Wealth Security Protocol

Casa's approach to designing key management and wealth security systems, including the chosen features and rejected alternatives to what we've built.

Authors

Jeremy Welch

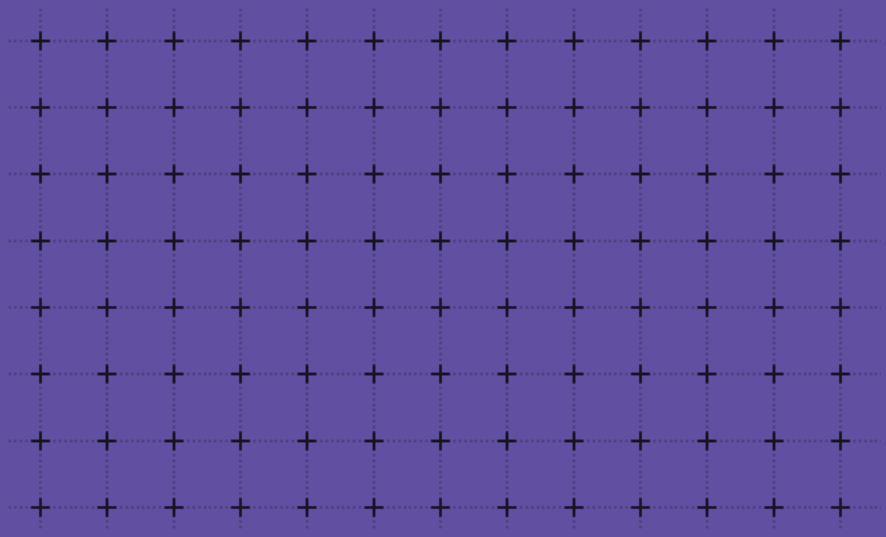
Jameson Lopp

Jacob Lyles

Nick Neuman

Logan Sease

Nick Fogle



Casa

keys.casa

Introduction

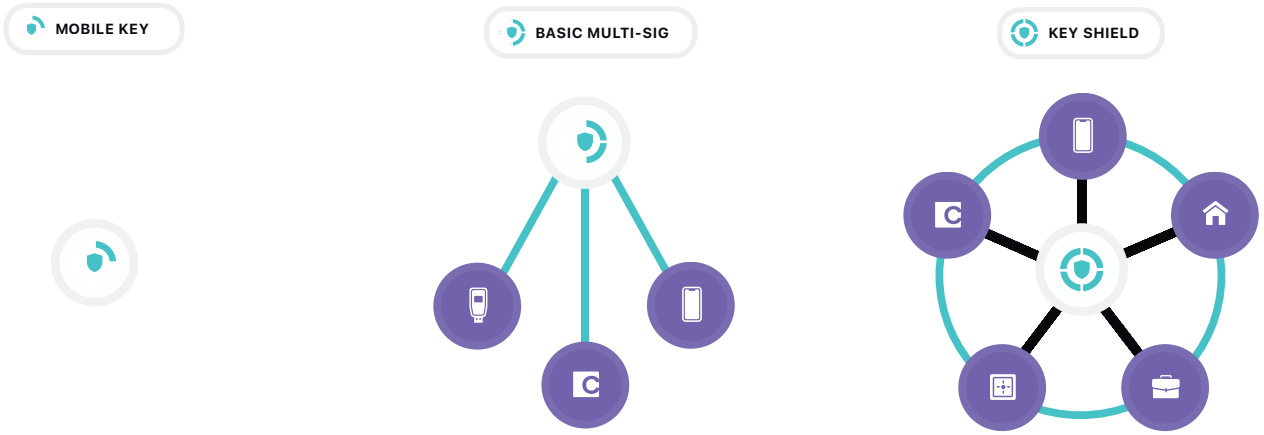
Casa provides security solutions for data wealth, namely Bitcoin.

Our flagship product is Keymaster, a software + expert service system designed to provide the highest level of cryptographic key security and usability.

In this document we outline our approach to designing key management and wealth security systems, including the chosen features and rejected alternatives to what we have built.

The Evolution of Keymaster

Keymaster is adaptable enough to meet most key security requirements.



Contents

Motivation

The same features that give cryptocurrency its appeal make cryptocurrency storage hard.

Most digital coins feature immutable ledgers and lack a central authority to appeal to in case of theft. Bitcoin is a digital bearer bond, like cash. Once sent, a transaction cannot be cancelled or reversed.

These features make the private keys that control a cryptocurrency wallet into an appealing target for thieves. Stealing cryptocurrency keys offers a much more certain and direct route to profit than other information thefts such as email or credit card credentials. Plausible attacks include phishing and social engineering, malware, fake software libraries and applications, malicious hardware, and network attacks. The rise of cryptocurrency marks a new era in information security for personal computing. Never before have the stakes been so high.

The importance of keeping private key information out of the wrong hands makes cryptocurrency owners cautious about where they store backups. They avoid storing backups on unencrypted clouds or common storage devices. But the precautions that protect against theft can open the door to the risk of loss. A failed disk drive, a lost hardware wallet, or a forgotten password can mean loss of cryptocoins with no possibility of recovery.

The storage of cryptographic keys violates the expectations that users might have developed from handling other pieces of sensitive data. If they forget their email password or lose their credit card, there are authorities to appeal to in order to restore their accounts to normal. If their credentials for a website are compromised, they can contact support to freeze their account and restore it to their control. These fail-safes are not available in the world of cryptocurrency.

Cryptocurrency storage requires new habits of thinking and action. With greater control comes great responsibility.

Risks can be separated into the risk of loss and the risk of theft. Some storage features will reduce one risk while raising the other, while others will reduce both.

With Casa's Key Security Protocol, implemented in Casa Keymaster apps and services, we've assembled the best known balance of features available with today's technology to minimize risk of both loss and theft.

Casa vs. Alternatives

Casa specializes in high security sovereign storage systems for bitcoin. Our flagship product, Keymaster app with Key Shield 3-of-5 multisig, was designed for users with large bitcoin balances (from $100k to $1mil and up). This is a challenging market to serve both because it is a tempting target for thieves and the consequences are large in case of accidental coin loss. We have to engineer our products to a high standard of usability, redundancy, and security.

In this niche, Casa competes against several other options.

Option #1: Do-it-yourself

The first alternative to consider is do-it-yourself storage systems, like the Glacier Protocol. These non-commercial options have the distinct advantage of being completely private. There is no need for anyone to know that the user holds cryptocurrency or has set up a storage system at all.

However, the downside comes in usability and support. For example, the Glacier Protocol was designed to serve a similar niche as Casa Keymaster. But in initial testing Glacier took 8 hours to setup and 4 hours to withdraw coins[1]. Even if practice can reduce this time, it still will require time on the order of hours for each transaction. Glacier involves hundreds of dollars' worth of equipment, a complicated process that involves modifying laptop hardware, using the command line interface, and installing operating systems, with no reliable support in case something goes wrong[2].

Casa Keymaster was inspired by the Glacier Protocol. We aim to provide a similar level of high security designed for users with large bitcoin balances. But interacting with the Keymaster system to set up a wallet or to make a transaction takes minutes instead of hours and requires the level of expertise of any normal computer user. If something goes wrong, there is 24/7 dedicated support.

We do need to collect some data on the user to take payment, ship products, and contact them for support. But we are careful to collect the smallest amount of data possible to provide our customers with our services, as outlined in our Privacy and Data Protection Policy. For example, we collect shipping information to ship hardware to our customers, but we delete it after the shipment is made. We also silo customer data internally, so that employees only have access to customer data directly related to their function.

1 Source: author's own experience and memory

2 There are community support forums and channels, but these are strictly voluntary and offer no guaranteed level of service.

It is possible to use Casa pseudonymously[3]. Since we offer a non-custodial service, we are not subject to AML-KYC requirements. In fact, we try to know as little as possible about our customers. That's because holding more customer data increases the risk of attack on our company directly. Additionally, holding more customer data dramatically increases the size of liability in the event of a direct hack or data leak.

In short, minimizing customer data not only protects our customers, it also protects Casa.

One major difference between Casa and open source solutions like Glacier is that Casa is more strongly incentivized to work in the interest of our users. The financial success of Casa is directly linked to our reputation and our yearly customer revenue fee. We succeed if our users succeed, and we fail if our users fail. If our users lose funds, they have no money to pay our yearly service fee. In contrast, open source projects are developed and maintained by volunteers. The developers don't have as much skin-in-the-game. If their users make a mistake and lose funds, they suffer no material penalty.

Option #2: Custodial Storage

Another option for storing your cryptocurrency is a custodial storage solution, such as an online wallet provider like Coinbase or Gemini. This outsources the decisions and effort that are required to secure and backup your crypto balances to a third-party company. Reputable custodial services with good security records are a reasonable option for people with small cryptocurrency holdings for whom it doesn't make sense to invest much time and money into a sovereign storage system.

The cryptocurrency community has a saying "not your keys, not your coins". Many wrongly assume that because a network of third-party custodial banks was the best security solution for the older fiat system, this third party custody model will also work best for cryptocurrencies. But cryptocurrencies have substantially different properties than fiat. In our opinion, the risk of holding coins with a trusted third party is unacceptably high for large crypto balances. Here are some reasons to avoid them:

- A history of loss. Many online services have suffered from hacks and internal theft that resulted in lost funds. This includes well-known and widely-used services. Sometimes, the company has gone out of business and been unable to reimburse their customers for the loss. At the time of the second Mt. Gox hack in 2014, it was the most widely-used crypto exchange. 650,000 bitcoin were lost. Although security practices have improved over time, hacks of market-leading service providers still happen regularly.

3 Casa collects a small amount of identifying information to verify the authenticity of emergency recovery requests

- A big target. Online services run network-connected machines responsible for holding millions or even billions of dollars' worth of crypto. They are under constant attack by clever attackers from all over the world. These attacks come not only from individual hackers, but directly from nation states.
- Phishing risks. Users of well-known online services are prime targets for phishing attacks. Attackers send official looking messages to users asking them to login, but redirecting them to a fake webpage instead of the real thing. These fake websites harvest credentials so that attackers can log-in to their real accounts and drain them. Attacks like this were used to steal 7,000 bitcoin from Binance users in 2019.
- Identity spoofing. Since the administrators of a web wallet service have control over customer accounts, they are a target for social engineering attacks where an attacker convinces the service that they are you[4]. Even reputable exchanges with no publicly-reported security leaks have had users lose funds due to identity spoofing attacks.
- Account freezes and seizure. A custodial storage service has the ability to deny you access to your funds. This might happen for several reasons. Your account could get flagged by automated fraud prevention algorithms. Government agents could choose to confiscate your funds. This might sound farfetched, but precedents exist, such as when Cypress conducted a bank deposit seizure in 2010 or the 1933 seizure of monetary gold in the United States. In times of economic turmoil, seizing cryptocurrency deposits could become appealing to legal authorities.
- Unpredictable fork support. In the case that a contentious blockchain fork occurs, the custodian may only provide you with access to the assets on one branch of the fork if they deem supporting the other branch to be not worth the effort. You will only have full control to redeem and use forks if you have full control of your Bitcoin keys.

Option #3: Other Commercial Sovereign Storage Systems

Casa is not the only company to offer sovereign storage systems for Bitcoin, but we do aim to provide the highest level of usability, control and security for personal and small team self-custody. We pride ourselves on having a highly experienced team and the most extensively tested security model in the market.

Please be careful and do your research. As this product category grows there may emerge companies that claim to provide sovereignty and security to users similar to Casa, but who don't live up to their promises. Remember – if the product is free, then you are likely the product.
The remainder of this paper will discuss the principles, design decisions, and security considerations that go into Casa Keymaster, our flagship key management and self-custody service for individuals and small teams.

4 https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124

System Design Principles

There is no perfect system, but some systems are better than others when pursuing a goal.

When designing a system, trade-offs have to be made between different values, like security vs. convenience, or security vs. system cost. We use the following design principles to guide our decision-making with the goal of building the most secure and usable key system on the planet.

Minimal Knowledge

For the most part, being a company offering a paid service lets us offer a superior user experience with greater security and usability to do-it-yourself systems. But there is a major disadvantage to purchasing a key management service from a commercial entity: you give up personal identifying information. The customer database from a key management service is a valuable collection of data that is an appealing target for attackers.

To counteract this, we collect as little data as possible about our customers. For example, we collect shipping information, but then we delete it after we make the necessary shipments. And our customers can provide us whatever shipping information or email address they want, they are free to be pseudonymous.

We collect only data that is necessary to running the service, as specified in our pioneering Privacy and Data Protection Policy. Unlike many privacy policies, we also specify all the data we don't collect. To the extent that we do collect customer data, we limit access to that data internally to those that need to know it. There is no reason for an engineer to have access to customer contact information, for example.

High Security

The Casa Keymaster system with 3-of-5 Key Shield multisig is designed to protect large Bitcoin balances ($100k to $1mil and up). Since we are securing large balances, our 3-of-5 Key Shield multisig is designed to fill a niche as a premium, high-security product that is more risk-averse than most other competing consumer crypto storage systems.

High security is not "maximum security", and chasing perfect security is a security hazard. More security can always be purchased at a greater cost of money and time. But some of the most involved systems we have seen involve dozens of hours of tedious and error-prone effort to set up. With overly complex systems, there is a danger that users will give up or get lazy momentarily, leaving them less secure. And with added complexity there is increased danger of user error leading to catastrophic loss.

We designed 3-of-5 Key Shield to protect against as many threats as possible while still leaving Keymaster with an excellent user experience.

We consider not only threats that are present now, but threats that are likely to occur in the future. As the popularity of 3-of-5 Key Shield grows and/or the value of bitcoin increases, the incentives for attackers will also increase. Attacks that are uncommon and unprofitable now will become profitable. We anticipate this in setting our security standard.

Usability is Security

This principle is the major differentiator between Casa and high-security DIY protocols. There is a history of security software that fails to achieve widespread adoption due to the difficulty of using it compared to less secure alternatives. For us, usability is a key component of security, not an afterthought. Again, it doesn't matter how secure a system is if nobody uses it.

Another reason why usability matters is that cryptographic systems often have "sharp edges" where mistakes can lead to lost data or loss of privacy. In security software, sharp edges are dangerous and should be minimized. It should be hard or impossible for users to shoot themselves in the metaphorical foot.

Our system can't remove all danger from our users. For example, 3-of-5 Key Shield can withstand two keys lost, but not three. When users do approach a dangerous situation, we warn them and provide mechanisms to recover with the goal of preventing a catastrophic loss.

Expert Support

We can't rely on our customers to be cryptocurrency experts, or even experts in our system. Expert support allows our software to serve a wider range of potential users.

Expert support also helps users through catching edge cases and bugs. Casa does not use invasive user-tracking tools in our software because these tools can be used for attacks. Instead, we've designed a 24/7 support service that quickly captures issues from users, solves the problem, then transfers knowledge across teams and customers to prevent the same issue from occurring again.

This creates a virtuous cycle where expert support captures product feedback for the Design and Engineering teams responsible for updates and new features. The resulting system grows more resilient over time.

Redundancy

An important principle of security engineering is defense-in-depth. There should never be a single point of failure that would allow for the whole system to be compromised.

Redundancy is vital because no matter how much attention a team puts into secure engineering, perfection is beyond reach. Although we limit our use of 3rd party software significantly, we do use some proprietary and open-source systems. Vulnerabilities and bugs are regularly discovered even in fundamental software like operating systems that are developed and supported with multibillion-dollar engineering teams. Our system's security should never rely on its components being bug-free.

Sovereignty

Many popular key storage systems attempt to bypass the user-experience problems involved with managing keys directly by relying on a trusted third-party organization to hold keys.

It's easier to make a custodial product. Development costs are less and timelines are shorter. Centralized key storage also makes it much easier to add features that mimic the existing financial system, which makes it easier to onboard new users..

At Casa, we don't do this for several reasons.

First, as Nick Szabo once said "trusted third parties are security holes". There is a long and dark record of exchange hacks and scams. Even sophisticated and well-funded entities have found themselves victims of malicious actors, both internal and external. Customers of custodial services are also frequent targets of social engineering attacks designed to gain access to their accounts.

A certain big tech company famously had the slogan of "don't be evil". For the crypto-asset space, this motto should be "can't be evil". The only way to ensure this is by maintaining user sovereignty. The user should be the only one who has control over their funds. It should be impossible for the service provider, through malice or negligence, to unilaterally create transactions or block the creation of transactions.

For Casa this is a matter of principle. Bitcoin was created to give people control over their money. Individual sovereignty is the idea that brought us into the cryptocurrency space. We make products for the sovereign individual. This is in Casa's DNA.

Incentive Alignment

Casa as a company is incentivized to help our clients store their funds securely, both by keeping them safe from thieves and by preventing user error. Our users' success is directly related to our commercial success or failure as a company. Open-source storage systems don't have this incentive. They are usually created on a volunteer basis and have no personal stake in the success of their users.

We want it to be clear how we make money and we want our incentives to be aligned with the best interest of our customers. We charge flat, annual subscription fees for our services for this reason.

There is a saying in the software industry that if you aren't paying for a product, then the product is you. "Free" services are inherently untrustworthy. They may change their terms down the line, in which case you don't know the deal you are going to get. Or they collect and sell large amounts of invasive user data for ad targeting purposes.

In contrast, Casa's commitment to incentive-aligned business models allow us to maintain a Privacy and Data Protection Policy that collects and stores as little customer data as possible.

Bitcoin First

Casa is a Bitcoin-first company. Bitcoin not only has the most value secured of any cryptocurrency ($170+ Billion as of this writing), but it also has the most robust and widely used multi-signature system.

The same multi-signature key management system used to store Bitcoin today will one day be used to secure high-value data and other kinds of high-value assets, but that is irrelevant for the foreseeable future. That is why Casa is focused only on Bitcoin and Lightning and other technologies based on these (such as ION decentralized identity).

Threat Overview

Threats to successful key management can be grouped into two categories: threats from malicious actors and threats that come from the inherent complexity of key storage itself. The following is a non-exhaustive list of specific threats that we considered in the design of our Keymaster systems.

Data and Credential Loss

When you forget that fancy password that you are remembering, or discard that old harddrive on accident you may lose access to the keys that control your cryptocurrency. This is another psychologically painful way to lose cryptocurrency, as there is the tantalizing possibility that the keys can be recovered if only the missing data is remembered or found. There are expensive hypnotists that specialize in helping desperate people recover forgotten passphrases.

Mitigation:

- Redundancy: avoid any single point of failure. Forgetting one passphrase should not make a wallet unrecoverable.
- Have a backup recovery plan.

Phishing

Phishing is the practice of tricking a user into using malicious software that is designed to look legitimate. The malicious site may try to harvest credentials, or trick a user into downloading a tampered version of key software. For example, if you are tricked into logging into a malicious website at c0inbase.com, the attacker can then use your username and password to access your Coinbase account.

Phishing is a common practice. Users of desktop wallets like Electrum were attacked with a false upgrade notice, tricking them into downloading a version of the software that steals their Bitcoin.

Mitigation:

- Watch carefully for HTTPS warnings on cryptocurrency sites.
- Always check the URL on cryptocurrency sites.
- Use a multi-signature wallet, which would require the user to be tricked multiple times before fund theft is possible.
- Use a sovereign key storage system that avoids single points of failure.

SIM Hijacking

Another common attack facing individual holders is SIM hijacking. In this attack, the attacker convinces the phone company to port the target's phone number over to another phone (or they pay off someone inside the phone company to do it). Since many websites use SMS to recover accounts when the password is lost, an attacker with control of the target's phone may be able to access some of their accounts.

Mitigation:

- Never use SMS for account recovery.
- Avoid SMS for 2FA. Use hardware tokens or OTP instead.
- Use a sovereign key storage system where no third parties have the ability to spend your coins.

Network Attacks

The internet is a complex set of interconnected systems that can be attacked at many points. MyEtherwallet was attacked through the DNS system, leading users to believe that a fake website was real. This resulted in the attacker walking away with $150,000 in funds. Other network attacks are possible from exploiting server vulnerabilities or configuration errors to gain access to crypto keys.

Mitigation:

- Don't use services with a single point of failure that could result in a high-value honeypot for attackers.
- Use sovereign key management where your keys aren't kept on networked services.
- Never ignore HTTPS error messages on sensitive websites.

Malware

Malware (viruses, trojans, and etc.) that finds its way onto a user's computer can steal crypto keys and send them to an attacker. Malware may be used with another technique like phishing, where an attacker tricks a user into downloading a malicious file with a malware payload.

Mitigation:

- Use a heterogenous hardware and software system for storing your funds, including hardware wallets. This creates a more difficult environment for malware to operate in.

Supply Chain Attack

All key storage software depends on some hardware to run, whether that be a phone, laptop, server, or hardware wallet. There are multiple places where malicious code or hardware can be inserted into the supply chain. Fake hardware wallets have been spotted in the wild. Earlier in the supply chain, malicious chips or

even tainted firmware can be inserted by someone who has access. Keep in mind the attacker might not be the creator of the hardware wallet. The attacker could be a manufacturing partner or a single rogue employee.

Mitigation:

- Always check authenticity of hardware and integrity of tamper-proof seals.
- Do not use only one brand of hardware wallet or software system. Use a mix.
- Use a multi-signature (multi-key) system that will enable recovery even if one of your hardware wallet types is compromised by an attacker or found to have a flaw/bug.

Physical Coercion

Kidnapping, torture, etc. Cryptocurrency faces a greater risk of this than traditional assets, since it is so portable and transactions are irreversible. Although other forms of wealth are harder to transfer, we are beginning to see increased ransom demands of crypto assets from targets who are wealthy from traditional assets.

Mitigation:

- Store keys in multiple locations to increase the difficulty of coercion. The attacker has to steal wallets from multiple locations, require more time and resources and increasing the chance that the attacker will be noticed and caught.
- Plausible deniability with BIP39 passphrases.

Child/Pet Attack

Kidnapping a relative or pet of someone known to have cryptocurrency or other wealth. This is a similar risk for someone who has a large amount of traditional assets, too, and not particularly unique to crypto.

Mitigation:

- Keep knowledge of wealth private if possible.

Internal Service Provider Attack

This is a common source of loss for custodial services. Internal employees often have access to databases and servers hosting the company's keys. The Shapeshift exchange was the victim of one such attack. Other exchanges have been attacked, not by employees, but by attackers that gain access to employee credentials or laptops. Employees are also in the best position to push out malicious software to their unwitting customers.

Mitigation:

- Not your keys, not your coins. Use sovereign products that give you key control.
- Redundancy: your key management system should not depend on trusting a single manufacturer or software. For example, if using hardware wallets, the wallet firmware can provide checks and balances on the provider of your key management software

Platform / Hosting Provider Attack

Software companies regularly rely on third-party platform providers to host code, build servers, web servers, and apps. These can be a source of vulnerability. The Linode web host was compromise in 2012, leading to the theft of bitcoin from several services that were clients of them.

Google's Play Store and Apple's App Store are potential points of failure. They could remove the Casa App from the platform at any time, or potentially be compromised and enable the app to be replaced with malware.

Mitigation:

- Code base is auditable, requires cryptographic signing of every commit.
- Two-man rule required for code commits.
- A system with a mix of different hardware and software provides checks against pieces of the system becoming untrustworthy.

Code Dependency Attack

Attackers have successfully inserted code designed to steal people's bitcoin into popular open-source software packages that are used by some crypto-wallets. The cost of auditing all the code that goes into a system is prohibitive, so this remains an appealing avenue for attacks.

Mitigation:

- Use a mix of different hardware and software for your key storage system.
- Use hardware wallets which have smaller and more carefully-audited code bases.

Official Seizure

This may seem like a far-off possibility. But there are precedents in the legacy financial system. In 2010, Cyprus seized bank deposits to deal with a budget crisis. In 1933, the United States government confiscated all monetary gold from its citizens.

Mitigation:

- If you hold your Bitcoin in sovereign storage, you will at least be able to decide how you respond to an order, rather than having keys and wealth automatically confiscated.

Inheritance Failure

There have been many cases of inheritance failure when a keyholder fails to adequately prepare for his death. The family of Ripple mogul Matthew Mellon lost assets worth $500 million when he died suddenly and unexpectedly without an inheritance plan. To protect his holdings against theft, he kept the storage details of his cryptocurrency wallets secret, but it was so secret that nobody could recover them after his death. This is an especially heartbreaking way to lose cryptoassets, as the surviving family is motivated to partake in painful and often fruitless scavenger hunts in search of the deceased's fortune.

Mitigation:

- Have an inheritance plan. Don't assume that your heirs will be able to recover your funds without guidance.

Chosen Features

The combination of system design principles and threats outlined above lead us to select the following features for Keymaster.

Hardware Wallet Signing

Hardware wallets offer the highest degree of usable security in Bitcoin today.

Hardware wallets are dedicated single-purpose offline computers used only to store private keys and conduct cryptocurrency signing operations. Private keys are generated on the device and never leave it. The devices connect to internet-enabled computers over USB to transfer data and provide signed transactions for broadcast.

Some people feel that paper wallets are more secure than hardware wallets since they are non-electronic and therefore free from direct malware threats. But paper wallets add a host of complexity, taking setup and use time from minutes to hours or even days. Additionally paper wallets can still be affected by malware, since PCs and printers are often used in their generation. Users of paper wallets still must consider supply chain attacks, air-gapping, how to trust the software stack, and side-channel attacks when generating paper wallets.

We use hardware wallets to store the majority of keys and conduct signing operations because it is the best way today to create secure storage systems that are usable by the general public.

Multi-signature

An ordinary single-signature bitcoin key is a single point of failure. If you're securing a large amount of funds, this represents an unacceptably large risk of theft and loss.

No key storage method is perfect. All users of cryptocurrency must assume that they might lose a key to accidental or disaster, or that an attacker will attempt and possibly succeed to steal a key. You might have a sturdy safe at home guarded by a security system. But what happens if your house burns down, or if a close relative that knows your security system decides to steal it?

You could keep backups to make single signature bitcoin keys more robust to loss. But every backup increases the risk of theft, since any one copy is enough to steal the funds held by those keys.

Multi-signature adds resiliency to the system because losing a single key to accident, disaster or theft does

not compromise your entire security. A disaster must wipe out multiple keys, or an attacker must compromise multiple keys, and all at the same time.

A 3-of-5 multi-signature (multisig) system is much harder to compromise than a 1-of-1 single key system. Multi-signature raises the cost of a successful attack by orders of magnitude, since the attacker must gain access to multiple private keys (in our case three), and not just one.

Multi-location

We encourage our users to keep their hardware wallets in multiple locations. A common configuration is storage in separate safes at home, work, and at a bank or private safe-deposit box service. This adds redundancy that helps to protect against both accidental loss, disaster and theft.

Multi-location protects against theft by making the thief's job much more difficult - now they have to visit multiple locations to retrieve a signing quorum of keys. If three keys were kept in one location it would be easy for a thief to coerce a user to giving over their bitcoin. With a multi-location system a single robber with a gun will no longer be successful since the user is not physically capable of handing over their bitcoins. The robber would either have to transport the client under duress to a second location (a highly risky maneuver) or coerce the client into giving up the location details on another hardware device and then break into the second location as well (another risky maneuver).

In a typical Casa setup, the user will have no more than two keys at any one location at a time (at home they would have Home device and the key on their mobile phone). That means the Casa client needs to travel to an additional location to finish signing a transaction with a third key. This adds some friction and cost to using the system, but we think it's worth it in exchange for extra safety and redundancy.

Additionally, by storing keys in multiple locations (and sometimes different cities or countries), users are protected from a catastrophic key loss due to natural disaster. If a hurricane or flood or fire affects the Home of a client, then only 1-2 keys would be lost at maximum, allowing recovery with the remaining 3 keys.

Heterogeneous Hardware and Software (Multi-Device)

In a typical 3-of-5 setup, we use three different hardware/software platforms at one time - currently Trezor, Ledger, and a mobile phone (either iOS or Android). Neither software nor hardware wallets are perfect. From time to time a vulnerability is discovered in one brand. Relying on multiple brands and types of wallets prevents a vulnerability in one brand from compromising the overall storage system.

This also protects against supply chain attacks. If a malicious actor were to infiltrate and tamper with the de-

vices produced by any one supplier, it would not be enough to compromise our clients' funds.

Seedless Hardware Wallets

Most bitcoin wallets ask you to write down a recovery seed and keep it secure when you set up the wallet for the first time. Underlying that seemingly simple instruction is an ocean of complexity. Keeping a recovery seed secure requires expertise and can be a labor-intensive and costly process. If mistakes are made, a recovery seed can make a wallet less secure, since the seed can be used to clone the wallet.

We decided not to use recovery seeds. Hardware devices aren't backed up. Instead, the Keymaster interface makes it easy for a user to swap in a new hardware device for one that is lost at any time. By simplifying the key rotation and wallet sweep process, we have eliminated a whole class of complexity that users have to deal with in other systems.

Emergency Recovery Key

In order to reduce the chance of user error leading to the loss of funds, Casa holds one of the signing keys in the user's multisig setup for use only in emergency recovery scenarios. The recovery transaction is used to transfer the client's funds to a new full keyset.

Casa only will use the Emergency Recovery key after a client has verified private data that they provided to us at setup. This signing of a single Emergency Recovery key must be combined with two other key signatures from the client to complete a recovery transaction. This insures that Casa (or a malicious actor attempting to compromise Casa) can never block or access client funds.

PIN or Biometrics for Mobile Key only

Biometrics provide a convenient and diverse layer of security preventing unauthorized use of the mobile key. A sensor checks the user's thumbprint or face to verify the user's identity before unlocking the app.

We choose not to use biometric locks for every key in the Keymaster system, for several reasons. First, biometric support is not widely used and available for hardware wallets. Secondly, using biometric locks for all of the keys incentivizes kidnapping, since a person's face or thumbprint can be used to forcibly activate the devices. Finally, the collection of biometric data by a third party could be used against a client.

Many clients already use fingerprint or face-scan technology on their mobile phones. Both iOS and Android store this data locally and not in a remote database. We make usage of this technology because it is already available, but we strongly recommend against using biometrics by default without an analysis of the biomet-

ric system's security and privacy.

Finally, always make sure any biometrics you use do not use a 3rd party system. We've heard reports of cryptocurrency apps that use 3rd-party face scan systems (instead of Apple iOS or Android directly on device). This is a security nightmare. If Apple, Samsung and other phone manufacturers refuse to store customer face scan data in centralized databases, you can be sure that you should never trust another 3rd party company with this data.

PIN for Every Device

Both Ledger and Trezor provide the option to lock usage of the devices with short numeric PINs. These provide an essential layer of security against theft so that physical possession of a hardware key is not enough to activate the device. Hardware devices will wipe themselves after a certain number of incorrect PIN guesses, protecting against an attacker brute-forcing the PIN.

Sovereign Recovery Instructions

All Casa 3-of-5 Key Shield balances can be recovered and accessed using widely available open-source software. The instructions for how to do so are sent to each customer when they sign up for Casa. The customer is kept fully in control of his or her own funds. They are never dependent on Casa or Casa tools to access their bitcoin.

Casa Keymaster makes using multisig much easier, but it is important that ease-of-use never comes at the cost of full control or full dependence.

Emergency Lockdown Button

To defend against attacks where the user is physically coerced, Casa Keymaster features an Emergency Lockdown button. Once activated on the mobile app, all functions that depend on the Keymaster app or Casa API will no longer function. This prevents the app from making new transactions or from using the Casa signing portal to add a signature to an existing transaction. The lockdown can only be removed by a customer service representative after the customer requests a removal of the lockdown and the representative verifies the customer's identity.

It is important to note that the Emergency Lockdown can never be used to block a client from making transactions because our clients always control the majority of keys. When the Emergency Lockdown is activated, a client can still access their funds using Electrum or other software.

Health Check

Hardware Wallet and Mobile Phone devices will eventually go bad. Radiation from cosmic rays and general wear-and-tear can damage digital devices slowly over time, corrupting the data stored on them. To prevent this resulting in the loss of funds, we have our clients to periodically run a device health check on all their hardware wallets to ensure they are still working properly. The Health Check process signs a message which does not cost anything to the client, and a history of Health Check signatures are kept under the Detail screen for each key type.

Identity Verification for Account Recovery

In a Casa Keymaster setup, Casa retains one of the keys to provide a signature in case of emergency recovery situations. This is useful to protect clients, but creates a vulnerability if an attacker can trick Casa into signing a recovery request that transfers the user's bitcoin into the attacker's wallet.

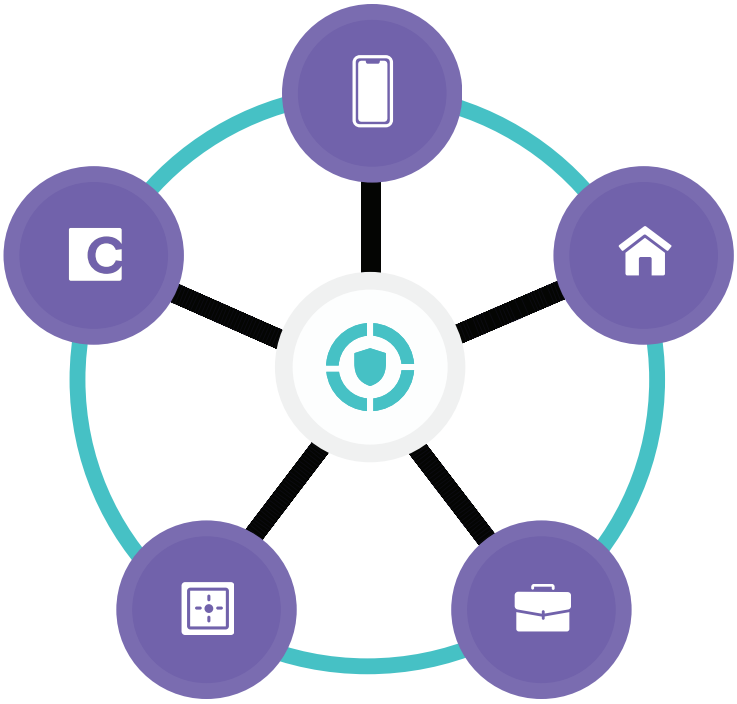
To protect against this Casa verifies the user's identity on all recovery signature signing requests using a special process detailed to clients during activation. We keep details of this process private, but note that the process includes a significant signing delay and a series of regular user notifications when a recovery request is made. The signing delay and notifications increase the odds that an attack would be caught and reversed before the recovery signature occurs.

Chosen Key Schemes

3-of-5 Key Shield

Target Use and Audience

Casa's flagship premium key management scheme is the 3-of-5 Key Shield. It is the highest security product offered by Casa, designed for clients with large bitcoin balances ($100k to $1mil and up) and with the strongest security needs. Like all Casa products, Key Shield is a sovereign storage system. Casa does not have the ability to control the client's funds.



The 3-of-5 Key Shield is Casa's highest-securty offering.

System Details

Three keys are needed to sign a transaction with Key Shield. The five total keys are typically distributed as follows:

- 1 key on the client's mobile phone
- 1 hardware key kept at home
- 1 hardware key at a separate location, such as an office
- 1 hardware key kept in a third location, such as a safety deposit box
- 1 emergency backup key kept by Casa

Features provided with the 3-of-5 Key Shield include:

- Emergency Recovery Service - Casa offers an assisted recovery service in case the client loses two of their keys.
- Mobile Key Backup - An encrypted copy of the mobile key is kept in the cloud storage offered by the client's mobile provider (iCloud or Google Drive). The decryption key is kept by Casa. This allows a client to recover their mobile key if it is lost, for example by dropping their phone off a boat. At the same time, neither Casa nor the mobile provider have access to the key.
- 24/7 Live Support with Client Advisor - Key Shield comes with live phone support from a dedicated client advisor who you know by name. Your Client Advisor can also call in dedicated engineering support to help solve even the most complicated issues.
- Sovereign Recovery Instructions - Casa provides clear instructions for how to transfer funds to a new

wallet at anytime without relying on Casa software. Casa clients get the best of both worlds with a fast, full-support user experience while also maintaining full control.

- Keymaster App for iOS and Android - Keymaster provides a simple, beautiful interface for managing your keys and funds.
- Device Health Check - Periodic healthcheck protects from loss of keys due to bitrot.
- Emergency Lockdown - The Emergency Lockdown button shuts off access to the app and API for a client, preventing unauthorized access. If a client is ever under attack, they can press this button to lockdown their account. Because the client holds most of the keys, the client is never fully locked out of their funds, but without access to our easy to use multisig interface an attacker will be slowed down significantly.

Threat Mitigation

Key Shield is designed to mitigate most sources of theft and loss.

- Disaster - Multi-location key storage + emergency backup reduce risk of loss due to natural disaster such as a flood, fire, or tornado.
- Inheritance Errors - Our highest-tier of service (diamond) offers an inheritance planning package with Key Shield.
- Data and Credential Loss - There are no passphrases or seeds that the client needs to manage. The nature of 3-of-5 provides redundancy that protects against key loss. New keys can be swapped in for lost or compromised keys at any time and very quickly. The emergency backup key and mobile key backup provide additional layers of safety against loss due to user error.
- Malware - Keyshield uses heterogeneous hardware and software platforms (Trezor + Ledger + iOS mobile OS + Android mobile OS) to protect against malware. Four out of five keys are kept offline, preventing remote key theft.
- Credential Theft - Four out of five keys are kept on devices that cannot be accessed through user account credentials alone. The remaining mobile key is guarded by two sets of credentials (mobile account login + Casa login) or two biometric/PIN gates (the phone lock screen and the Keymaster app lock screen).
- Network-based attacks - If Casa's servers were compromised, the client's private keys would still be safe because they are stored offline or on their mobile phone. No private keys are stored on Casa servers.
- Phishing - All the details of signed transactions are confirmed independently on each hardware device, protecting against fake Casa apps or websites.
- Supply Chain Attack - Key Shield does not rely on a single hardware or software vendor, so clients are protected against a supply chain attack. A thief would have to compromise multiple independent supply chains at the same time to attempt an attack.

- Physical Coercion - Multi-location storage mitigates the risk of physical coercion. Clients could still be attacked, but any attacker will need to travel to multiple locations or stay with the client while client travels to multiple locations. The increase in actions, travel and time required to gain access to funds drastically increases the chances that an attacker will be detected and caught. By increasing the cost to attack Casa clients, many potential thieves will be deterred from even attempting an attack.
- Code Dependency Attack - Mitigated by heterogenous software and hardware.
- Official Seizure - Because Key Shield is a sovereign storage system, there is no centralized point that can be attacked for seizure. If officials wanted to confiscate the bitcoin of Casa clients, they would have to go to each Casa client individually.

2-of-3 Basic Multisig

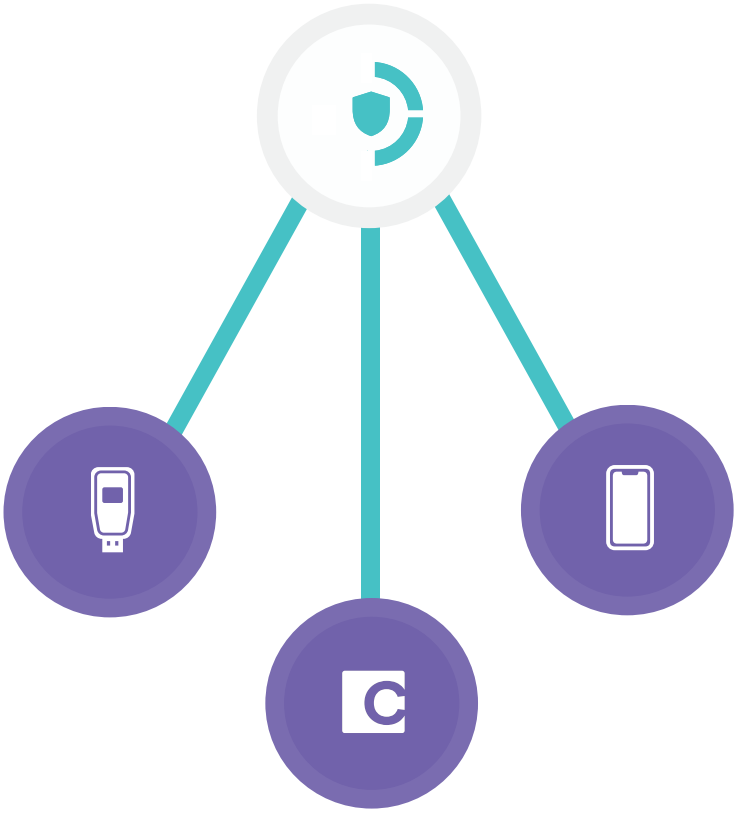
Target Use and Audience

Casa 2-of-3 Basic Multisig is designed for clients holding smaller amount of bitcoin for whom the added cost and difficulty of a 3-of-5 system is too costly. A typical client of the Casa 2-of-3 basic multisig system is expected to hold between $1k and $100k worth of bitcoin.

System Details

Two keys are needed to sign and send a transaction with Casa Basic Multisig. The keys are distributed as follows:

- 1 key on the client's mobile phone
- 1 hardware key kept by the client
- 1 emergency backup key kept by Casa



Casa's 2-of-3 Basic Multisig product is designed for clients holding smaller bitcoin balances.

Features provided with 2-of-3 Basic Multisig include:

- Recovery Service - Casa offers an assisted recovery service in case the client loses one of their keys.
- Mobile Key Backup - An encrypted copy of the mobile key is kept in the cloud storage offered by the client's mobile provider (iCloud or Google Drive). The decryption key is kept by Casa. This allows a client to recover their mobile key if it is lost, for example by dropping their phone off a boat. At the same

time, neither Casa nor the mobile provider have access to the key.
- Email Support - 2-of-3 Basic Multisig comes with email support.
- Keymaster App for iOS and Android - Keymaster provides a simple, beautiful interface for managing keys and funds.
- Device Health Check - Periodic healthchecks protect from loss of keys due to bitrot.

Threat Mitigation

2-of-3 Basic Multisig is designed to provide an intermediate level of security against threats:

- Data and Credential Loss - There are no passphrases or seeds that the client needs to manage. The emergency backup key and mobile key backup provide additional layers of safety against loss.
- Malware - Basic multisig uses heterogeneous hardware and software platforms (Hardware Wallet + mobile OS) to protect against malware. 2 of 3 keys are kept offline, preventing remote key theft.
- Credential Theft - Two of three keys are kept on devices that cannot be accessed through user account credentials alone. The remaining mobile key is guarded by two sets of credentials (mobile login + Casa login) or two biometric/PIN gates (the phone lock screen and the Keymaster app lock screen).
- Network-Based Attacks - If Casa's servers were completely taken over by attackers, the client's private keys would still be safe because they are stored offline or on their mobile phone. No private keys are stored on Casa servers.
- Phishing - All the details of signed transactions are confirmed independently on each hardware device, protecting against fake Casa apps or websites.
- Supply Chain Attack - The hardware wallet or the mobile device alone being compromised would not be enough to steal the client's funds. An attacker would have to compromise both hardware platforms.
- Code Dependency Attack - Mitigated by heterogenous software and hardware (mobile code + hardware wallet).
- Official Seizure - Because Basic Multisig is a sovereign storage system, there is no centralized point that can be attacked for seizure. If officials wanted to confiscate the bitcoin of Casa clients, they would have to go to each Casa client individually

Mobile Key

The lowest tier of Casa storage is a single-key storage system kept on the client's mobile device.

Target Use and Audience

The Mobile Key storage system is designed for beginning clients that have small amounts of bitcoin (<$1k) that do not need more complex and secure storage systems

System Details

The Mobile key storage system is a 1-of-1 system with the single key kept on a client's phone.

Features provided with the Mobile Key system:

- Mobile Key Backup - An encrypted copy of the mobile key is kept in the cloud storage offered by the client's mobile provider (iCloud or Google Drive). The decryption key is kept by Casa. This allows a client to recover their mobile key if it is lost, for example by dropping their phone off a boat. At the same time, neither Casa nor the mobile provider have access to the key.

Threat Mitigation

- Data and Credential Loss - The mobile key backup provide additional layers of safety against accidental loss.
- Credential Theft - The mobile key is guarded by two sets of credentials (mobile login + Casa login) or two biometric/PIN gates (the phone lock screen and the Keymaster app lock screen).
- Stolen Phone Attack - Use of the mobile key in the Keymaster app is protected by biometric identification or a PIN and the phone manufacturer's locking system.
- Official Seizure - Casa does not have access to the client's encrypted key backup, and so cannot be forced to turn over client's funds. However, an authority could force both Casa and the mobile provider (Apple and Google) to turn over information (the decryption key stored with Casa and the encrypted backup stored with the mobile provider) that in combination could be used to access client funds.

Rejected Alternative Key Schemes

Key Sharding (Shamir's Secret Sharing)

Key sharding can function as an alternative to multisig, but after testing we rejected the use of key sharding because it exposes clients to higher security risks.

Key sharding is achieved by splitting a single key into multiple pieces and copies of those pieces, such that some subset of the pieces can be recombined to recover and use the key for a signature and transaction. This key splitting or sharding can be used to provide a similar experience to true multisig.

However, key sharding has many drawbacks that caused us to reject it in favor of multisig.

Drawbacks:

- Single point of failure - The single private key exists on a single device at creation and it is recon-

structed onto a single device in order to sign transactions. If the key is compromised either at creation or during reconstruction, a user's funds can be stolen.

- No key invalidation - With multisig, the user can invalidate a single lost key and replace it. The other keys can be kept and used with the new key to construct a new multisig setup and set of addresses. With key sharding, all the shards must be replaced whenever one is compromised. This makes rapid recovery from an attack or even just a simple system update difficult. All shards/pieces must be replaced each time there is a change to the setup, where with multisig a client can replace just a single key.
- No standard implementation - There is no standard for key sharding. This means that shards made with one piece of software might not be usable with a different piece of software. This locks users into one vendor and compromises user sovereignty. It increases the risk of loss due to user error. It is an obstacle to the use of heterogeneous hardware and software.
- Poor auditability - If a key is reconstituted from secret shares, it's not possible to tell which secret shares were used to recreate the key. Whereas with on-chain multisig, the "identity" of each signing key is stored on the blockchain and can be useful for forensic analysis in the case of compromised keys.

2-of-2

2-of-2 multisig offers some resistance against theft, but it increases the risk of key loss to unacceptable levels. If any one key is lost, the user's funds will also be lost.

Duplicating or key-splitting one of the keys in a 2-of-2 setup can offer improved usability, but the system is still weak against disasters and attacks compared to a 2-of-3 or 3-of-5 scheme.

1-of-2

1-of-2 multisig offers some resistance against loss, but it offers insufficient protection against theft. If any one key is compromised, a thief will be able to steal the user's funds.

Rejected Features

Biometrics General Usage

We use biometrics as an added layer of security for our mobile applications. But we do not use biometric data for all the keys in the key storage system, for several reasons:

Biometrics in isolation can introduce strong incentive for physical attack. For example, an attacker is incentivized to chop off a finger to defeat a fingerprint scanner.

3rd Party Biometric Systems are a security hole. They store the biometric data on the company's servers, which are attractive targets for attack. It's acceptable to use for the phone key because phone providers store face and fingerprint data locally only.

Seed Phrase Backups

Casa does not use seed phrase backups in our storage systems for the following reasons:

While seed phrases reduce the threat of accidental loss, they increase the threat of theft since the seed phrases must also be secured.

Seed phrase backups double the number of sensitive items our customers have to manage and store. In a 3-of-5 system, this would mean 10 items to protect instead of 5.

Financial Products and Services Integration

Casa does not and will not provide financial products because the data collection required to provide financial products is not in the best security interest of clients:

Casa may partner with other companies for financial products, but our technical systems and legal systems will always stay independent.

Any company providing financial services has a much higher attack surface, both from nation state actors, outside attackers and internal attackers. There is more software to secure and more custodial value to protect.

Brain Wallet — Memory Based Solutions

A "brain wallet" is the practice of memorizing a seed phrase that is converted into a bitcoin private key. They present a major risk of theft and loss.

One major problem with brain wallets is a lack of true randomness. Attackers can guess and check many brain wallet seeds quickly in parallel. As of 2016 researchers reported an active community of thieves checking brain wallets for balances and draining them within minutes of creation.

Brain wallets also present a significant risk of loss. Injuries or just forgetfulness can cause a seed to be lost forever. To be of comparable security as a normal bitcoin key, a brain wallet seed phrase has to contain a large number of words, such as memorizing a 12-word BIP39 seed phrase. If any of the words are missing or remembered out of order, it may be hard or impossible to recover.

Web-Based Key Management

A common way of distributing key management software and wallets is by embedding them in web pages. The user can simply navigate to a web page hosting a javascript application that allows them to generate a wallet, view their balances, get addresses, and/or sign transactions. To protect against potential malware, the user can download the page and use it offline on an air-gapped computer.

We decide against using web-based key management for several reasons.

Drawbacks:

- Phishing - Due to the nature of hypertext, it is easier to direct someone to a fake web page than a fake app.
- Browser Privacy - Many popular browser extensions have permission to read and alter every web page a user visits. When a user chooses to trust a web wallet, they are also choosing to trust every extension provider they are using with the security of their funds. Even if the keys are not present on the web page, a malicious extension could alter addresses, showing the user a receiving address that belongs to the attacker.
- Complexity - To protect against malware, a web wallet should only be used on a dedicated single-purpose air-gapped computer. Due to the complexity of setting up an air-gapped system, many users will fail to do so, putting their funds at risk.

Hardened Addresses

Using "hardened" receiving addresses provides some extra security in case of a private key falling into the

hands of an attacker. Hardened addresses prevent other private keys in the wallet from being exposed, limiting the scope of damage from an attack. If the private key corresponding to a regular non-hardened address were stolen along with the master public key of the wallet, the other private keys in a wallet could be stolen as well.

However, there is a trade-off to using hardened addresses. Regular addresses are derived from public keys, but hardened addresses are derived from private keys. So to generate new hardened addresses requires access to private keys. This means either that private keys would need to be kept on our servers or that the client's hardware wallets would need to be accessed whenever they wanted to generate new addresses. Both of these options are unacceptable.

We take a different approach to security. We focus on securing and quarantining private keys on offline hardware wallet devices. Using regular, non-hardened addresses helps us enforce this quarantine since the private keys never have to leave the device and hardware devices may remain idle for long periods of time.

Using non-hardened addresses creates an additional vulnerability in case of an attack which manages to steal one private key from a wallet device, but not others. We judge that such a scenario is unlikely. If an attacker finds a vulnerability in a wallet device that allows them to steal the private key corresponding to one address, it is likely that they will be able to steal the other keys also. This vulnerability is an acceptable trade-off considering the stronger private key quarantine that is available for users of non-hardened addresses.

Remaining Attack Vectors

Address Spoofing

While the Casa system is highly secure, the user still needs to obtain a destination address for each transaction from an exchange or wallet outside Casa's systems. Malware on a user's computer could theoretically cause their web browser or other communication software to display an incorrect address. This would defeat the security of any storage system, as it occurs outside of that system.

Mitigation:

- Use of a mobile app mitigates browser extension based address modification.
- We re-derive addresses independently on both server and mobile device. The app will throw an error if there is a mismatch between server and mobile device.
- Use of Casa's Sovereign Recovery tool allows an external validation of addresses. We are working on improved methods for this secondary check.

Malicious Insider Key Theft

In a typical customer setup, Casa Inc. provides all the hardware wallets (we are an authorized reseller of both Trezor and Ledger). Keymaster phone app is downloaded directly from either the Apple iOS App Store or Google Play Store. If an insider attacker got a customer to install a malicious version of the app and provided the customer with malicious hardware devices, it would be possible for an insider to steal the user's keys.

Mitigation:

- Casa is an authorized reseller of both Trezor and Ledger, so the devices we provide come directly from the manufacturer.
- Casa supports the use of hardware wallets obtained directly from manufacturer or from other authorized hardware wallet retailers.

Extreme disaster scenarios

In a typical Casa setup, the user is instructed to store their keys in separate locations to protect against key loss in case of a disaster, such as at home, their office, and a bank vault. If any one of those keys survives, the user will be able to recover their funds. However, in case of a disaster that destroyed a whole city (nuclear bomb or conventional bombardment, exceptionally large earthquake, tidal wave or major flood, etc.) all three of the keys might be lost.

Mitigation:
For exceptionally large balances, store one key in a different city / state / country.

Extortion

The possibility of a loved one being kidnapped and held for ransom is not directly protected against by our systems. However, this isn't a unique danger to users of cryptocurrency. Anyone known to be wealthy will be subject to the same risk. We attempt to mitigate this risk on our end by collecting as little user data as possible and allowing users to be pseudonymous.

We expect that most wealthy individuals in the world will own Bitcoin within 5-10 years time, so keeping your Bitcoin ownership secret may not even be an option if your general wealth is commonly known in your social circle or city. Any clients with significant wealth should consider hiring physical security to protect themselves and their loved ones.

Mitigation:

- Keep your cryptowealth secret for as long as possible.
- Hire a security consultant to help you improve your home and travel security, and to educate your family about kidnapping risk and mitigation strategies.
- Hire physical security to directly protect you.

Future Improvements

Casa has many future improvements and new features planned for our Keymaster products. We will update this Casa Key Security Protocol occasionally after major feature or technology updates.

There are also several proposed improvements to the Bitcoin protocol that will enable Casa to offer new features for our users.

Taproot/MAST

Merkelized Abstract Syntax Trees (MAST) is an improvement to the bitcoin protocol that will allow for more complex unlocking scripts on the bitcoin blockchain. Taproot is one codename for an upgrade that would add MAST.

While these scripts are available now, there are several drawbacks in the current system that prevent us from using them. First, they add additional size to a transaction, thereby raising the transaction cost. Secondly, using them would compromise user privacy by adding a distinctive format to Casa user transactions on the blockchain that would stand out.

MAST would make complex unlocking scripts look identical and have identical size to simpler ones. This would allow us to add new layers of security for our users. For example, we could offer a 3-of-5 wallet that reverts to a single signature wallet after a few years have passed without spending from it. This would add a failsafe in inheritance scenarios where a user dies unexpectedly and some of their keys are unrecoverable. The single signature fallback could be controlled by the user's estate executor.

Schnorr Signatures

Schnorr signatures will make multi-signature transactions look identical to single signature transactions on the blockchain. This will reduce fees to our users and increase user privacy

Conclusion

Casa aims to offer the most secure and easy-to-use key management system for Bitcoin. In designing our systems, we've carefully considered many alternatives and analyzed many attack vectors. But no system is bullet-proof.

As time goes on, we will remain vigilant in uncovering new threats and will continue to upgrade our systems to reduce risk. As we make improvements to Casa systems to protect our client's security, we will periodically update this protocol document with the details and effects of new features and changes.