Yeti 2.0 Design Document

Yeti is a free and open source software project to make bitcoin more difficult to lose, steal, or extort than any other asset. It's designed to secure amounts in excess of $5,000.

Yeti stores bitcoin private keys on SD Cards. The Yeti wallet has a high security area that requires 5 out of 7 SD Cards to spend and a lower security area that requires only 2 SD Cards (or 1 SD Card and 1 hardware wallet).

After 4 years Yeti decreases the number of SD Cards required to spend, making it nearly impossible to lose bitcoin.

Yeti uses encryption so even if an adversary finds 3 of the SD Cards he will not be able to determine your Bitcoin balance or transaction history.

Yeti also provides the option to pay third party services (Blind Password Servers) for emergency access to your funds or to alert police if you are under duress, but you'll only pay for these services if you invoke them in an emergency.

The software itself is free/libre and open source and relies primarily on Bitcoin Core (the reference implementation and most secure bitcoin node/wallet software).

Instructions

Storage Locations

SD Cards should be stored in 4 different types of locations. These location types are the result of carefully considered tradeoffs between privacy, security, and inheritance planning.

Nickname	Location	Secrecy	Inheritance	Access	Location
Attic	SD Card 1	OK	Bad	Good	Near Home
Home Safe	SD Card 2	Very Bad	Very Good	Very Good	Near Home
Aunt Jane	SD Card 3	OK	Very Good	Bad	100 km away from home and 20 km from 1-4
Caves	SD Cards 4-7	Very Good	Very Bad	Very Bad	100 km away from home and not with each other

Accessible and Easy to Discover

SD Card 1 should be accessible to owners and also likely to be discovered by heirs.

Example Locations:

- Home Safe
- Bank Safety Deposit Box

Secret and Accessible

SD Card 2 should be stored in an easily accessible location that is not likely to be found by heirs in the case of the owner's death. This should be easy for owners to access, but unlikely to be found by anyone searching for your coins.

Example Locations:

- Hidden in an attic inside a wall.
- Underneath floorboards.
- Inside the upholstery in a car.
- Tied to a rope and dropped down an abandoned well on your property.

Secret and Discoverable

SD Card 3 should be in a moderately secret location that is still likely to be discovered by an heir, but not certain to be suspected by anyone looking for your SD Cards. To ensure it is not readily accessible the location needs to be at least 100 km from your home.

Example Locations:

- Place the SD Cards in an envelope labeled “Last will & testament” and placed in the care of a distant relative.
- Ask a trusted co-worker that works in another state to keep an envelope of personal information in his desk.

Very Secret and Inaccessible

The first 4 SD Cards (4-7) should be stored in very secret locations known only to the wallet owner(s). These locations need to be so secret that if the owner(s) die it is likely that these SD Cards won’t ever be found. These locations should normally not be accessed for many years.

Example Locations:

- Buried in a secret location.
- Hidden in the foundation of a building.
- Hidden in a photograph using steganography and then donated to a museum.

Spending Accounts

Yeti contains two accounts so that users can make funds highly secure or more easily accessible.

Immediate Account

This is a 2 of 7 multi-key account. This account allows users to spend funds without any delay using an easy to memorize “Authentication Passphrase” (used to authenticate with Blind Password Servers) and only two SD Cards. SD Cards labeled 5 and 7 are easily accessible to the user.

When you access your Yeti wallet you can enter a “Duress Passphrase.” For example if your Authentication Passphrase is “granite sparkle” you might set a Duress Passphrase that is “fat donut.” Normally you will enter “granite sparkle” to access your bitcoin, but if you are under duress and enter “fat donut” Yeti will automatically send a 1.0 bitcoin bounty and personal information such as your name and home address to the third party services that will notify police.

Delayed Account

This is a 5 of 7 multi-key account. This account allows users to spend with only 5 SD Cards and is time locked until the end of four years. Funds that are not expected to be spent for 4 years should be placed in this account. It is possible to get to these funds early, but that requires sharing personal information with a third party and involves considerable time and expense.

If you want to spend from the delayed account before the end of 4 years you will need to meet with a third party that will verify your safety and the safety of close family members before allowing you to spend bitcoin early. This makes you a significantly less attractive target for extortionists.

Read and Spend Schedules

Yeti uses the smart contract capabilities in Bitcoin to reduce the number of SD Cards required to spend over time. This allows for high security (requiring 5 SD Cards to spend) and very low likelihood of loss (requiring only one SD Card to spend after many years).

Spending Bitcoin Schedule

These are the components required to spend bitcoin from your immediate account and from your delayed account.

Time	Immediate Account	Delayed Account

< 4 years	2 SD Cards + Auth Passphrase	5 SD Cards + 2 Time Machine Spend Keys
4 years 2 months	2 SD Cards + Auth Passphrase	5 SD Cards
4 years 4 months	2 SD Cards + Auth Passphrase	4 SD Cards
4 years 6 months	2 SD Cards + Auth Passphrase	3 SD Cards
4 years 8 months	2 SD Cards	2 SD Cards
4 years 10 months	1 SD Card	1 SD Card

Reading Transactions

This is the number of SD Cards required to read transactions with your Auth Passphrase or if you have forgotten it. This applies to both the immediate and delayed accounts.

Time	With Auth Passphrase	Without Auth Passphrase
< 4 years	1 SD Card	5 SD Cards
4 years 2 months	1 SD Card	5 SD Cards
4 years 4 months	1 SD Card	4 SD Cards
4 years 6 months	1 SD Card	3 SD Cards
4 years 8 months	1 SD Card	2 SD Cards
4 years 10 months	1 SD Card	1 SD Card

Tripwire Account

Each SD Card also contains a tripwire account with .01 BTC each (about $500). The purpose of this account is to encourage anyone that discovers a SD Card to steal this small amount of bitcoin. If this bitcoin is stolen the user will be notified via Yeti that the specific SD Card is no longer secure and that they are to move their funds to a new bitcoin wallet immediately.

This is accomplished using a 1 of 7 multi-key wallet that is unrelated to any other wallets used in Yeti.

Yeti Physical Security Training

During the Yeti setup users watch a series of videos showing home invasions and other relevant physical attacks.

Yeti users won't be likely targets of intelligent criminals because any wealthy non-user of Yeti could more easily be coerced into buying a large amount of bitcoin with less effort and risk than coercing an Yeti user to hand over his bitcoin. This means the primary threat remaining is unintelligent and desperate attackers. The cheapest and most effective defense against unintelligent criminals is a readily accessible handgun. If you are with another person that also carries a handgun your chances of success are increased even further.

Yeti users are encouraged to take additional law enforcement quality training from a school like frontsight.com, obtain an AR-15, dog, security cameras and other practical and cost effective physical security safeguards.

Technical Information

This section is not necessary to understand how to use Yeti, but it will help you understand how Yeti works and the design decisions made by Yeti contributors.

Keys Used in Yeti

Yeti uses two types of keys to prevent unauthorized spending and to preserve your privacy if some of the SD Cards are stolen.

Spend Keys

Yeti uses standard bitcoin private keys to secure your bitcoin - we call them *Spend Keys*. Spend Keys are stored on SD Cards (or hardware wallet signing devices). Each SD Card contains a Spend Key, but all Spend Keys are hidden unless decrypted with 5 *Read-Only Keys*.

After 4 years the number of Spend Keys and Read-Only Keys required are reduced every 2 months so that if a user loses all but one SD Card the bitcoin will not be lost.

Spend Keys Schedule

The number of Spend Keys required to access the bitcoin is enforced by the Bitcoin network itself. After time has passed, transactions will be accepted by the Bitcoin network with fewer and fewer Spend Keys. This is completed through multiple taproot script-path spends.

Time	Number of Spend Keys Required (out of 7)
< 4 years	5
4 years 2 months	5
4 years 4 months	4
4 years 6 months	3

4 years 8 months	2
4 years 10 months	1

Read-Only Keys

In some bitcoin multikey wallets, users are required to store Spend Keys in clear text. This would allow an attacker to read past transactions on the bitcoin blockchain. To prevent this, we ensure that all Spend Keys in Yeti are encrypted with Read-Only Keys, and that you must obtain 5 Read-Only Keys to decrypt any Spend Key. This is completed through Shamir's Secret Sharing.

Read-Only Keys are stored in clear text on each of the SD Cards. There is 1 Read-Only Key per SD Card and additional Read-Only Keys inside of blind, third party servers (Blind Password Servers). Four Blind Password Servers are randomly selected from the available pool of Blind Password Servers.

Read-Only Keys are a 5 of 11 encryption scheme, as there are 7 SD Cards and 4 Blind Password Servers. The Read-Only Keys stored with Blind Password Servers are also duplicated on SD Cards 1-4 (1 per each SD Card). So SD Cards 1-4 each have 2 distinct Read-Only Keys.

If a user forgets their Auth Passphrase and can't find at least 4 SD Cards after 4 years, the Read-Only Keys stored in Blind Password Servers are published to the bitcoin blockchain according to a specific schedule. This means as long as a user retains at least one SD Card the bitcoin can not be lost.

The 4 Read-Only Keys published by the Blind Password Servers, plus the 1 Read-Only Key held in the 1 SD Card remaining, equals the 5 Read-Only Keys required to decrypt the 1 Spend Key held by the remaining SD Card. This allows for the final SD Card to spend your funds after 4 years and 10 months.

Read-Only Key Publishing Schedule

Blind Password Servers publish their Read-Only Keys to the Bitcoin blockchain after a specified amount of time (unless the time period is extended by the user). Once a Read-Only Key is published you no longer need an Auth Passphrase to access it. Read-Only Keys are published at the same time the number of Spend Keys required for the Delayed Account decreases, so you never need your Auth Passphrase to spend from the Delayed account after a predetermined amount of time passes. This also enables you to still spend your bitcoin, even after losing up to 6 of 7 SD Cards, as long as you wait a minimum of 4 years and 10 months (and all 4 Blind Password Servers operate as they should – there is a very strong financial incentive for them to do so). This is because to publish the key, they propagate a pre-signed time-locked transaction that is now valid, which pays them from your account, and publishes the Read-Only Keys to the blockchain for you to see.

Time	Number of Published Read-Only Keys
< 4 years	0

4 years 2 months	0
4 years 4 months	1
4 years 6 months	2
4 years 8 months	3
4 years 10 months	4

Tripwire Wallet

Each SD Card contains a Tripwire Wallet that is a 1 of 7 mutli-key bitcoin wallet loaded with 0.01 bitcoin (about $500). When funds are spent from a Tripwire Wallet users are notified that one of the SD Cards has been illegitimately accessed by a thief and funds should be moved to a new wallet.

SD Cards contain a user experience that encourages attackers to spend the bitcoin stored in the Tripwire Wallet and make it likely that an unsophisticated attacker will never know additional funds exist.

Time Machine Spend Keys

In addition to 5 Spend Keys, 2 of 4 Time Machine Keys are also required to spend from the Delayed Account, if you would like access to your coins prior to the 4 year timelock expiry. These Time Machine Keys are held by the Blind Password Servers and will only be released after the Blind Password Server Operators have verified the identity of the user and that the user is not under duress.

Time Machine Spend Keys Required Schedule

The number of Time Machine Spend Keys required to spend bitcoin is enforced by the bitcoin network. After time has passed, transactions will be accepted by the bitcoin network without Time Machine Spend Keys and they are no longer needed.

Time	Number of Time Machine Spend Keys Required
< 4 years	2
> 4 years	0

SD Cards Used in Yeti

The SD Cards used in Yeti contain different information because users are expected to store them in different ways to make it as difficult as possible for attackers to steal bitcoin or compromise the user's privacy. Each SD Card is also stored with an identical DVD to make data corruption less likely.

On each SD Card there is a “Clear Partition” and an “Encrypted Partition.” The Encrypted Partition can only be read if the user has access to 5 Read-Only keys. Encrypted Partitions are encrypted using a 5 of 11 shamir's secret sharing scheme. 7 of the Read Only keys are stored on each of the 7 SD Cards and the other 4 are stored in each of the four Blind Password Servers. In the event that the Blind Password Servers are not functional the four Read Only keys stored in the Blind Password Servers are duplicated on SD Cards 1-4.

SD Card 1

On each of these three SD Card Yeti stores the following data:

On the Encrypted Partition:

1. A unique Spend Key
2. A copy of the Descriptor
3. A copy of the decryption key provided to the BPS to give access to the name and photo of yourself and your close family when spending early from the delayed account.

On the Clear Partition:

1. A unique Read-Only Key
2. Four random numbers. Each one is hashed with the passphrase and used to authenticate to the corresponding Blind Password Servers.
3. An ID number we can use to see if any of the other Read-Only keys have been published to the blockchain.
4. A pre-signed transaction to reward BPS Operators for responding to your duress passphrase. This is sent to the BPS when the duress passphrase is used.
5. A copy of the decryption key provided to the BPS to give access to your name and address if you use the duress passphrase. This is provided silently in the background when/if the duress passphrase is used.

SD Card 2-3

SD Card 3 in Yeti stores the following data:

On the Encrypted Partition:

1. A unique Spend Key
2. A copy of the Descriptor
3. A copy of the decryption key provided to the BPS to give access to the name and photo of yourself and your close family when spending early from the delayed account.

On the Clear Partition:

1. A unique Read-Only Key
2. Four random numbers. Each one is hashed with the passphrase and used to authenticate to the corresponding Blind Password Servers.

3. An ID number we can use to see if any of the other Read-Only keys have been published to the blockchain.

SD Cards 4-7

On each of these four SD Cards Yeti stores the following data:

On the Encrypted Partition:

1. A unique Spend Key
2. A copy of the Descriptor
3. A copy of the decryption key provided to the BPS to give access to the name and photo of yourself and your close family when spending early from the delayed account.

On the Clear Partition:

1. A unique Read-Only Key
2. A unique copy of one of the Read-Only Keys stored by one of the Blind Password Servers.
3. A pre-signed transaction to reward BPS Operators for responding to your duress passphrase. This is sent to the BPS when the duress passphrase is used.
4. A copy of the decryption key provided to the BPS to give access to your name and address if you use the duress passphrase. This is provided silently in the background when/if the duress passphrase is used.
5. An ID number we can use to see if any of the other Read-Only keys have been published to the blockchain.

Blind Password Servers Used in Yeti

Blind Password Servers provide access to four Read-only keys using an easy to memorize passphrase and they publish the Read-only keys after 4 years if users forget their passphrase. They also provide early access to the delayed account and alert local law enforcement if a user enters their duress passphrase.

Data Stored by each BPS

Each of the four Blind Password Servers hold the following information:

- An encrypted folder that contains the user's name and home address that will become readable with a decryption key provided when the user enters their duress passphrase.
- A unique Time Machine key.
- A unique Read-Only key.
- A pre-signed transaction that pays 0.01 BTC (about $500) to the Blind Password Server Operators that won’t be valid for 4 years and contains the Read-Only Key in the transaction metadata.
- A unique private key used in the 2 of 2 Duress Wallet

Functions Performed by each BPS

Each of these four functions are provided by each of the Blind Password Servers and their Operators.

1. Provide access to Read-Only Keys with an Auth Passphrase

Blind Password Servers allow users to obtain Read-Only Keys using very easy to remember passwords. Four Blind Password Servers are used. Users are expected to memorize a 2 word Authentication Passphrase like “granite sparkle.” All Blind Password Servers have the same passphrase. Blind Password Servers don’t allow more than 10 guesses before permanently locking out the user from future attempts.

With 1 Authentication Passphrase, a user can unlock 4 Read-Only Keys, one from each Blind Password Server.

Blind Password Servers only protect these Read-Only Keys (not Spend Keys), so if those words are guessed or the services are hacked there is no impact unless at least one SD Card is also stolen.

2. Publish Lost Read-Only Keys

At the end of 4 years Blind Password Servers publish the Read-Only Key they are storing to the bitcoin blockchain. This is performed via a time locked pre-signed transaction that pays the Blind Password Server Operator at the 4 year mark, assuming they broadcast the transaction once the timelock expires. They are each financially motivated to with 0.01 bitcoin. This ensures that if the user forgets all of the words in his Auth Passphrase and loses all SD Cards except for one, the bitcoin will not be lost.

3. Alert Police When Requested (Duress Protocol)

Blind Password Servers also hold an encrypted file with personal information about the user including home address. This file is unreadable unless the user is in distress and enters the Duress Passphrase created at setup time.

If the Duress Passphrase is entered, Yeti will send a reward transaction with 0.25 BTC to each Blind Password Server Operators’ Duress Wallet. The 1.0 BTC (0.25 for each server) enter 4 separate, preconfigured 2 of 2 multisig wallets where the user holds 1 key and each Blind Password Server Operator holds their corresponding key.

This locks the funds so that they are only spendable with your approval and the approval of the corresponding Blind Password Server Operator. It also provides the key to decrypt your personal information. When the Blind Password Server Operators are notified that you are being coerced and that a bounty of 1.0 BTC has been sent to the Duress Wallets, they will contact law enforcement and take any other legal and helpful actions they think is appropriate, such as hiring private security to assist local police.

Each of the four Blind Password Server Operators receives 0.25 BTC to the Duress Wallet, and the expectation is that the funds will be distributed amongst the 4 Operators in proportion to their success in helping to rescue the user.

4. Provide Early Access to Delayed Account

Blind Password servers store an encrypted file that they can't read that contains instructions from you and personal information they would need to know to carry out your instructions.

If an emergency arises requiring you to spend funds from the Delayed Account before four years have elapsed, you can activate the Time Machine Protocol, and provide the password to decrypt this file (the password is stored in the encrypted file on each of your SD Cards). The instructions require that the Blind Password Server verify your close family is present and is not under duress before providing early access to your Delayed Account.

This is an expensive service to use and it has a negative impact on your privacy as the service operators will know the personal information required to authenticate you, but it is free to set up and have as an emergency option. As long as it is not used to spend funds early it does not harm your privacy or cost anything.

Once the Operator has authenticated the user they will provide a Time Machine Spend Key used to spend from your Delayed Account early. You will need to do this with 2 Operators. The Time Machine Spend Key is useless without 5 Spend Keys obtained from your SD Cards.

Pre-signed Transactions Used in Yeti

Read-Only Key Publishing Transaction

This is a transaction created at setup time and given to the BPS. This transaction is not valid for 4 years, but it pays the BPS 0.1 BTC ($4,000 USD) and it contains the Read-Only key inside the metadata of the transaction. Normally the user will invalidate this transaction before the end of 4 years, but if the user loses access to his funds this transaction incentivizes the BPS to publish the data he needs to regain access. Each BPS has their own Read-Only key and therefore each has it's own Read-Only Key Publishing transaction for a total of 0.4 BTC. The transactions are staggered so that they do not all become valid on the same day. This gives the user the opportunity to invalidate any remaining Read-Only Key Publishing Transactions as soon as he regains access to his funds.

Additional Achieve Media Used in Yeti

It is unclear how long SD Cards used in Yeti will last, but a decade is probably a safe, lower, estimate. DVDs and CDs are estimated to have a shelf life of over 100 years unless they are stored poorly. Yeti is already very resistant to loss because as long as a single SD Card remains functional the bitcoin can be spent eventually. Additionally, the SD Card that is likely to fail first is the one used most often and failure would alert the user to take action.

However, Because DVDs and CDs are so inexpensive (less than $1 each) Yeti stores all required data on a DVD and a CD for each SD Card with the exception of SD Card 2. SD Card 2 is the only storage location where the small size of the SD Card is a significant advantage because it needs to be quickly accessible to the user and also as difficult as possible to find for an attacker.

Attic Key Utility

Only 1 key (typically SD 1) will function as the “Attic Key”. This key contains special information that will inform arctica it is to be used for constructing transactions. It is also the key which is required to initiate time machine protocol and duress protocol as it contains clear text, presigned txs to be broadcast for these protocols.

An attic key assumes an online connection with a BPS can be established in order to obtain a read key. However, this can be overridden if the user engages in a manual decryption by obtaining 4-5 privacy keys from other SD cards.

In the event a user should lose access to their attic key, they will be required to convert another one of their 6 remaining SD cards into an attic key via a utility program.

Scenarios Considered

These scenarios explain how Yeti addresses various circumstances that have been considered by contributors.

SD Card is Maliciously Replaced
If the SD Card that is easy to access and likely to be found by an heir is replaced the user could be tricked into revealing their passphrase to the attacker. This, along with the stolen SD Card, would give access to transaction history and balance.

However users are instructed to normally boot up with SD Card #5 and then the SD Card 5 OS is the only place the user enters their passphrase. SD Card #5 is accessible, but better hidden from potential attackers.

This does mean that we are more heavily reliant on the safer of #5’s OS than in a typical multisig use, but these instructions only apply to spending from the immediate account. Spending from the delayed account requires 3 other SD Cards that are all booted to independently.

SD Cards are Stolen

If a SD Card is stolen the thief is encouraged to spend the tripwire bitcoin and this will alert the user next time they access their wallet because the transaction will be visible on the bitcoin blockchain and Yeti will display an alert and instructions.

1 SD Card Stolen and User Killed or Jailed

With only a single SD Card, an attacker could be sure that he could eventually spend the bitcoin as long as the user didn't take any action before 4 years and 8 months from setup time. Jailing him or killing him in an attempt to achieve this would be unlikely to succeed because his heirs would likely find 2 SD Cards and have plenty of time to realize that they must move funds as soon as possible.

With only 1 SD Card the attacker does not know how much bitcoin is available to steal. If he gives the victim the opportunity to check, a Duress Passphrase may be used and a bounty issued for help. At 4 years 8 months, a second SD Card would still be required to view the balance.

2 SD Cards are Stolen

A thief with 2 SD Cards can't read the contents without the Auth Passphrase. If he attempts to guess the Auth Passphrase he will probably lock the Blind Password Server before guessing correctly as very few attempts are allowed. This would require that the user obtain the other 4 of the remaining SD Cards to spend from either the immediate or the delayed accounts because he also won't be able to use the Auth Passphrase.

Only 4 are required because one of the remaining 4 will include one of the very secret SD Cards (1-4) and they each have a duplicate of the keys stored with the Blind Password Servers. Only if the user does not properly retire* the Read-Only Keys stored by the Blind Password Server will the Blind Password Server eventually publish the three other Read-Only Keys needed by the attacker to see your balance and transaction history. If the user waits until 4 years and 8 months after setup, instead of extending the timeout after 4 years as instructed, the thief would be able to steal the bitcoin using only 2 SD Cards and the published Read-Only Keys.

When SD Cards are stolen, the user will be walked through the process of moving their UTXOs to a new wallet, so that the pre-signed Read-Only Key transactions held by the Blind Password Servers are no longer valid. This is necessary so that the attackers can't eventually see your transactions or spend your coins.

3 SD Cards are Stolen

If an attacker gains control of 3 SD Cards the owner will not be able to spend bitcoin and the thief will not be able to read the contents of the stolen SD Cards initially. This is because the owner needs access to 5 SD Cards to spend. However at 4 years and 4 months only 4 Spend keys are required so the owner will be able to spend with only the remaining 4 SD Cards. At 4 years and 4 months only 1 Read-Only key has been published by the Blind Password Servers so the attacker still does not have

access to the required 5 Read-Only keys to read the contents of the stolen SD Cards. The owner would then retire the other 3 Read-Only keys before they are published by the remaining 3 Blind Password Servers so the users privacy will not be damaged by the loss of 3 SD Cards.

Because the thief can't read the contents of the SD Card he also can't spend from your Immediate account even though he does possess the 2 SD Cards required to spend (he can't read the contents of those SD Cards).

4 SD Cards are Stolen

If an attacker gains control of 4 SD Cards he will be able to read your bitcoin balance and past transactions when the first Read-Only key is published by the first Blind Password Server at 4 years and 4 months. He will also be able to spend your bitcoin at 4 years and 4 months because only 4 Spend keys are required.

The attacker can also spend from your immediate account without delay.

SD Cards are Lost or Damaged

Lost SD Cards are not as concerning as stolen SD Cards because they won't be used to compete with the user for control of the bitcoin. If 6 SD Cards are lost or damaged the user will need to wait 4 years and 8 months from setup, but as long as the Blind Password Servers function (and publish the Read-Only Keys, which they are financially incentivized to do) the funds will not be lost even in that extreme situation.

SD Cards are stored with identical DVDs to reduce the risk of damage. DVDs are less prone to bitrot and damage, but more importantly having a variety of formats decreases the risk that a bad batch of SD Cards or DVDs could make recovery difficult.

Home Invasion

Yeti users are instructed to have only 2 SD Cards easily accessible so the attacker would need to force you to divulge the location of 2 other SD Cards and your Auth Passphrase in order to obtain a spending threshold of keys.

The attacker would also need to travel to these one or two additional offsite locations to obtain more than the 2 SD Cards which are easily accessible to you.

While only the 2 SD Cards easily accessible to you and your Auth Passphrase are required to spend from your Immediate Spending account and to see your transaction history and balance from your Delayed Account the attacker will need to wait 4 years before he can spend the funds unless he brings you and your family to a Blind Password Server Operator and somehow deceives them into believing you are not under duress.

Unfortunately once the attacker obtains 4 SD Cards he will eventually be in control of your bitcoin.

In order for the attacker to view your bitcoin balance to determine if obtaining a total of 4 SD Cards is worth his trouble, he must enter the Auth Passphrase. At this point the user can provide the Duress Passphrase he created during setup. The attacker has no way to verify that the Passphrase given is the Duress Passphrase before it is entered and processed by the Blind Password Servers, but when the Duress Passphrase is used the Blind Password Servers lock the Read-Only Keys and receive a 1.0 BTC bounty to assist the victims along with enough personal information to make assistance from law enforcement and private security possible.

Unexpected Death of Owner

If the owner dies and the heir is completely uninformed, the heir should discover at least 2 SD Cards. After the timeout period any one SD Card will be able to read the Spend Keys with the included Read-Only Key and the 4 Read-Only Keys that will be published on the bitcoin blockchain by the Blind Password Servers. As long as 2 SD Cards are recovered, one Blind Password Server can fail and the heir will still gain the required 5 Read-Only Keys.

If one SD Card is recovered by the heir and the other is lost he will only be able to spend the bitcoin if all 4 Blind Password Servers function correctly. They are financially incentivized to do so with significant bitcoin rewards which they only recieve by successfully publishing the Read-Only Keys. However, in this circumstance if even one Blind Password Server fails to do so the funds are lost.

If the heir and an attacker retrieve one SD Card each, neither will be able to spend until both are able to spend the bitcoin. For example, if a corrupt lawyer is holding one key he has equal access to the funds as the heir, but he is not likely to be able to retrieve the funds if the heir becomes informed during the timeout period. They are in a relationship of mutually assured loss unless they negotiate a deal together.

Evil Blind Password Servers

Extorting the Uninformed Heir

A single evil Blind Password Server can’t do anything, but if two of the Servers are operated by the same person or they collude together, they can extort an heir for their bitcoin by failing to publish their Read-Only Keys after the timeout period. However the heir has no way to interact with the Blind Password Servers outside the calls made by Yeti, therefore coordinating the extortion would be difficult and the moment the transaction becomes valid the Blind Password Servers are incentivized to publish the Read-Only Key to gain the bitcoin reward in the transaction that could become invalid at any moment.

Blind Password Servers also don’t know the status of any bitcoin they help secure because their Read-Only Keys are never used in any on-chain bitcoin transaction. They could assume that if a Read-Only Key is not accessed for a long time after being accessed regularly the user is dead, but they

have no information that could help them contact the heir. The IP address of the user is obscured by the use of Tor. By logging access events they may be able to guess the user's time zone.

Extorting the Owner after 4 years without SD Card loss

The Blind Password Servers don't know enough to contact the user and if they somehow discovered the user's identity they don't have significant leverage. Only 5 Read-Only Keys are required of the 11 total and each Read-Only Key held by a Blind Password Server is duplicated on SD Cards 1-4.

Extorting the Owner before 4 years without SD Card loss

If the owner needs to access their bitcoin before 4 years they need assistance from 2 of the 4 Blind Password Server Operators and will need to expose their name and photos and the name and photos of their close family members to the Blind Password Server Operators.

If a Blind Password Server is evil he could attempt to extort the owner before providing access to the time machine key they hold, however as long as at least 2 of the 4 Blind Password Server Operators are satisfied with the $10,000 they will receive as payment the owner will be able to ignore extortion demands. If 3 of the Blind Password Server Operators collude to extort the owner the owner retains the option of simply waiting until 4 years when they will no longer need the time machine key to spend.

Extorting the Owner after 4 years with SD Card loss

After 4 years the Blind Password Servers are only needed if more than 3 SD Cards are lost. Any 4 SD Cards contain the 5 required Read-Only keys. If the owner does not have access to 5 Read Only keys because he only has 3 SD Cards and two of them are not SD Cards 1-4 he becomes dependent on the Blind Password Servers publishing their Read-Only keys. The owner has no way to contact the Blind Password Servers to foolishly inform them that they are dependent on this service and open themselves up to an extortion attempt and the BPS has no way to identify the user to extort them. The BPS is incentivized to publish the Read-Only keys to obtain the reward transaction they were provided at setup time as soon as the transaction becomes valid (and before the user might invalidate it). The BPS is also incentivized to publish the Read-Only key immediately because if they delay for 2 months the next BPS will be able to publish their Read-Only key and once the user regains the ability to spend he will invalidate the transaction.

Compromising Privacy with One Stolen SD Card

If an evil Password server has access to one SD Card he will be able to crack half of the Password and reuse it with one of the other Password servers. This is because the Password has two distinct words such as “granite sparkle” and the first word is used with the first 2 Password servers and the second word is used with the second 2. So an evil Password server with 1 SD Card can get to 3 Read Only keys. The first is on the SD Card in clear text, the second he can get by looking at the metadata in the Read-Only Publishing Transaction he holds and the third by cracking the part of the Password used to authenticate to his server. He can crack this portion of the Password because the salt used with this portion of the Password is hashed together to authenticate the user to the Password server. Because the Password server has access to the resulting hash used to authenticate the user and the salt from

the SD Card, he can brute force the portion of the Password required to create the matching hash. Once he has the Password he can use the salt on the SD Card with the Password to authenticate with one of the remaining 3 honest Password servers. However, with only 3 Read-Only keys the evil BPS still can't read the wallet.

Compromising Privacy With Three Stolen SD Cards

If an evil Password server gains access to 3 SD Cards (Home Safe, Attack, Aunt Jane) he can read the contents of the wallet (see Compromising Privacy with One Stolen SD Card for details). The attacker would still be unable to spend bitcoin, but he would be able to see the balance and transaction history.

Compromising privacy with a single external DVD drive swapped between machines

This is a thing that might happen.

Grief Attack

Any SD that is storing a pre signed & clear text duress transaction, poses a risk of being grief attacked. If a bad actor discovers this transaction, they could broadcast it and at most cause a risk of losing those funds, (the funds would now be in control of a BPS operator who would follow duress protocol) and at least cause a temporary loss of access to those funds.

Design Priorities

- An Yeti user should be less attractive to extortionists than other potential victims, all else being equal. Other potential victims can convert their wealth into Bitcoin within a few weeks. Yeti users will have their wealth encumbered for longer and have more safeguards than someone storing their wealth in stocks or other physical assets.
- Compromises are made in the following order.
    - Compromise inheritance to the uninformed heir first.
    - Compromise immediate account security second.
    - Compromise transaction history and balance privacy for both delayed and immediate accounts third.
    - Compromise delayed account security last.

Hard Engineering Tradeoffs

- **You can't use join market for onchain privacy without exposing transaction history on an online device.**
    - Spending and receiving through join market is the current best practice for on chain privacy. This is particularly important for legacy yeti users that have an unusual 3 of 7 multisig that was created pre-taproot, but without any mixing it is trivial for someone to know you have a significant amount of bitcoin if you pay them anything. But join market

requires coordinating transactions with other users so it must be online and this means that that online wallet is subject to physical snooping if the device is stolen. This can be mitigated by moving between join market wallets and ensuring no trace of the previous wallet is left on the online device.

- **You can't make a location very secret and easy to access.**
    - Even with something like steganography, regular access degrades the security of a storage location. It is better to make the highest security locations rarely accessed by the user. If an attacker knows that you have keys you need to access regularly, the potential hiding places of those keys are greatly reduced.
- **You can't make it both safe for an uninformed heir and difficult for an attacker with the Auth Passphrase to read your balance.**
    - Yeti has chosen not to protect the knowledge of amounts of bitcoin from an attacker that gains one SD Card and the Auth Passphrase. If more than one SD Card and the Auth Passphrase is required to view bitcoin transactions then more than one SD Card will be required for a loved one to inherit your bitcoin. Since there are only two SD Cards that are available to be discovered by an heir, it is important that only one SD Card is required (after the timeout period expires). Already this requires that at least 3 of the 4 Blind Password Servers function correctly and publish the Read-Only Keys at the end of 4 years.
- **You can't make it both safe for an uninformed heir and difficult for an attacker to gain ownership of your bitcoin using only easy to find SD Cards unless you take action to extend the time decay period.**
    - Yeti has chosen a long timeout period (4 years), but if an heir (or an attacker) gets control of a single SD Card and the owner does not take action to extend the time decay period the attacker will gain control of the bitcoin.
- **You can't give an uninformed heir the ability to spend from easy to find keys and prevent a corrupt local government from gaining the ability to see your bitcoin balance using only easy to find keys without involving third party services.**
    - Yeti has chosen to use Blind Password Servers that are operated by reputable, but pseudonymous bitcoin advocates with services operating over Tor. This harms inheritance if the Blind Password Servers don't disclose keys after the timeout period and harms privacy if the Blind Password Servers don't keep keys secret until the timeout period expires. Blind Password Servers are paid well for disclosing the Read-Only Key after the timeout and identifying their operator is difficult because the services are only identified by a public key (the link between the pseudonymous bitcoin advocate and the public key is only known to Yeti contributors that place the public key on the allow list). Publishing Keys before the timeout period would remove future revenue from Blind Password Server operators as their public key would be removed from the allow list.
- **You can't have a node online constantly for quick spending, use your own node for privacy and keep your node locked away from physical attackers.**
    - There might be mitigations to this one, such as encasing your node in concrete, but even then whatever computer you physically interact with isn't going to be trustworthy. But we shouldn't give up on this one yet.

- **You can’t receive bitcoin without 1. Authenticating with the BPS or 2. Manually decrypting with 4-5 SDs**
- **You cannot sign a PSBT with an offline machine unless you are willing to transfer over read only keys on transfer SD which is a significant privacy hit**
- **Can't offline sign and have access to duress protocol**
  A user is at their greatest risk when intercepted by a sophisticated attacker who thoroughly understands the arctica protocol when signing a PSBT at SD 2-7. This is because the user is less likely to have immediate access to the duress protocol. To mitigate this, we can include the Duress TX on the transfer CD, but the user would still need to have a network connection to initiate duress protocol.
  Additionally, a sophisticated attacker who intercepted a user at this point, could use the attic key utility to create a new attic key with SD 2-7 and also have access to the user’s read key and attic key.

Terms/Glossary

Authentication Passphrase - Memorized by the users. Used to authenticate with the Blind Password Server to access Read-Only Keys.

Blind Password Server - An anonymous third party entity with a blind relationship to the user. Holds encrypted Personally Identifiable Information, a Read-Only Key, and a Time Machine Spend Key. A financial incentive to participate fairly.

Blind Password Server Operator - A pseudo-anonymous entity that provides blind emergency services & Read-Only Keys over TOR via a Blind Password Server.

BPS Auth key - the key that authenticates the user with the BPS

Descriptor - The information required by Bitcoin core to construct the transactions to spend from a multi key wallet. Contained on every SD Card.

Duress Passphrase - An emergency passphrase that activates a distress protocol with the Blind Password Servers.

Duress Wallet - A 2 of 2 multisig wallet only funded when Yeti receives the Duress Passphrase. Each of the 4 Blind Password Servers hold 1 of 2 keys to a single Duress Wallet and the user holds the other 1 of 2 keys for all 4 Duress Wallets.

PII Key - The key used to decrypt the PII folder held by the BPS

Read-Only Key - The keys used to decrypt information contained on a SD Card. Held by Blind Password Servers and SD Cards. A minimum of 5 are required to decrypt Spend Keys and Descriptors.

Spend Key - The key used to sign for part of a multisignature Bitcoin transaction. Encrypted. One per SD Card.

Time Machine Spend Key - Used to unlock the timelock. Does not work without 5 Spend Keys. Encrypted and held by the Blind Password Servers. Can only be obtained by going through expensive and cumbersome means.

Transfer key - the key held on each SD 1-7 that decrypts information on the transfer SD

Tripwire Wallet - A clear text Bitcoin Private Key with a small amount of money used to entice a criminal who illegitimately obtains a SD Card into betraying their acquisition.

Trusted Heir/User - Someone who knows the locations of SD Cards 1-4 and may or may not know the Auth Passphrase. This person could spend the bitcoin without anyone else's permission.

Uninformed Heir - Someone that does not know anything about bitcoin storage locations, but should inherit the bitcoin if the owner(s) die. Examples include the very young or the very old.

FAQ

Why Use Read-Only Keys. This is not a standard part of bitcoin core?

Unfortunately the bitcoin seeds and private keys and descriptors reveal transaction data even if only one is discovered by attackers. To fix this, Yeti encrypts this data on each SD Card and requires 5 Read-Only Keys to decrypt it. This provides excellent privacy, but if only one Spend Key is required to spend after 4 years, but the Spend Keys are encrypted with 5 Read-Only Keys, the user would still need to obtain 5 SD Cards to spend after 4 years.

To achieve a better balance between privacy and the risk of loss, Yeti uses Blind Password Servers (a fork of Blockstreams FOSS Password Server), to allow users to access Read-Only Keys with a memorized Auth Passphrase. And if the Auth Passphrase is forgotten by the user the Blind Password Server publishes the Read-Only Key to the bitcoin blockchain - in this case, the user only needs one SD Card to spend his bitcoin after time decay reaches completion.

Why use Hardware Wallets? Is that not against Yeti's Philosophy?

We still believe that hardware wallets have their fair share of security issues (https://robertspigler.com/in-defense-of-my-attack). However, they are still commonly requested. In an attempt to not fall into the trap of security nihilism, we believe allowing 1 HWW doesn't degrade the security of this protocol fatally, and introduces many more users to a much more secure private key management scheme.

Why include DVDs and SD Cards?

As mentioned, DVDs are less prone to bitrot (data degradation).

All discs go through something called disc rot, which is the tendency of optical discs to become unreadable due to physical and/or chemical deterioration. This is usually due to one or more of the following: oxidation of the reflective layer, physical scuffing and/or abrasion of the disc itself, reactions with contaminants, ultraviolet light damage, or de-bonding of the adhesive used to adhere the layers of the disc together.

DVDs have a different structure from SD Cards. In SD Cards, the reflective layer is typically aluminum (reacts with many chemicals), and is immediately beneath a thin protective layer. In DVDs, a plastic disc covers each side of the reflective layer, sandwiching it. Therefore a scratch on either surface of a DVD is not as likely to reach the reflective layer and exposite it to contamination.

In addition, the larger capacity of DVDs allow for computer programs such as DVDisaster to be used, which enhance data survivability by using error detection and correction data.

Implementation Notes:

- We need to encrypt all PSBTs so that they are unreadable until they are opened on the next device for signing. This can be done by encyrpting each 6 times (once for each of the SD cards remaining) and by having a unique decryption key on each SD card. We should also sign the PSBT to make sure it isn't tampered with.
- Minimum Funds must be kept in the immediate account (though maybe some can be in the delayed account) in order to properly incentivize the BPS Operators to perform their functions. These UTXOs need to be tracked by Yeti and users should be warned, and need to accept multiple warnings, before spending these.

- For the Read-Only Keys to decay the UTXO can be spent if 4 years have passed and it's signed by key A or it's signed by key B. Key B is the user. Key A is also the user. User pre-signs a transaction with key A and sends it to BPS. The user still can sign with key B at any time.
    - Spending Conditions
        - Sign with key A AND 4 years have passed.
        - Sign with key B
    - User of Yeti retains both key A and key B.
    - User signs a reward transaction sending money to the BPS using key A (so the transaction is invalid until 4 years pass).
    - If the user doesn't lose access to his wallet he can use key B to move the funds making the transaction sent to the BPS invalid. BPS will notice the transaction is no longer valid by looking at the blockchain and discard it so that the meta data is never published. User can send BPS a fresh reward transaction to reset the clock for 4 years.
- To make sure a forked version of yeti can't be used or local debugging could be used to determine that the duress Password is used the Passwords are selected at setup time and the Password server knows what Password is duress and what is the normal Password. Local code simply relays the Password provided by the user so there does not need to be any local decisions made based on the Password provided. After the Password is sent we also need to send the reward transaction and the key to decrypt the private information so that could be avoided, but the Password servers will still lock out access no matter what happens to the local code if the duress passphrase is provided.
- When we sign a PSBT we also need to encrypt it and stego it so that it is as safe for transport as possible. We should ask the user to provide a few dozen photos at setup. We will encrypt each PSBT 6 times with a public key for each of the other SD Cards.
- We can allow SD Card 7 to be a hardware wallet for signing purposes. We should make this an optional step after the normal setup is completed. SD Card and DVD will still be used to store the seed so we don't need to be concerned with bitrot.
- This is still a good option for smaller amounts as long as we can communicate in the UI that for smaller amounts it's fine not to use the delayed account or to have a reward transaction for using the duress passphrase or even the tripwire account.
- We should have look at having presigned transactions so we can extend the 4 year time lock without having to retrieve any of the 4 high security SD Cards.
- When receiving a payment we should minimize trust on the online node. Maybe a list of valid deposit addresses are on each SD Card and cross referenced. This is more important after initial setup where attackers might have physical access to the online node. This is mitigated by full disk encryption, but if the whole disk is maliciously replaced it doesn't help. Bad guy physical access means it's no longer trustworthy.
- Users will always boot from SD 1, create and sign the transaction and place it on the temp CD along with the 4 BPS read only keys, boot and sign on one additional SD for the immediate account or 4 additional SDs for the delayed account and then return to SD 1 to broadcast the transaction. This allows SD 1 to be the only one that has an internet connection for use with the BPS.
- When users enter their Password they must enter it twice and we won't attempt login unless they match. This will help them remember their password by tyPasswordg it twice, but more importantly they will have fewer failed guesses due to tyPasswordg mistakes we need to allow for. After the first

failure we tell them to get to a private place because their Password will be shown on screen and from there on all attempts are on screen attempts. Increasing periods of delay from 30 seconds on first failure to 5 minutes on last attempt (only enforced locally unless that is already built into the blockstream Password servers server side).

- When accessing the immediate account we should suggest a donation to the Password servers. The suggested donation should be 20k sats and we can locally keep track of how many months have passed since the wallet was created so that people can donate a year or two in advance to save network fees.
    - We should pay the donation to the same address as the read only publishing transaction and timelock it so that the Password servers have guaranteed rewards for not losing the private key that is needed to retrieve their read only key publishing transaction. If we can think of a way to make the donation also dependent on retaining that read only reward transaction itself we should implement that, but it might not be possible.
    - Donations should be made to a new bitcoin address each time and this will create additional incentive for the Password servers to be online (in order it get donations). In other words we won't save the donation address and reuse it because this is bad for privacy and also bad for uptime incentive. If the server is not online we mark the donation as made and the server misses out.
- The transaction that rewards BPS operators for responding when a user enters their duress password is only stored on SD 1. This is to make it less likely someone finds an SD card and broadcasts that transaction to simply be malicious. This also makes it easier to setup the duress protocol as a "nag task" after initial setup because the transaction does not need to be stored on SDs that are not always easily accessible. But this does mean we need to remember to include re-creating thing transaction in the SD 1 recovery utility.
- All data placed on the temp CD is encrypted so that it can only be read using a key stored one of the other SD 6 SD cards.

Setup Procedure

1. Create Ubuntu install thumb drive on daily driver laptop.
2. Install Ubuntu on primary laptop.
3. Install Yeti on primary laptop.
4. Create SD cards 1-7 on primary laptop. Includes Ubuntu, bitcoin core.
5. Boot 1,2,3,4 on secondary, generate SD keys, bitcoin seeds, export pubkeys for both in clear text to setup CD.
6. On primary SD 5,6 and generate SD keys, bitcoin core HD seeds and export pubkeys to setup CD in clear text.
7. On primary boot SD 7.
    a. Generate SD keys & bitcoin core HD seeds & export pubkeys to setup CD in clear text.
    b. grab pubkeys for 1,2,3,4,5,6, 7 from the setup CD.
    c. Generate public key descriptor for the wallet(s).. Encrypts it to SD card pubkeys.
    d. deletes all unencrypted pubkey data setup CD & destroy setup CD
    e. Insert transfer SD
8. Boot each SD card and feed it the descriptor using the transfer SD. Make CD / DVD backup disks.

Open Design Issues

- It would be helpful if an attacker could not determine that two SD cards were for the same owner unless he had 5 of them or the Password.
    - CDs may have microdots from the CD drive that could be used to correlate the two. DVDs probably don't have this problem, but having two different optical formats is great for fault tolerance.
    - We have an ID number that we use to scan the blockchain for published read-only keys. We can place 7 IDs in each transaction so that each SD card only contains one matching ID in each of the 4 transactions that will be published. This prevents knowing that they SD cards match one another until after the 4 year period expires and the other SD cards haven't been used to reset the wallet.
    - Fingerprints, the brand of CDs, DVDs and SD cards all matching and more importantly the storage locations and the fact that the attacker has already discovered two locations probably means that the attacker already knows the are a matching set.
    - The way that they are stored is also probably a tell that they are a matching set. Do they have the same color envelopes? Is the paper equally discolored from age?
    - Until Yeti becomes very popular (it might not ever since most people today don't have enough savings to justify more than a phone app in effort) it will be obvious they are from the same wallet.
    - Version updates to Yeti are inevitable and might result in changes to the unencrypted data that could reveal the same version and therefore likely from the same owner.
    - A pre-signed transaction to reward BPS Operators for responding to your duress passphrase. This is sent to the BPS when the duress passphrase is used. This could be made unique by generating a new transaction for each SD card if it was also paying to a unique address owned by the BPS.
    - A copy of the decryption key provided to the BPS to give access to your name and address if you use the duress passphrase. This is provided silently in the background when/if the duress passphrase is used. This could also be made unique if 7 encrypted packages were provided to the BPS instead of just 1.
    - We probably can't do this with a tripwire account unless we duplicate the amount across all of the locations. Instead of $500 total it would be $500 per SD card.

V2 Design Ideas:

- Allow users to make updates to their PII package should they wish to change their encrypted folder used for the duress protocol & time machine protocol.