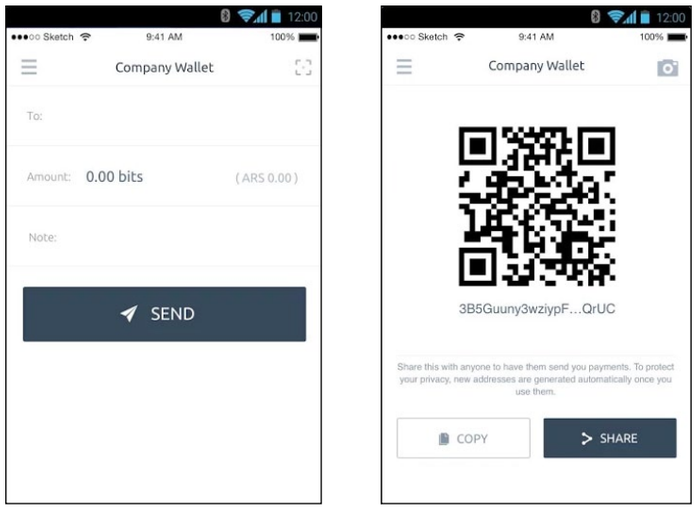
1 / 4

PRIVACY FROM WALLET PROVIDERS

13 / 17

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

Copay



Version Reviewed: 1.1.2 (Android)

Supported Platforms: Android, iOS, Windows Phone, Chrome, Linux, OSX, Windows

Hardware Integrations: Trezor

Copay is a multi-signature wallet produced by the payment processing company, BitPay. Their multi-signature technology allows multiple users to have partial control over the same funds on different devices. In the Google Play store description for the app, Bitpay stated it could be used for cases such as “saving for vacations or joint purchases with friends,” “tracking family spending and allowances,” and “managing business, club, or organization funds and expenses.”

The primary privacy defense that Copay utilizes is their HD address architecture, which helps to avoid address reuse. Because of the use of P2SH-style multisignature addresses, the number of cosigners involved in each transaction is recorded in the blockchain, and all cosigners can track each other’s activity with respect to the shared wallet.

Some privacy defenses missing from Copay but commonly present in other wallet clients include BIP-62 compliance to avoid client fingerprinting, avoiding the querying of balance information for separate accounts in the same request, protecting physical access to wallet data with a PIN, and allowing users to review their telemetry data before it is submitted to the company.

Advanced users can download the Copay server source code from GitHub and run their own personal Copay server, rather than using the company’s, to better protect their network traffic privacy.

OVERALL RANK

14TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE **37 / 100**

USABILITY	QUALITY	FEEDBACK
13 / 28	**14** / 50	**10** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE **19 / 43**

PRIVACY FROM NETWORK OBSERVERS

1 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

4 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

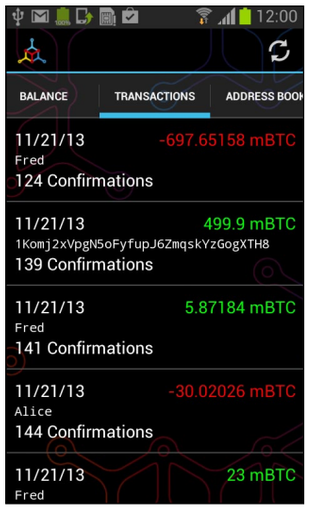
1 / 4

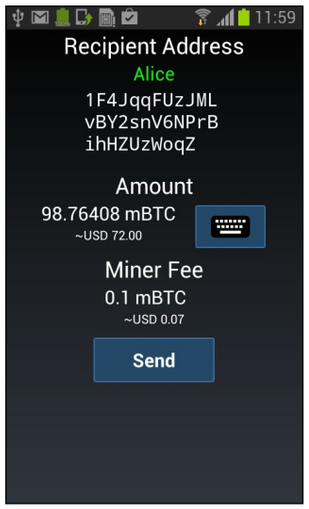
PRIVACY FROM WALLET PROVIDERS

13 / 17

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

Mycelium





Version Reviewed: 2.4.4 (Android)

Supported Platforms: Android, iOS

Hardware Integrations: Ledger (requires OTG adapter), Trezor

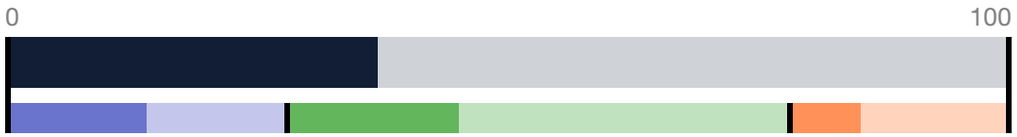
Mycelium is a popular and well-regarded wallet client on the Android platform. Mycelium uses an HD architecture based on BIP-44, which helps users avoid address reuse and segregate their funds into separate accounts; managing multiple accounts lets a user keep funds separate for different online identities, establish spending and savings accounts, and so on. Mycelium's Android client also features a built-in, peer-to-peer system called Local Trader that helps users exchange between local fiat currencies and Bitcoin, similar to LocalBitcoins.com.

Since our last report, the Android client has not changed much with respect to its privacy, and the wallet has fallen somewhat behind its mobile competitors. However, it is rumored that Mycelium is working on a CoinShuffle implementation; this would be an industry first, and could dramatically decrease the amount of information leaked to the blockchain concerning users' finances.

At the network level, Mycelium uses a traditional client-server model, obtaining balance information and broadcasting transactions via dedicated Mycelium servers. 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.

OVERALL RANK
15TH

OVERALL WALLET PRIVACY



TOTAL SCORE
37 / 100

USABILITY
14 / 28

QUALITY
17 / 50

FEEDBACK
7 / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
17 / 43

PRIVACY FROM NETWORK OBSERVERS

1 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

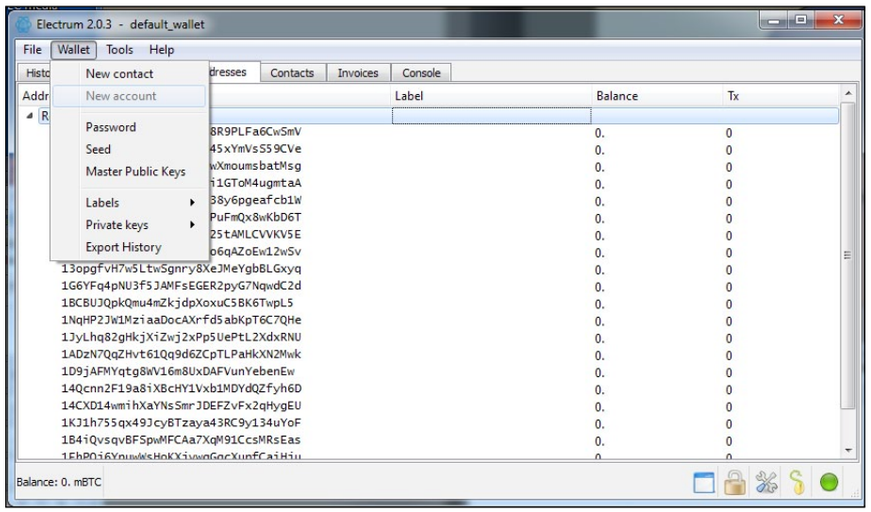
1 / 4

PRIVACY FROM WALLET PROVIDERS

16 / 17

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

Electrum



Version Reviewed: 2.4.4 (Linux)

Supported Platforms: Linux, OSX, Windows

Hardware Integrations: Ledger, Trezor

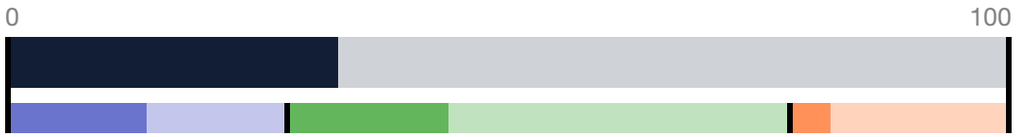
Electrum is a cross-platform lightweight desktop wallet that has been under active development since November 2011. This wallet uses a deterministic seed to generate all keys, backed up by a 12-word string.

Instead of downloading the entire blockchain, the client 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 also supports two-factor authentication, and provides compatibility with hardware wallets such as Ledger and Trezor.

Electrum was the first wallet to implement BIP-69 in version 2.3.2, as a countermeasure against passive blockchain observers attempting to identify Electrum transactions on the blockchain.

Because the Electrum client connects to servers for data, users sacrifice privacy and must rely on trust in the blockchain information received. 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



USABILITY **14** / 28

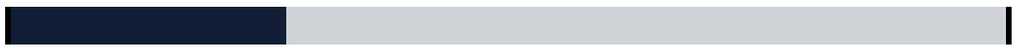
QUALITY **16** / 50

FEEDBACK **4** / 22

TOTAL SCORE

33 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS



CATEGORY SCORE

12 / 43

PRIVACY FROM NETWORK OBSERVERS

2 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

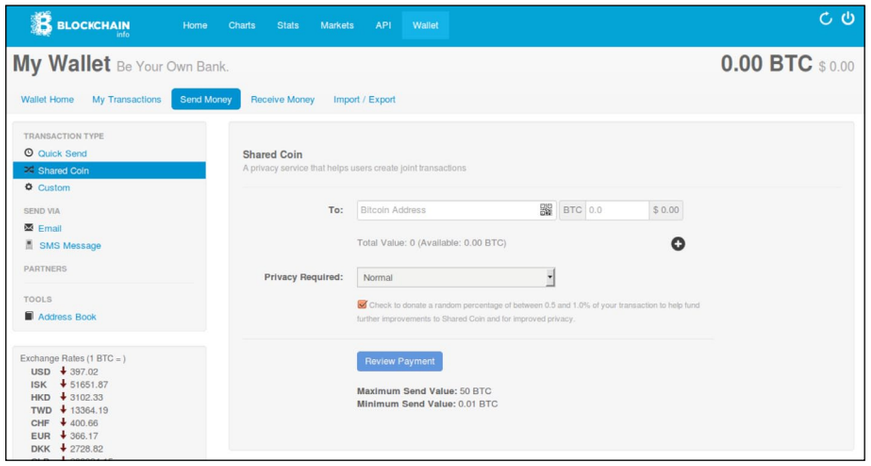
1 / 4

PRIVACY FROM WALLET PROVIDERS

16 / 17

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

Blockchain



Version Reviewed: Web

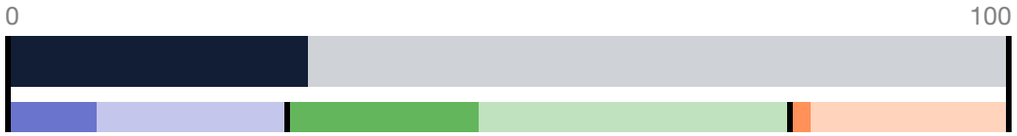
Supported Platforms: Android, iOS, Web

By most reckonings, Blockchain has the single largest user base of Bitcoin wallets, with nearly 6 million wallet accounts created. The wallet and API combined represent 30% to 60% of all on-chain transaction volume. The company has recently been developing a revamped version of their long-standing web and mobile wallet apps. As these products remain in a pre-production stage at the time of writing this report, we assessed the web wallet in production, which is largely unchanged from our first report.

Blockchain's SharedCoin feature, exclusive to the web wallet (not available on Android or iOS) helps users defend their privacy against attackers using clustering analysis of the blockchain. To date, the only other wallet to offer a service of this kind is Darkwallet.

Overall, Blockchain's outdated web wallet offers fewer privacy protections than most of its competitors. Users must perform additional actions outside of the normal sending and receiving workflows to avoid simple privacy pitfalls such as address reuse. 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 company-owned server. This can potentially shield the privacy of users from the larger Bitcoin network, but requires users to trust Blockchain with this sensitive data.

OVERALL WALLET PRIVACY



USABILITY **9** / 28

QUALITY **19** / 50

FEEDBACK **2** / 22

TOTAL SCORE

30 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

8 / 43

PRIVACY FROM NETWORK OBSERVERS

2 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

7 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

2 / 4

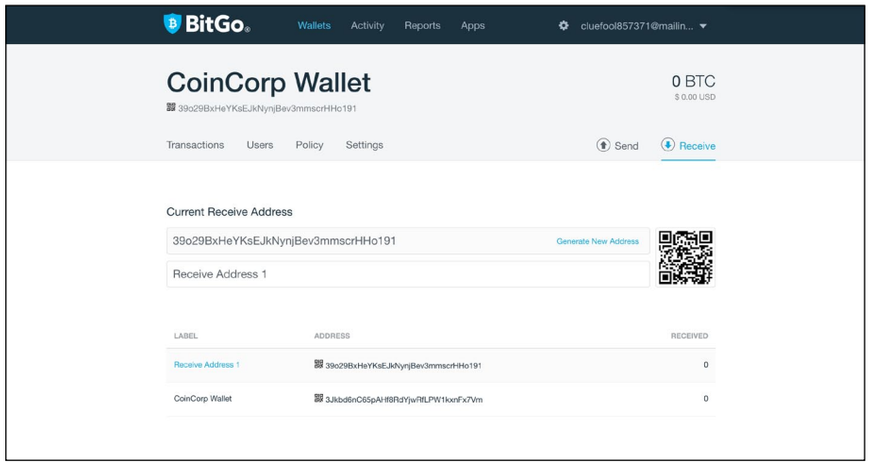
PRIVACY FROM WALLET PROVIDERS

12 / 17

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

BitGo

OVERALL RANK
18TH



Version Reviewed: Web

Supported Platforms: Google Chrome Browser, Web

BitGo is a US-based company founded in 2013 that provides wallet and API services for Bitcoin users and businesses. They were one of the first companies to pioneer a Multi-signature wallet, and their current product line emphasizes the use of multisignature addresses to boost security for users. This approach to wallet security is particularly suited for corporate users, and permits a tiered hierarchy when checking the balance of and sending an organization's funds.

For the second edition of our report, we took a look at BitGo's web wallet. In many ways, its privacy was comparable to other web wallets we've reviewed, such as the blockchain.info web wallet. One current key difference is that BitGo requires an email address for registration; users unfortunately cannot determine the degree to which BitGo's servers tie the email address to funds. For the average user, this is a risky privacy proposition, since email addresses are often closely tied to a person's online and offline identity.

The web wallet can be used by individuals or groups. In the case of a group using the wallet's multi-signature technology, the number of signatures provided and required in order to move funds will be included in blockchain data due to the use of traditional P2SH "m-of-n" multi-signature scripts. Additionally, members of the wallet will have mutual knowledge about their finances.

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE
27 / 100

USABILITY	QUALITY	FEEDBACK
11 / 28	**11** / 50	**5** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
13 / 43

PRIVACY FROM NETWORK OBSERVERS

6 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

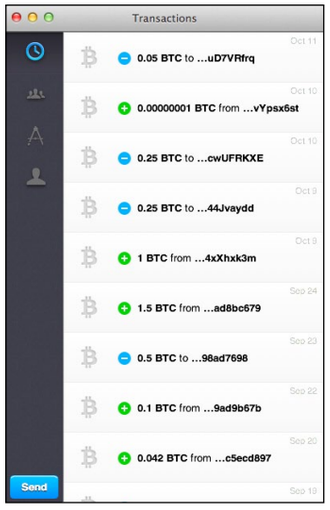
2 / 4

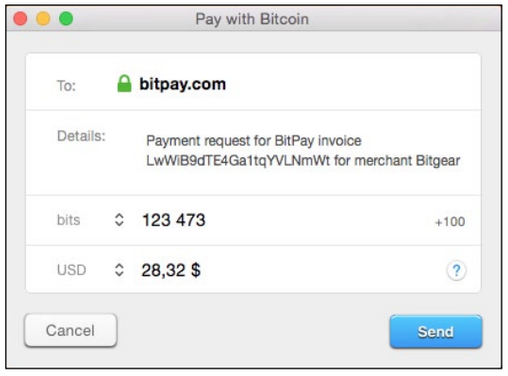
PRIVACY FROM WALLET PROVIDERS

4 / 17

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

Hive





Version Reviewed: 1.4.2 (OSX)

Supported Platforms: Android, iOS, OSX, Web

Hive is a cross-platform wallet available on for the Mac, mobile devices, and web. Our assessment for this report focused on the OSX version of the app.

An early version of Hive was released in late 2013, but by 2015 the project had largely fizzled out. It is currently available for use, but unmaintained.

To date, the Hive OSX client is the only client we've found that lacks a fundamental privacy control: the ability to generate more than one Bitcoin address in a wallet. As users cannot escape a pattern of address reuse, they are subject to trivial blockchain analysis attacks.

OVERALL RANK

19TH

OVERALL WALLET PRIVACY

0 — 100

TOTAL SCORE

19 / 100

USABILITY	QUALITY	FEEDBACK
5 / 28	**12** / 50	**1** / 22

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE

1 / 43

PRIVACY FROM NETWORK OBSERVERS

7 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

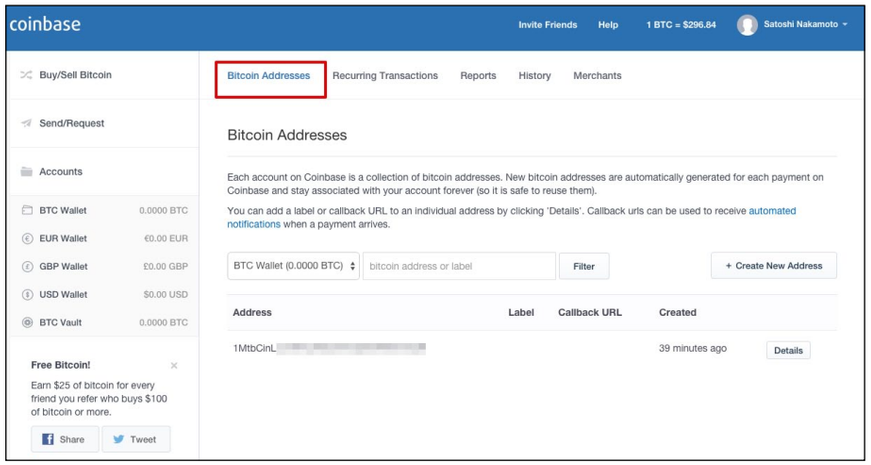
1 / 4

PRIVACY FROM WALLET PROVIDERS

8 / 17

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

Coinbase



Version Reviewed: Coinbase classic wallet (Web)

Supported Platforms: Android, iOS, Web

Coinbase is a prominent company in the Bitcoin space that provides Bitcoin exchange, payment processor, and wallet services on the web with a reported 3.1 million users. Their wallet can be subdivided into two components: a classic version, and Coinbase Vault. For both versions of their wallet, 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. As with our last report, we focused on the classic version of the wallet functionality.

Coinbase also provides mobile applications that allows users to access their custodial accounts, with similar privacy properties.

We reviewed Coinbase in our last report, but the quality of its privacy remains unchanged since.

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 when sending funds from the wallet, but employs few other 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 RANK
20TH

OVERALL WALLET PRIVACY

0 — 100

USABILITY **7** / 28

QUALITY **9** / 50

FEEDBACK **1** / 22

TOTAL SCORE
18 / 100

PRIVACY FROM BLOCKCHAIN OBSERVERS

CATEGORY SCORE
6 / 43

PRIVACY FROM NETWORK OBSERVERS

6 / 22

PRIVACY FROM TRANSACTION PARTICIPANTS

3 / 13

PRIVACY FROM PHYSICAL ADVERSARIES

2 / 4

PRIVACY FROM WALLET PROVIDERS

0 / 17

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

Privacy Ratings Methodology

Each wallet is subject to 68 privacy tests 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.

A complete description of the ratings methodology can be found in our GitHub repository:

https://github.com/OpenBitcoinPrivacyProject/wallet-ratings

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

BOOLEAN

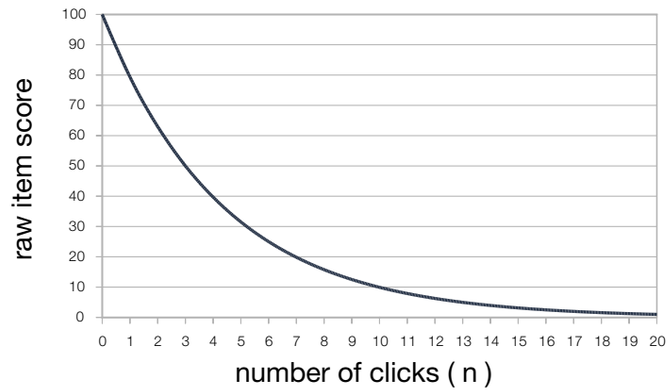
When the result of a test is true, that item is assigned a score of 100.
When the result of a test is false, the item is assigned a score of 0.

NUMBER OF CLICKS/TAPS

The number of clicks (with a mouse) or taps (on a mobile device) 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

Some privacy tests are evaluated on an individualized basis according to tiered assessments. For example:

II E 1 a: 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

Acknowledgements

SURVEY PARTICIPATION

In preparation for this report, we sent questionnaires to wallet providers to facilitate accurate assessment. These questions asked about “under the hood” aspects of the wallet that would be difficult for volunteers to assess on their own without the use of code review and special tools. Topics covered by the questionnaire include transaction formatting, mixing capabilities, automatic donations and fees, balance query and transaction broadcast architecture, and the collection of telemetry data.

We received detailed responses to our survey from the following wallet providers:

- Airbitz
- ArcBit
- Armory
- Bitcoin Wallet
- BitGo
- Breadwallet
- GreenAddress
- Ledger
- LUXSTACK
- MultiBit HD
- Mycelium
- Samourai
- Trezor

The following wallet providers either did not reply to repeated attempts to contact them, or abstained from responding:

- Bitcoin-Qt
- Blockchain
- Coinbase
- Copay
- Darkwallet
- Electrum
- Hive

SPONSORS

This report was sponsored by Stash Crypto (stashcrypto.com)

CONTRIBUTORS

To help gather the large amount of data required for each wallet, we reached out to wallet providers for volunteers to help with ratings. All ratings were cross-checked independently by multiple raters and subjected to an open consensus process by mailing list.

We’d like to thank the following wallet providers for volunteering their support:

- Airbitz
- Samourai
- ArcBit
- BitGo
- Ledger
- GreenAddress
- LUXSTACK
- MultiBit
- Mycelium
- SatoshiLabs (Trezor)

The following individuals assisted in the rating process:

- Kristov Atlas
- LaurentMT
- Justus Ranvier
- Samourai Wallet developers
- Tomas Horvath
- Andreas Antonopoulos
- Block Lud
- Gabe Higgins
- Jaco de Beer
- Jameson Lopp
- Jim Burton
- Kevin Aleman
- Lawrence Nahum
- Martin Sip
- Nicolas Bacca
- Rassah
- Stephanie Murphy
- Tim Lee
- Wei
- Will Pangman

Testing hardware was donated by:

SatoshiLabs (Trezor)

Threat modeling was developed by these individuals, along with other contributors via GitHub:

- Justus Ranvier
- Kristov Atlas
- Chris Pacia
- LaurentMT
- Samuel Patterson
- Alon Muroch
- Eric Voskuil
- Jeremy Rand
- Olivier Lalonde
- Peter Todd
- Sergio Demian Lerner
- Whit J

Graphic design and production work was provided by BTC Design (btcdesign.com).

To assist with our privacy threat modeling, wallet ratings, or other future projects, please contact us via openbitcoinprivacyproject.org/connect.

open bitcoin privacy project

The Open Bitcoin Privacy Project (OBPP) is a world-wide not-for-profit organization focused on improving financial privacy in the Bitcoin ecosystem. Our mission is to make financial privacy visible so that individuals and organizations can make informed decisions about privacy risks.

Our efforts to date include:

- Bitcoin wallet client privacy reports
- An ever-evolving Bitcoin wallet client threat model
- Gathering and visualizing blockchain privacy statistics
- Collaboration on proposals to improve Bitcoin privacy, such as BIP-47 and BIP-69
- Ongoing support for Bitcoin wallets and services seeking advice on improving their privacy
- An open Wiki documenting key technologies related to Bitcoin privacy

All source materials for our projects can be found on our GitHub account:
https://github.com/openbitcoinprivacyproject

We hold regular, publicly accessible meetings to discuss our projects. We also maintain an open mailing list for discussion. Details about meetings and access to the mailing list can be found here:
https://openbitcoinprivacyproject.org/connect/

Producing this report requires many volunteer hours and other contributions from OBPP participants. We gratefully accept your donations to help support future reports like this one; all donations go toward covering the costs of testing hardware, graphic design, and other expenses.

MULTISIG ADDRESS:

3CNH4hKztZLDha7Vw8
GHrP829BRGoebqbU

STEALTH ADDRESS:

vJmva9AvqqjvhtzBKmaGmXgweAt964Mo3fR
VRjWUu6sGRgdbDkxop5PuDuWfvCpWtdm6
zH3K47zPhByQXsiDXStK77zTCjUWe6Tsn8