Enterprise Best Practices for Cryptocurrency Adoption

Pat Litke and Joe Stewart
Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Release Date: 27 January 2014

Introduction

Bitcoin is a digital currency and payment system introduced in 2009. It is a cryptocurrency, so-called because it uses cryptography to control the creation and transfer of money.

When working with Bitcoin, wallet security is the name of the game. A Bitcoin wallet is a collection of private encryption keys that can unlock funds sent to their corresponding public keys, or Bitcoin addresses. Whoever controls the private key of a Bitcoin address can spend the funds it contains. Once funds are transferred (that is, signed over to another Bitcoin address), the original owner cannot retrieve them. Essentially, holders of Bitcoin act as their own bank. No one can seize funds without the private key, but no one can replace funds if the private key is lost or stolen.

Ultimate responsibility for the security of a large sum of Bitcoins may be intimidating, but transacting with Bitcoin does not need to be a daunting or risky task.

This analysis requires a basic understanding of the following concepts as they relate to Bitcoin:

- Addresses
- Mining
- Wallets

The official Bitcoin glossary provides easy to understand definitions. Additional technical information, including answers to frequently asked questions, can be found on the Bitcoin wiki.

Wallet fundamentals

Real-world wallet loss

These two examples of poor security practices and subsequent ramifications illustrate some of the avoidable risks associated with cryptocurrencies such as Bitcoin.

According to a news story, a laptop discarded in mid-2013 hosted a wallet containing approximately 7,500 Bitcoins. Bitcoins weren't valuable in 2009 when they were mined, so the wallet was not backed up. At present value, this user's loss can be calculated in millions of dollars.

Lesson: Back up your wallet!

In 2012, the BTC-E crypto-currency exchange was hacked and lost 4,500 Bitcoins. People who stored Bitcoins in the exchange lost all their funds. Fortunately, BTC-E was able to reimburse customers, but this same scenario has been repeated several times at other exchanges without a positive outcome.

Lesson: Trusting someone with your wallet is a bad idea.

Keeping your wallet safe

A wallet on a device that has network connectivity is at risk. Bitcoin is very much on the radar of computer criminals and Bitcoin-harvesting malware is increasingly popular. A wallet is stored on a device that is not connected to the Internet (or any network), becomes much more difficult to steal.

Types of wallets

Online wallet

An online wallet is "online" in the sense that the client is connected to the Internet, versus a wallet accessed via a website, which is known as a web wallet. The online wallet is the "traditional" type of wallet implemented in the Bitcoin reference client, as well as used by most desktop and mobile Bitcoin clients. Keypairs are stored in a file on the local device and accessed by the Bitcoin client that is connected directly to the Bitcoin peer-to-peer network.

Online wallet risks

- Physical theft of device
- Hard drive failure
- Theft of wallet file by malware

Online wallet risk mitigations

Use of wallet encryption is recommended when a wallet file is created on a networked device. However, malware that can steal a wallet file can also record decryption passphrases as they are entered on the keyboard or pasted from the clipboard. Therefore, the best mitigation is to avoid using this type of wallet.

Brain wallets

Because a private key is essentially a very long number, a wallet need not be stored in digital or written format. The private key could simply be memorized. However, as most humans are unable to reliably remember numbers with dozens of digits, there are shortcuts that can produce a "brain wallet" that is completely non-physical, existing only in the memory of the owner.

There are two types of brain wallets:

- The first type is created by accepting a user-provided passphrase as an input to an algorithm that generates a longer key based on the passphrase. This type of brain wallet is only as secure as the entropy of the passphrase. Because most humans are remarkably bad at thinking of a random string of characters or words, some brain wallets of this type have been stolen in seconds by thieves using "rainbow tables," which are large pre-generated lists of private keys created from common words, phrases, and combinations of characters.
- The second kind of brain wallet contains a private key generated with randomized data. An algorithm then generates a sequence of words that can reconstruct the private key. This sequence of words can be memorized and the key can be deleted from the device that generated it. As long as a copy of the program that generated the word list exists and the word sequence is remembered, the wallet can be recreated at any point in the future.

Brain wallet risks

- Loss of memory
- Weak passphrase

Brain wallet risk mitigations

Only use high-entropy seed passphrases generated by a secure offline device. Write down the passphrase (without reference to what it is) and store in a safe or bank vault.

Paper wallets

A paper wallet is a keypair that has been written or printed to paper. Often the keys are displayed as both text and QR codes for easy importation into a Bitcoin client.

Figure 1. An example of an unencrypted Bitcoin paper wallet. (Source: Dell SecureWorks)

Paper wallet risks

- Physical destruction (e.g.: water, fire, fading ink)
- Theft by duplication (attacker can photograph or manually copy the private key if shown the paper wallet)

Paper wallet risk mitigations

Seal paper wallets in watertight UV-resistant plastic. Store multiple copies in different secure locations, such as a fireproof safe or bank vault. Use Bitcoin Improvement Protocol (BIP)BIP 0038 passphrase encryption to protect the private key from unauthorized use. Do not transmit a picture of an unencrypted paper wallet to public destinations such as social media sites.

Figure 2: . An example of an encrypted Bitcoin paper wallet. (Source: Dell SecureWorks)

Web wallets

Web wallets have become a popular choice for newcomers to Bitcoin. They're easy, accessible, and users only need to keep track of a typical account username and password. From a convenience standpoint this sounds great, but for security, not so much. Any wallet where the owner does not control the private key technically does not belong to the owner. Anyone who manages to access the server where the web wallet is stored can transfer the funds. Users might think their funds are insured when using a web wallet service, much like putting money in a bank. However, there is no insurance organization such as the Federal Deposit Insurance Corporation (FDIC) for Bitcoin. If the funds are stolen, then they will likely not be replaced.

Web wallet risks

- Physical theft
- Hard drive failure
- Theft of web wallet by malware
- Loss of memory
- Weak username or password

Web wallet risk mitigations

Avoid web wallets except as necessary to convert between currencies. At publication time, cryptocurrency exchanges (e.g.: Mt. Gox, Bitstamp, CampBX, and BTC-E) are the easiest way to trade large amounts of fiat (backed by a government) currency for Bitcoin and vice versa. Unfortunately, they also tend to be primary targets for Bitcoin theft, due to the amount of funds stored at the exchange.

As exchanges are essentially web wallets, currency should be stored only for as long as necessary for the trade. Once Bitcoin have been purchased or sold, the funds should be transferred out as quickly as possible to mitigate any potential security breach of the site.

Many web wallets and exchanges offer two-factor authentication (2FA) using one-time passwords (OTP). While this is a step in the right direction, this type of authentication provides no security against malware that can hook into the web browser. Conventional banking malware has been bypassing this type of authentication for years, and these techniques will likely soon be adapted to compromise web wallets protected by 2FA.

Hybrid wallets

A hybrid wallet is a combination of a web wallet and a traditional wallet. It uses JavaScript to manage private and public keys on the client side, so keys are never stored on the server and cannot be stolen en masse. Hybrid wallets are popular, but trusting its security because the keys are not stored server-side is misguided, as an attacker can still steal a user's keys. Because hybrid wallets offer slightly more security than web wallets, while maintaining the convenience of a single wallet that can be easily accessed from both mobile devices and desktops, they are likely to be the most popular form of Bitcoin client for the foreseeable future.

Hybrid wallet risks

- Website compromise can modify JavaScript delivered from server to leak private keys and passphrases from client
- Malware on client side can steal keys and passphrases directly from web browser

Hybrid wallet risk mitigations

Only use this type of wallet for small transactions.

Offline wallet

An offline wallet is a traditional wallet created on a device that runs Bitcoin client software but is never connected to a network. A Raspberry Pi computer running the GNU/Linux operating system and the Electrum wallet software makes an excellent offline wallet. In this configuration, the offline wallet pairs with an online wallet that connects to the network. The online wallet knows what Bitcoin addresses belong to the offline wallet and can create transactions. However, the online wallet cannot sign transactions because it does not have access to the private key. A transaction request must be manually transferred to the offline wallet (e.g.: via a USB drive or by QR code webcam capture). The offline wallet reads and signs this request, authorizing the transfer of funds out of the wallet. This signed transaction is then manually transferred to the online wallet, where it is submitted to the network for verification.

Offline wallet risks

- Infection of offline device by exploit delivered by USB or QR code
- Preloading of device, operating system, or wallet software with code that weakens the random number generator used to create the private key (so-called "kleptographic attacks")

Successful exploitation of an offline wallet is more difficult than a compromise of an online wallet, but it is still a possibility. An attack on the code repository used by a popular wallet client could insert code to weaken the random number generation algorithm. These types of attacks would likely be detected eventually, but any users of the software that downloaded the client during the affected period would have generated weak wallet keys and be subject to theft of funds.

Offline wallet risk mitigations

All code used by offline wallets should be open-source, compared against the public code repository, and audited for potential vulnerabilities. A blackbox audit of the random number generator inside the key generation binary should be conducted to ensure that the key being generated is seeded with random data in a truly unpredictable fashion.

Type-2 deterministic wallets

Similar to brain wallets, Type-2 deterministic wallets are based on a seed number that can be exported as a sequence of words, which can be memorized and saved. Their primary feature is that any number of private keys can be generated from the seed data in a deterministic fashion, that is, the same seed will generate the same sequence of private keys and corresponding public keys every time. There is a special "master" public key that is derived from the seed and can be imported into online clients. The master public key allows the online client to know all of the public keys that belong to the wallet, without knowing the seed value or private keys. A wallet configured this way is called a "watching" wallet and knows the balance of the wallet's addresses, but cannot authorize transactions without the transaction being signed by the offline wallet.

This analysis does not cover Type-1 deterministic wallets, as they are functionally equivalent to Type-2 but lack security measures and additional features. As a result of the lack of security, their use is not recommended.

Because the master public key need not be a secret, the wallet can be simultaneously used on multiple devices. While metadata won't remain synchronized (e.g.: nicknames you give your addresses, or notes about given transactions), data such as addresses, transactions, and balances will automatically stay synchronized.

At publication time, two variants of the Type-2 wallet exist: Armory and Electrum. Both are Type-2 deterministic wallets and either is an excellent choice.

Hardware wallets

A hardware wallet is a single-purpose electronic device that stores one or more private keys and allows for easy offline transaction signing. Bitcoin wallet clients that support hardware wallets generate and send an unsigned transaction to the device. The transaction details are displayed by the device, verified and signed by the user, and returned to the online client for submission to the Bitcoin peer-to-peer network.

One such wallet is called the "Trezor", which is German for "vault" or "safe." This particular device requires a USB cable to connect the hardware wallet to the online computer. While the creators of this device claim a high degree of security using this connection method (if an attempt to read data from the device is made, the device will reject the request), there is always a risk when connecting an offline device to an online (and potentially compromised) computer.

Hardware wallet risks

- Must trust device manufacturer to not have weak random number generator or backdoor method to access the key
- The potential exists (albeit small) for exploitation of device when connected to compromised computer

Hardware wallet risk mitigations

Open-source hardware and software should be required elements of hardware wallets. However, unless a user has the resources to perform physical chip logic verification, always assume a small amount of risk with all security solutions.

Best practices

This section discusses methods to safely use Bitcoin wallets in the enterprise.

Backups

Wallets holding significant funds should be backed up using the "3-2-1" rule: three copies of the wallet file, backed up on two different types of media, with at least one offsite backup. Clients should consider the duration of the intended storage and the lifespan of the media storing the wallet.

Special consideration is required for the backup of non-deterministic (traditional) wallets that hold multiple keypairs. The backup of these wallets only contain the keypairs generated up until the backup time. If the wallet is used after the backup, new keypairs may be generated, and if the wallet file is lost before the next backup, funds assigned to those addresses will be lost.

Encryption of wallet files

Akin to practices used for sensitive data, encrypting your private key is a good idea. A malicious actor in possession of the wallet file would still need to decrypt the keys within to gain access to the funds. Most wallet software has a built-in wallet encryption feature. For the best security, the password encryption method used by the client software should conform to BIP 0038.

Cold storage

Cold storage wallets are never connected to a network. The cold storage wallet stores the larger part of the cryptocurrency when it's not needed.

Deposits can be made to a cold storage wallet at any time, but withdrawals should be relatively infrequent, requiring manual intervention. A "hot" (online) wallet is where smaller and frequent transactions are instead performed. Offline wallets, paper wallets, and hardware wallets can be used as cold storage, depending on how often the funds need to be accessed.

For example, a company holds 6,000 BTC in cryptocurrency. On a daily basis, the company receives approximately 45 BTC from sales, and spends 15 BTC. This means they only need to keep about 20 BTC in their online wallet per day. At close of business, all but 20 BTC should be transferred to a cold storage address. An even better practice is moving all funds into cold storage at the close of business, and moving back only what is required the following morning.

Access controls

Whoever has access to the private key of a Bitcoin address controls the funds. An ex-employee with copies of still-used private keys can transfer funds out of the company's wallets in perpetuity. For this reason, any time an employee with access to a company wallet leaves the company, a new wallet should be immediately generated and the funds from the old wallet transferred to it.

Employee access to the cold storage wallet should be strictly limited by employee role. It is a bad idea to have the company's funds controlled by a single person who might become incapacitated and unable to authorize transactions moving funds out of the wallet. Bitcoin supports the concept of "m of n" transactions, where multiple persons can sign a transaction but not all parties are needed to move the funds. This feature can prevent a single person from either freezing or stealing funds from a company account, and is a highly recommended part of any Bitcoin wallet access policy.

BIP 0070: Payment protocol messages

Malware performing a man-in-the-middle attack on the network may redirect Bitcoin payments by replacing a merchant's Bitcoin address with that of an attacker. An individual with a random-looking Bitcoin address or QR code has a hard time knowing if it really belongs to the merchant.

BIP 0070 adds a layer of authentication to Bitcoin payments similar to that used by secure HTTP. BIP 0070 uses public-key infrastructure (PKI) certificates to validate that a site belongs to the merchant and not an attacker. An additional BIP 0070 feature allows clients to enter a Bitcoin address where any refunds should be sent, as well as notes about the transaction. Implementation of BIP 0070 also allows clients to prove payment of a certain invoice.

BIP 0070 does not address the case where the compromised system is infected by malware that can both change what is seen by the browser and redirect the BIP 0070 transaction being conducted by the Bitcoin client software. If an attacker has malware on the infected system, it is far easier to steal the contents of the wallet instead of intercepting individual payments.

The mitigation is to offer a signature that can be compared against using the public key of the remote party. A verification failure indicates data tampering and would discourage transferring currency to the address being displayed.

The enterprise wallet appliance imagined

The ideal enterprise wallet appliance can be used in the enterprise for secure cold-storage wallet management. This yet-to-be-developed solution would be a secure device that generates type-2 deterministic wallets using random data. The hardware and software of the device would be open-source and auditable by users of the device. The device would support transaction signing via an optical link (i.e. QR code shown to camera, and an embedded display shows signed transaction, or as a static or animated QR code) to transfer transaction data to and from an online-only wallet software. This device would not possess a physical network connection such as USB or Ethernet. The device would be physically secure and difficult to steal. An internal printer could back up the wallet's deterministic seeds to paper using non-fading waterproof ink. The paper seed backups would then be laminated and placed inside tamper-proof envelopes and stored securely in a vault in another geographic location.

Incident response

If a theft occurs, following an incident response plan helps to identify the weaknesses in the system that allowed the theft to occur, as well as prevent the incident from happening again. A good incident response plan includes several steps followed in order, and is ideally documented and understood by all parties involved in the response.

The standard incident response plan outline for cyberintrusions can be extended to a Bitcoin theft incident, because a Bitcoin wallet is essentially digital data. In general, these steps are:

1. Preparation
2. Detection
3. Containment
4. Remediation
5. Resolution
6. Lessons Learned

While recovering funds stolen in an incident is unlikely, it is still useful to activate the incident response process to prevent additional funds from being stolen. More information on network incident response and handling can be obtained from the SANS Institute.

Best practices for exchanges

The proliferation of malware has made online banking risky for many. Malware can inject itself into the web browser and change what the user thinks the bank is asking for. Likewise, malware can alter user transactions to the bank software, intercepting and changing transactions on the fly.

Because it is nearly impossible to guarantee that a consumer operating system is infection-free, all parties should assume the computer is already compromised and work under that assumption when conducting transactions. This doesn't mean that transactions can't be performed under these conditions; it just means that an extra layer of verification is needed for both parties to be assured that no tampering has occurred on the transaction.

OCTV – Offline Cryptographic Transaction Verification

To securely verify a transaction that has transited a potentially compromised waypoint requires an offline device that can display the details of the transaction before it is processed. Public-key cryptography signs the transaction data on the bank's server before it is sent to the user. The offline device can verify the signature of the transaction and determine if any changes occurred in transit. If the transaction shows no tampering, the offline device generates a one-time code that authenticates this (and only this) transaction.

Bitcoin exchange implementation

All Bitcoin exchanges should make OCTV a mandatory security feature. In practice, the exchange displays a QR code when a transaction is requested, especially for an outbound transfer to a wallet. The QR code contains the following data:

- The destination address of the transfer
- The amount of the transfer
- A one-time code generated on the server (for validation)
- A signature of the data that verifies the transaction details

The user scans the QR code using the offline device. The offline device uses the exchange's public key to verify the accuracy of the signature in the QR code. If the signature is valid, the device displays the one-time authorization code, which the user enters into the exchange's prompt, authorizing only the transaction shown in the device's display. It is still incumbent upon the user to verify that the transaction shown matches the transaction desired.

The QR code has the following properties:

- Generated on the server
- Would be entirely unique
- Would only be valid for that specific transaction, globally
- Would be valid only for a small time duration (e.g.: 15 minutes)

Instead of a dedicated device, a smartphone app could be substituted. Because smartphones are both networked and have been targeted by malware to bypass authentication systems, this option should only be considered as a stopgap measure until inexpensive dedicated cryptographic devices can be produced en masse.

An OCTV system called Cronto already exists, works nearly exactly as described above, and has been used at banks worldwide.

Indirect Bitcoin security considerations

Blockchain analysis

At the core of the Bitcoin protocol is the public ledger, known as the blockchain. It allows anyone to look up what funds are owned by what addresses and prevents Bitcoins from being double-spent. But this public record is a double-edged sword for those who want to keep details of their Bitcoin finances secret. For this reason, "tumblers" can obfuscate the flow of Bitcoin funds across multiple users. A user sends Bitcoin into the tumbler's wallet address, as do many other users at the same time. The tumbler then sends the Bitcoins to their original owners at completely different addresses in different amounts at different times, making it nearly impossible to trace a single user's funds in and out of the tumbler (assuming many users are using the tumbler service).

Discussions about the obfuscation of Bitcoin transactions quickly lead to claims of money laundering. There are legitimate reasons to use tumblers, such as protecting sensitive financial information. For example, to gain "inside" information on a company's financial transactions, anyone could analyze the blockchain and determine the cash flow associated with the company's public Bitcoin addresses. They would be able to trace the flow of payments from those addresses to the company's cold storage wallet, and then trace other payments to that wallet, to determine the rate of that company's income. The use of a tumbler, under ideal circumstances, would mitigate this risk. However, tumblers introduce another risk: trusting the tumbler operator for the duration of the transaction.

In the future, it may be possible for tumbler services to operate transparently for regulatory authorities (to assuage claims of money laundering or tax evasion), but that are opaque to would-be opportunist traders.

Denial-of-service attacks

One overarching problem that impacts Bitcoin and e-commerce is distributed denial-of-service (DDoS) attacks. As more companies hold Bitcoin in their portfolio, criminals have an opportunity for quick and easy extortion attacks where they can be paid instantly and the money cannot be traced.

Most of the largest DDoS attacks could be completely neutralized simply by making it impossible to falsify (or spoof) the source of traffic on the Internet. In 2000, Cisco employee Paul "Fergdawg" Ferguson published technical document RFC 2827 showing how ISPs could and should filter spoofed traffic crossing their networks, thus drastically mitigating the effects of DDoS attacks. The need for complete adoption of this recommendation has never been more urgent.

Conclusion

Any enterprise wanting to transact business using Bitcoin must perform careful due diligence to ensure the security of the company's cryptocurrency accounts. The approach discussed in this analysis for wallet security may make handling Bitcoin at the enterprise level more cumbersome than an individual's experience. However, the threat landscape will most likely evolve so that these precautions will be practiced by all Bitcoin users. The general adoption of Bitcoin should ultimately lead to more secure computing and network architectures for everyone.

Recommendations

Wallets

- Encrypt private keys
- Limit employee access to wallets
- Store private keys on offline devices that only serve to sign transactions
- Keep all funds not needed for daily operation in "cold storage"
- Use type-2 deterministic wallets (Electrum, Armory) for enhanced security and availability
- Use secure hardware wallets where possible
- Keep secure offsite backups of wallets
- Implement an incident response plan for wallet theft

Exchanges and web wallets

- Do not use web wallets
- Keep funds on exchanges for as little time as is necessary
- Encourage exchanges to implement offline cryptographic transaction verification

Authenticating payments

- Implement BIP 0070 for customers and vendors