#SmartCustody Workshop

San Francisco, January 28th, 2019

Agenda

9:30am: Registration & Coffee
10:00am: Introduction and Fundamentals
10:30am: Simple Cold Storage Scenario & Checklist
11:00am: Digital Asset "Adversaries" and Case Studies
12:00pm: Lunch (provided)
1:00pm: Intro to Digital Asset Risk Modeling
1:30pm: Demo of Self-Custody Digital Risk Model
2:00pm: Demo and live discussion of various digital asset wallets and custody hardware
2:30pm: Break
3:00pm: Salon to address open questions/missing requirements
4:00pm: Close

Intro

What is #SmartCustody? About this workshop. About your faculty.

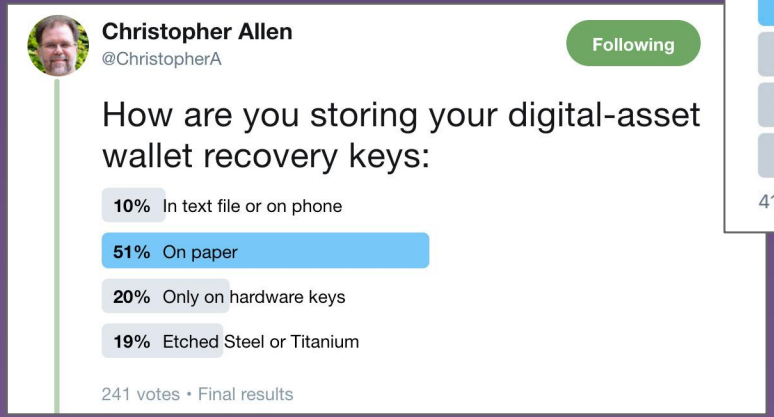
#Smart Custody

“The use of advanced cryptographic tools to improve the care, maintenance, control, and protection of digital assets.”

Our goals:

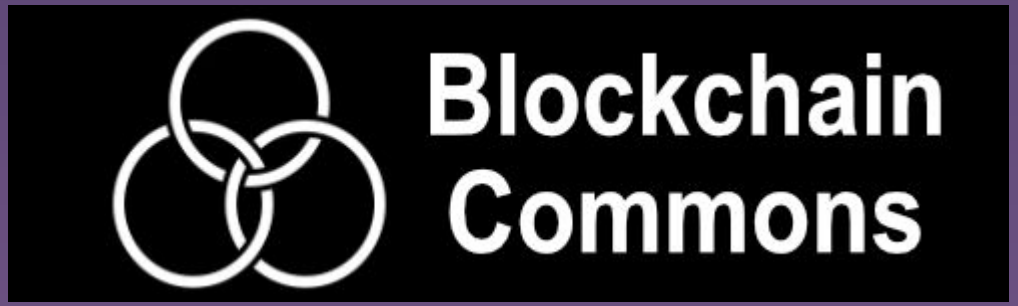
- Raise the bar on best practices for digital-asset custodianship by building a greater understanding of different custody use cases, risk models, and adversary threats.
- Prepare for newer custody technologies that break older models for custodianship.

What did people say on Twitter?



Blockchain Commons

#SmartCustody is a project of **Blockchain Commons**, which supports blockchain infrastructure, internet security, and cryptographic research.



This Workshop

Designed for **individual holders** of digital assets, such as cryptocurrency traders and high net-worth individuals who are already familiar and working with digital assets.

- Are you considering all possible threats to your digital assets?
- Do you have comprehensive procedures to assess your risk profile?
- How does your system stack up against others in the industry?

We will presents a **cold-storage scenario** for the **self-custody** of your own digital assets

We will help you optimize the scenario for your needs through a **risk modeling** exercise and **adversary analysis.**

Disclaimer:

The information below is intended to inform a set of best practices. It may not address risks specific to your situation, and if it does not, you should modify appropriately. While this information may inform best practices, there is no guarantee that following this advice will sufficiently ensure the security of your digital assets. In addition, this information is only a window on best practices at a specific moment in time. Be aware that the Bitcoin & blockchain ecosystems may have evolved and the risk assessments of specific products may have changed since the publication of this draft. In other words: be cautious, be careful, and be aware of the current Bitcoin & blockchain landscape before you use this information.

Your Workshop Faculty

Christopher Allen

Bryan Bishop

Angus Champion de Crespigny

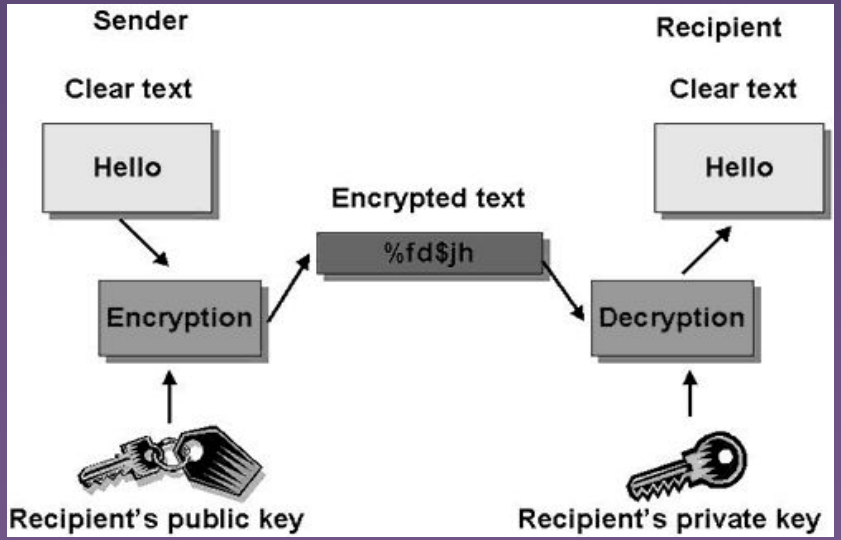
Shannon Appelcline

Technical Basics

Fundamentals of digital assets, keys, and self-custody

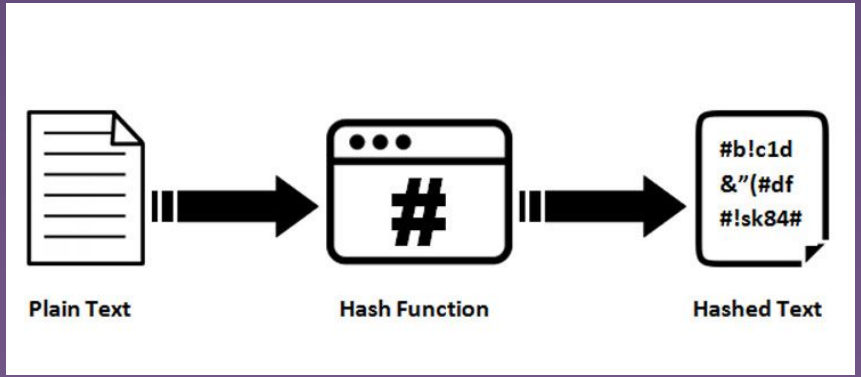
Digital assets use public key cryptography and hashing to secure transactions

- Public key cryptography
  - Different keys used for encryption and decryption
  - Avoids the key distribution problem

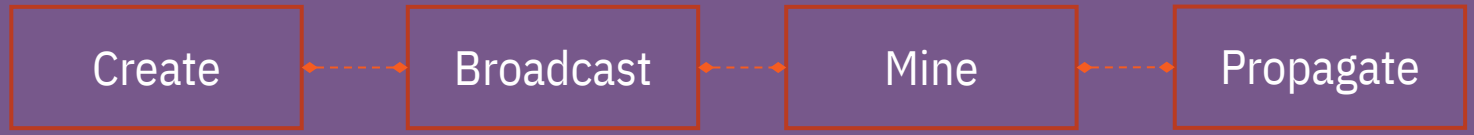


Digital assets use public key cryptography and hashing to secure transactions

- Hashing
  - Produces unique digital fingerprint
  - Can be verified instantly; computationally impossible (in theory) to reverse



Transactions have four main steps



Create

1. Create a transaction record based on funds previously sent to public address
2. Specify the recipient and conditions
3. Sign the transaction using the private key associated with the public address

Broadcast

1. Send the transaction over the internet
2. Transaction is relayed across the network

Mine

1. Transaction is collected by a miner along with other transactions
2. Miner runs software to produce a hash of all transactions that meets unique requirements
3. Once solved, the miner creates a ‘block’ consisting of all transactions, the calculation solution, and a new transaction granting them bitcoin

Propagate

1. Miner sends the block of confirmed transactions out on the network
2. The network verifies that the block is valid
3. The block is propagated and added to the blockchain

Managing private keys are hard; wallets simplify the process

- **Key**: usually short for private key, like a signature. Used to sign and create transactions received at an address
- **Address**: like a bank account. Cryptographically linked to a key.
- **Wallet**: collection of addresses with keys associated with those addresses. May be connected to the internet (hot), not connected (cold), and/or on a hardware device (hardware wallet)

Private keys are critical. How are they secured?

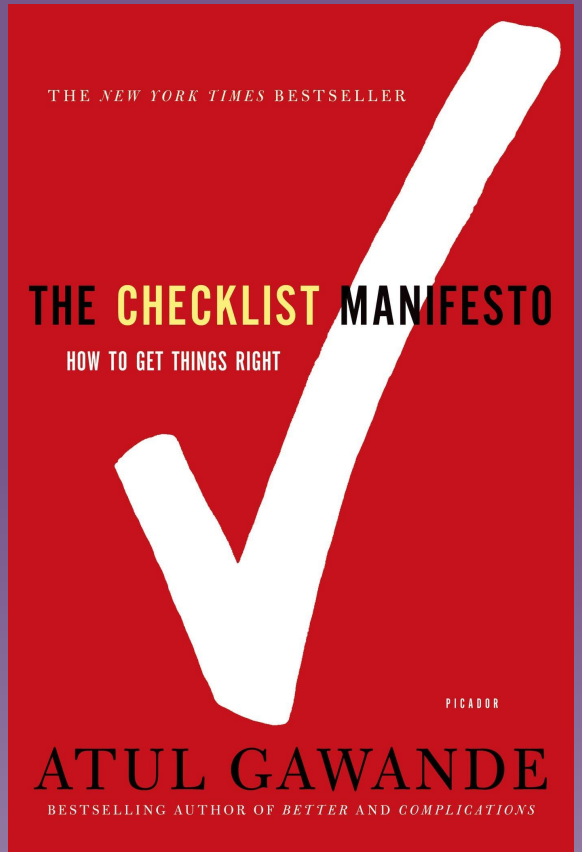
Other important terminology for today

- **Smart contract**: code attached to one or more transactions that contains certain programmatic conditions
- **HD key/wallet**: “hierarchical deterministic”. Allows one private key to control multiple addresses
- **Recovery words**: natural language words that are linked cryptographically to a private key, allowing easy recovery

Cold custody walkthrough

How to build a cold custody setup, from end to end

The power of checklists

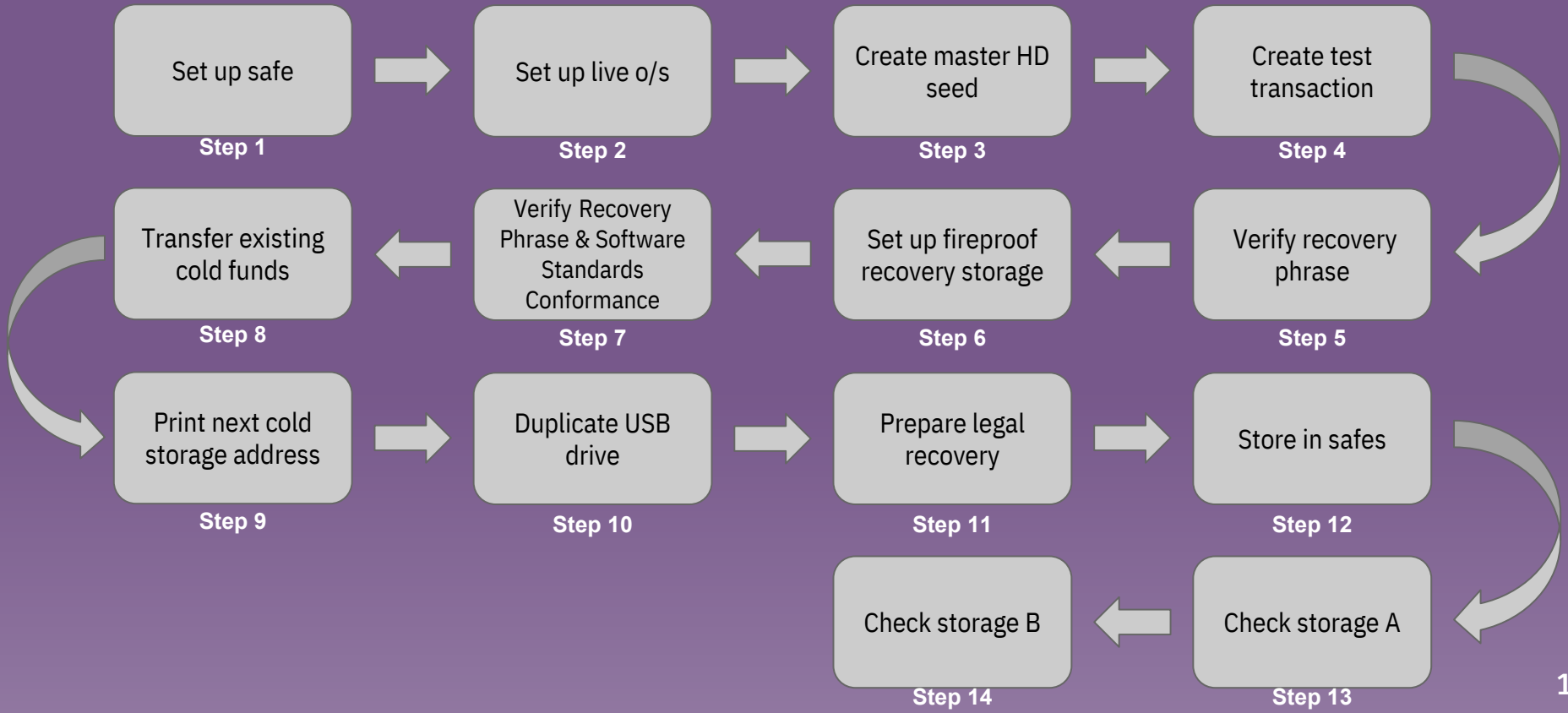


- Used by doctors, airline pilots, engineers
- Eight hospitals in eight major cities from Delhi to Toronto reduced complications by 35% and deaths 47%
- WHO one day training in checklists led to 18% reduction in mortality
- Pilots do years of training on the proper use of checklists required for every flight

We need checklists!

Cold storage configuration

Overview



Adversaries, risks, and controls

Who or what may compromise your environment, and how can you protect it?

Adversaries are risks pictured as living threats

- Risks are threats to the organization.
- By anthropomorphizing threats, we can consider their motivations.
- This makes it easier for users to determine which adversaries are actual risks *to you*.
- Another perspective: risks are inside-out, adversaries are outside-in

There are seven categories of adversaries;

We will cover some examples

1. Loss by Acts of God
2. Loss by Computer Error
3. Loss by Crime, Theft
4. Loss by Crime, other
5. Loss by Government
6. Loss by Mistakes
7. Privacy-related Problems

Death/Incapacitation

“I am your last firing neurons, and I seek to drag everything you ever knew down with you, into the darkness..”

- The lack of centralization and the high levels of anonymization for cryptocurrency make it hard to know when someone is holding cryptocurrency.
- This is usually considered a feature, but in the case of death or incapacitation, an asset holder usually want their heirs or guardians to know about the cryptocurrency, lest it be lost forever.

Death/Incapacitation

Case Studies

Abstract Case Study: Suffering a Stroke. Bob, an early bitcoin entrepreneur, suffers a stroke that leaves him considerably mentally impaired. His medical bills quickly pile up. Since he left no information about his bitcoins, his wife Alice is forced to sell their house to pay them.

Historic Case Study: Dying with Deposits. A moderator of a bitcoin discussion group knew that he was dying. He was holding not only his own bitcoin funds, but some for the forum as well. After he passed, the other staff of group spoke with his next of kin, to recover their funds, but the next of kin didn't know about the funds, let alone how to recover them. Some time later, the funds still had not moved, suggesting that they were genuinely lost.

Death/Incapacitation

Risks and Controls

Risks:

1. **Funds Loss.**
2. **Key Loss.**

Process Solutions:

1. **Register Your Funds.** *Dangers: Legal Forfeiture, Nation-State Actor.*
2. **Redundantly Relay Your Secrets.** *Dangers: Internal Theft.*
3. **Reveal Your Funds.** *Dangers: Internal Theft, Institutional Theft.*

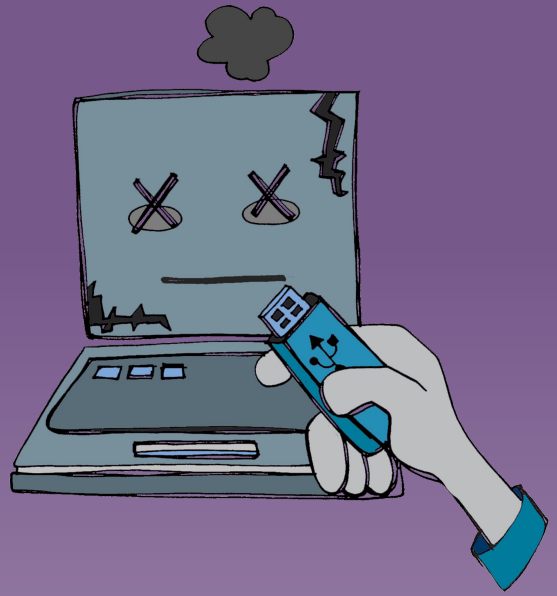
Cold Storage Solutions:

1. **Redundantly Store Your Keys.** *Dangers: Casual Physical Theft, Institutional Theft.*
2. ***Cold Storage Scenario* Optional Steps:** Use Cryptosteel (or Steel Tile); Use a Safety Deposit Box.

Bitrot

“I am entropy writ large. I want to break down your storage, crash your hard drives and degrade your optical media. I want to prevent your programs from running, and your data from reading; in the end, I always win.”

- Electronic storage methods for private keys can become unusable over time.
- This could be due to:
  - A physical hardware problem
  - Faulty electronic storage media
  - Aging software
  - Time-related hardware incompatibility



Bitrot

Case Studies

Abstract Case Study: Obsoleting Software. Carol loads up her Bitcoin wallet for the first time since she upgraded to Windows 10 … and discovers that it doesn't run. Digging further, she learns that it's been years since the developer of the wallet updated it. She has no idea of how to recover her keys from the wallet.

Historic Case Study: Throwing Out Bitcoins. James Howells of the UK is widely reported to have accidentally thrown out the hard drive with keys for 7,500 bitcoins after he broke down his laptop for parts. *News Story*.

Historic Case Study: Obsoleting Seeds. A user on StackExchange reported that he had a 15-word recovery phrase and a passphrase for his Bitcoins, but he had no idea what wallet had generated it. This isn't the standard 24-word phrase used by Ledger or Trezor, nor the variant phrases used by Electrum or GreenAddress. Despite having the codes, he didn't know what to do with them. *StackExchange*.

Bitrot

Risks and Controls

Risks:

1. **Key Destruction.**
2. **Key Loss.**

Cold Storage Solutions:

1. **Backup Your OS File System.**
2. **Maintain Setup Information.**
3. **Physically Store Your Keys.** *Dangers: Disaster, Casual Physical Theft, Institutional Theft.*
4. **Rotate Your Key Storage.** *Dangers: Correlation.*
5. **Verify & Rotate your Backups.**
6. **Verify Your Key Storage.**
7. ***Cold Storage Scenario* Optional Steps:** Use Cryptosteel (or Steel Tile); Use a (Second) Ledger; Use a Trezor; Use a (Second) USB Stick.

See Related — Key Fragility

Internal Theft

"You trusted me with your private keys. I intend to violate that trust because I want to steal your funds for my own use. And, I'll do my best to cover it up."

- A person trusted with private keys could steal funds. This might be an asset holder's heir or executor; within a corporate setting, it could be one of the persons trusted to use the keys or someone using social hacking to convince or coerce a trusted person to do the wrong thing.
- The asset holder has typically trusted someone with a key because they need to have it in order to do their job.
- Trust may have been mislaid or coercion used.

Internal Theft

Case Studies

Historic Case Study: Stealing from Shapeshift. Shapeshift.io's IT lead stole 315 bitcoins from them, then fled. However, that wasn't the end of the story. Afterward, he sold information about the company's security to a hacker, initiating a second breach, then sold the hacker access to a backdoor he'd installed, creating a third.

Internal Theft

Risks and Controls

Risks

1. **Funds Loss.**

Process Solutions:

1. **Create Paper Trails.**
2. **Limit Funds Spending.** *Dangers: User Error.*
3. **Monitor Your Funds.**
4. **Use Funds Multisignatures.** *Dangers: Internal Theft, User Error .*
5. **Use Funds Timelocks.** *Dangers: User Error.*

Cold Storage Solutions:

1. ***Cold Storage Scenario* Optional Steps:** If there's no requirement for ongoing access to funds, Use Bags (Tamper Evident), Use Redundant Metal Tiles, Use a Safety Deposit Box.

Non-Financially Motivated Attackers

"I don't care about your money, but I'll still going to mess with you. Maybe I'm your enemy, who wants revenge or to out you in some way. The key is: I know who you are, I know what you have, and I want to use that knowledge as a lever for my own purposes."

- Attackers may not care about acquiring your cryptocurrency, but could instead have other motives, such as wanting to reveal your transactions or wanting to keep you from accessing your own funds.
- Nature is the ultimate non-financially motivated attacker. It introduces pure chaos. Given enough time, it might do anything that a financially motivated attacker could!

Non-Financially Motivated Attackers

Case Studies

Abstract Case Study: Infecting the Machines. Trudy writes malware that infects and crashes peoples' computers. No reason. She just enjoys knowing that she's ruining the lives of people who are too stupid to defend themselves. Dan has his bitcoins on a computer that is hit by Trudy's newest virus.

Historic Case Study: Destroying Parity. Parity multisigs wallets for Ethereum all depended upon a single code library; because of flaws in the code, a regular user was able to take ownership of the library, then destroy it. This caused $280 million dollars in Ethereum funds to be locked up. The actual motive of the attacker isn't known. He claims it was a beginner mistake, but it also could have been a malicious attack or a poorly considered attempt to steal funds. *News Story*, *Twitter Feed*.

Non-Financially Motivated Attackers

Risks and Controls

Risks:

1. **Cascade: Correlation.** Some non-financially motivated attackers may be trying to determine who you are and what you're doing with your cryptocurrency.
2. **Cascade: Censorship.** Some non-financially motivated attackers may just want to keep you from accessing your funds.
3. **Cascade: Key Loss.** Some non-financially motivated attackers may just be destructive.

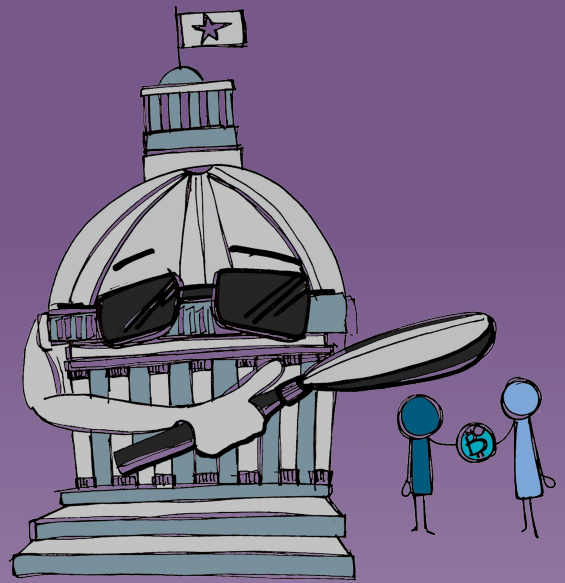
Process Solutions:

1. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.

Nation-State Actor

"I am the all-powerful state. I can surveil, I can seize. I can imprison, I can threaten. However, I am hopefully bound by laws and morality: if my citizens obey the rules and don't interact with criminals, then they have nothing to worry about."

- A nation-state could exert its tremendous power to corrupt the cryptocurrency market.
- A nation-state has such expansive powers that almost all risks are possible, requiring almost all solutions.
- Individuals might take on the mantle of the nation-state and use its powers in ways that are either abusive or illegal.



Nation-State Actor

Case Studies

Abstract Case Study: Targeting Lawfully. Alice operates a Bitcoin business in China, where the currency has come under increasing scrutiny in recent years. She is not a financial institution, so she should be able to legally operate, but the grey area surrounding the currency in China leaves her vulnerable. Grace, a government operative, takes advantage of this. She needs information on one of Alice's customers and uses the questionable status of Bitcoin in the country to threaten Alice.

Historic Case Study: Stealing Safe Deposit Boxes. During a series of fiscal crises, the state of California reduced their time period for property to be considered abandoned to a paltry three years, and safety deposit boxes were then confiscated and auctioned off. Sufficiently aggressive banks began seizing safety deposit boxes that were unchecked, even when they remained in contact with the customer on other topics! Bitcoin keys stored in safety deposit boxes could be vulnerable to this malfeasance. *News Story*.

Historic Case Study: Walking the Silk Road. While investigating Silk Road, Secret Service agent Shaun Bridges gained the login credentials of an admin and used them to steal 20,000 Bitcoins from Silk Road by transferring them to Mt. Gox. He then moved his funds from Mt. Gox just before the US government seized $2.1 million dollars worth of Mt. Gox funds. He then stole another 1,600 bitcoins that had been seized from Bitstamp — this time *after* being found guilty to the first crime! *News Story*, *News Story*, *News Story*.

Nation-State Actor

Risks and Controls

Risks:

1. **Key Loss.**
2. **Cascade: Coercion.**
3. **Cascade: Correlation.**
4. **Cascade: Legal Forfeiture.**

Process Solutions:

1. **Neutrally Store Your Funds.**
2. **Practice Anonymity.**
3. **Use Paranoid Key Procedures.** *Dangers: Process Fatigue*

Cold Storage Solutions:

1. **Obscure or Protect Your Keys.** Store keys in an obscured way that would be readily obvious to the asset holder, but not to a thief. Alternatively, protect keys with a PIN or other code. *Dangers: Key Fragility.*
2. **Widely Separate Your Keys.**

See Related — Coercion

Convenience

"I know that you want things to be simple. I encourage that. Life should be easy. Don't use that tamper-proof bag. Don't keep your safety deposit box in another state, away from California's fault lines. And if you're going on a trip, definitely ease up on the security of your bitcoins, so that you can access them from the road. "

- Convenience can be the bane of any security procedure.
- Because of Process Fatigue, a bitcoin holder might eliminate some of the more onerous elements of his procedure.
- There can also be real, pragmatic, and understandable reasons for increasing the Convenience of bitcoin access, despite the cost to security.

Convenience

Case Studies

Abstract Case Study: Trusting the Wrong Person. Alice is going to be out of town all month. She expects to make some very large bitcoin purchases during that time period, so she needs her coins more conveniently accessible than her normal cold storage procedure allows. She opts not to go with the convenience of carrying them on one of her electronic devices because she's afraid they could be seized. Instead, she gives her husband, Bob, access to her keys. When she calls up Bob to have him make a transaction, she finds his phone line disconnected. He's gone, with her bitcoin wealth!

Convenience

Risks and Controls

Risks:

1. **Funds Loss.**
2. **Key Loss.**
3. **Cascade: Personal Network Attack.**
4. **Cascade: Coercion.**
5. **Cascade: Theft, All.**
6. **Cascade: User Error.**

Process Solutions:

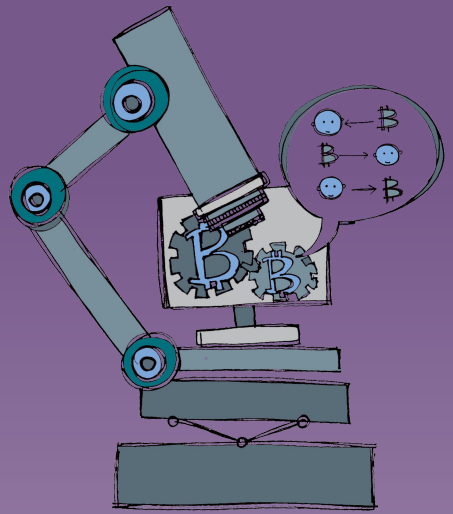
1. **Create Checklists**.
2. **Maximize Security.**

See Related: Process Fatigue

Correlation

"I want information. I watch cryptocurrency transactions with an eagle eye, ready to swoop in on any mistake. If you keep making the same payments or receiving the same payments or using the same addresses, I'll figure it out. I want to connect the dots to determine who is spending cryptocurrency for what, and I can figure that puzzle out if you give me enough pieces."

- Cryptocurrency use is pseudo-anonymous and somewhat private. However, it's not totally so: it's possible to build up correlation.
- Through statistical analysis and through the discovery of accidental revelations, a third-party could tie together an asset holder's usage of various funds to paint a larger picture of their finances and contacts.



Correlation

Case Studies

Abstract Case Study: Correlating over Coffee. Alice is sloppy with her bitcoins and tends to use one address for everything. She goes out to buy a coffee with bitcoins; while she sips away at the café, working at her laptop, the barista notes the huge number of bitcoins going into the address. She follows Alice home, planning larceny.

Abstract Case Study: Correlating Identities. Carol uses the same online identity on bitcointalk and on twitter. Eastern European hackers monitor twitter, see her talking about bitcoins, track that back to bitcointalk, and find wallet addresses mentioned there that reveal her bitcoin wealth. They then set their scripts lose, hoping to break into her computer and steal her keys.

Correlation

Risks and Controls

Risks:

1. **Funds Revelation.**
2. **Cascade: Censorship.**
3. **Cascade: Coercion.**
4. **Cascade: Legal Forfeiture.**
5. **Cascade: Loss of Fungibility.**
6. **Cascade: Sophisticated Theft.**

Process Solutions:

1. **Practice Anonymity.**
2. **Practice Anonymizing Your Funds.**
3. **Practice Key Hygiene.**

Disaster

“I want to destroy. I want to crumble and burn. I want to ruin with water, to blow things into the air. I am bombs, bullets, and explosions. I am sudden and unexpected but disastrous destruction.”

- A sudden, large-scale destructive event can destroy copies of private keys. It is usually a natural event such as an earthquake, fire, hurricane, or tsunami.
- It could also be an accident such as a building collapse; or it could be a man-made catastrophe, such as a bomb blast, an EMP blast, or full-scale warfare.

Disaster

Case Studies

Historic Case Study: Flooding Keys. A bitcoin user had a strong procedure for protecting his keys. Every quarter he reprinted his paper wallet to ensure that the ink didn't fade and immediately shredded the old one. Unfortunately, he placed his paper wallet in the basement, which flooded; the ink was washed off the wallet. The user came to IRC for help, and though they suggested dumping his printer's memory buffer, it was already too late.

Disaster

Risks and Controls

Risks:

1. **Key Destruction.**
2. **Key Loss.**

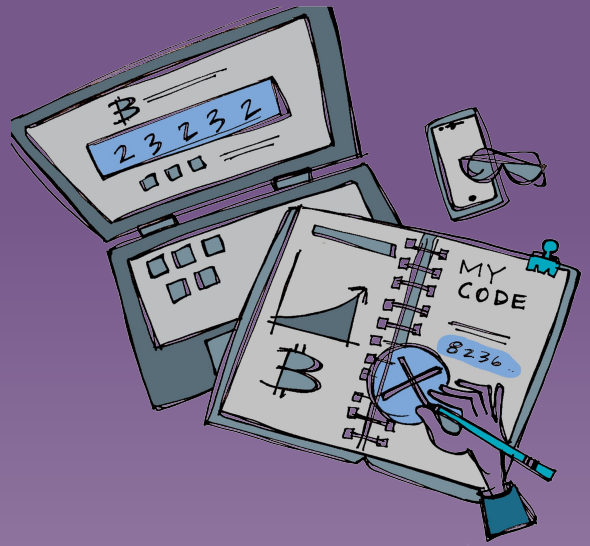
Cold Storage Solutions:

1. **Fortify Your Key Storage.**
2. **Redundantly Store Your Keys.** *Dangers: Casual Physical Theft, Institutional Theft.*
3. **Widely Separate Your Keys.**
4. ***Cold Storage Scenario* Optional Steps:** Use Bags (Fire Resistant); Use Cryptosteel (or Steel Tile); Use Redundant Metal Tiles; Use a Fireproof Safe; Use a (Second) Ledger; Use a Safety Deposit Box; Use a Trezor; Use a (Second) USB Stick.

Key fragility

“I am entropy writ small. All I need to do is mislay a digit or two from a ridiculously large number, and my job is done. Perhaps you could make my job easier by encoding or obscuring your key or by maintaining just a single copy; complexity and singularity both beget fragility in different ways..”

- A key may be lost because its complexity makes it innately prone to loss.
- This could be a physical loss, or a computer error, corrupted at key generation or a recovery corruption where the wrong key is recreated from an external source.
- When key storage is obscured or protected, it might not be the key itself that is lost, but instead the method to unobscure the key or the code to decode it.



Key fragility

Case Studies

Abstract Case Study: Losing Addresses. Alice generates an address on an exchange so that she can send funds there, and immediately sends bitcoins, but the exchange has a massive failure. The address is never recorded! Alice shows them that she sent the funds, but they have no record of the address, and she's unable to prove it's really theirs.

Historic Case Study: Breaking VanityGen. A patched version of the VanityGen address creator generated compressed keys. Unfortunately, there was a bug with how it padded out keys. 1 time in 256 when it serialized the private key, it would prepend a 0 to the address and lose the last byte.

Historic Case Study: Forgetting the PIN. A Wired author stored 7.4 BTC on a Trezor and protected it with a PIN. A cleaning service threw away the paper with the PIN, which also contained the recovery words. The author soon realized that he didn't remember the PIN and every time he entered it incorrectly, the Trezor doubled a timeout period before he could try again. *News Story*.

Key fragility

Risks and Controls

Risks:

1. **Key Loss.**

Process Solutions:

1. **Redundantly Relay Your Secrets.** *Dangers: Internal Theft.*
2. **Take the Time.**
3. **Verify Your Keys.** *Dangers: Correlation.*

Cold Storage Solutions:

1. **Redundantly Store Your Keys.** *Dangers: Casual Physical Theft, Institutional Theft.*
2. ***Cold Storage Scenario* Optional Steps:** Use Cryptosteel (or Steel Tile); Use Redundant Metal Tiles; Use a (USB) Laser Printer; Use a Safety Deposit Box.

See Related — Bitrot, Transaction Error, User Error

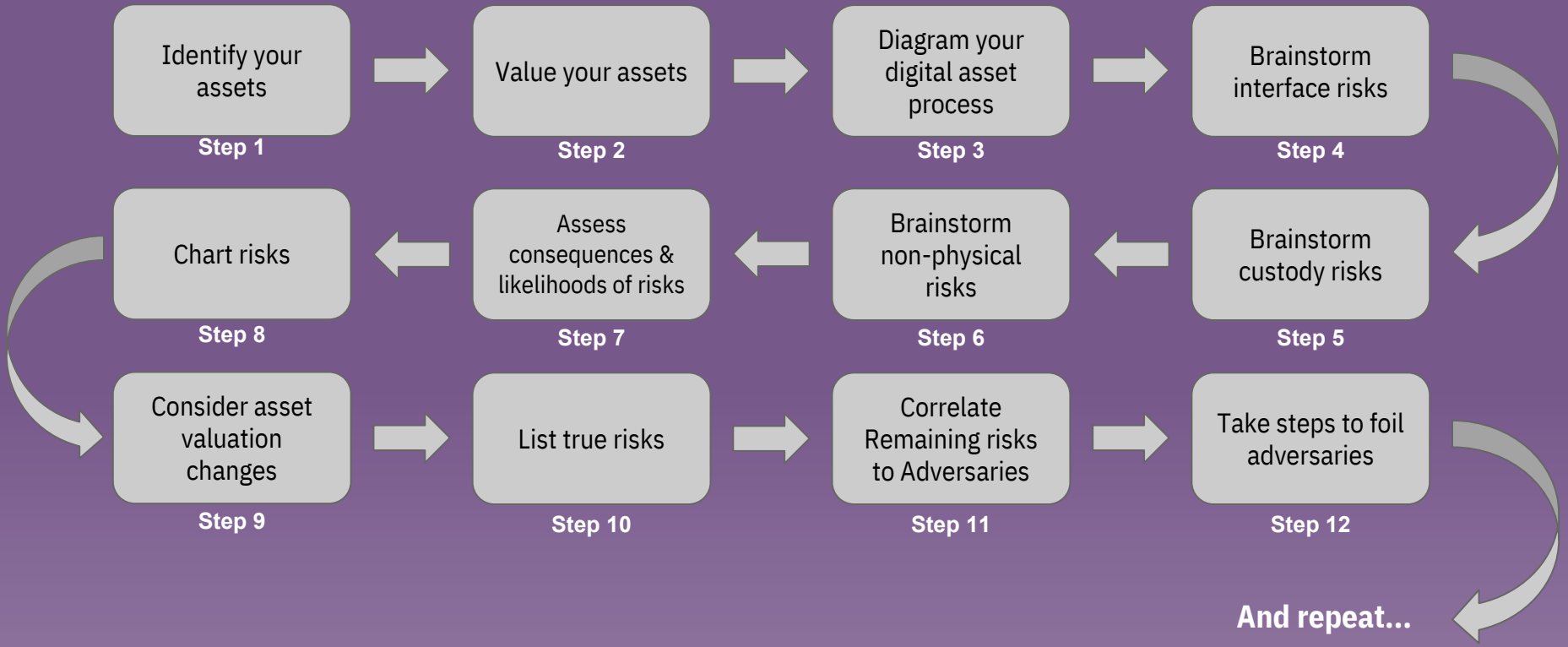
Lunch break

Risk modeling

Modeling the technical and non-technical risks of your configuration

Risk modeling process

Overview



Step 1 & 2

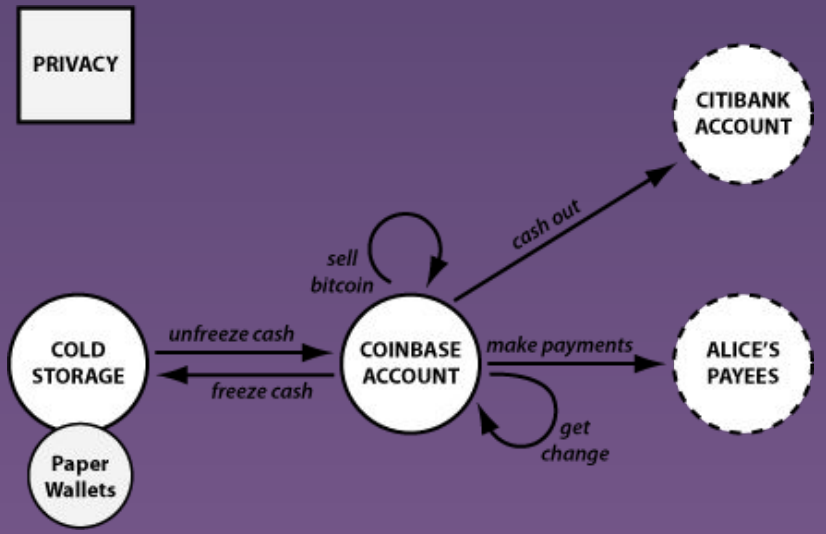
Identify your assets & Value your assets

Categories	***Examples***
1. Digital assets; a. Where is it being held? b. What sort of asset is it?	a. Bitcoin held at Coinbase b. Bitcoin held in cold storage c. Ethereum held in a paper wallet
2. Keys: a. How is it stored? b. Where is it located?	a. Key on Ledger in fireproof home safe b. Key on Cryptosteel in safety deposit box
3. Non-physical assets, eg a. ***Privacy*** regarding your identity? b. ***Compartmentalization of*** your activities? c. ***Confidentiality*** of your total funds?	

Step 3

Diagram Your Digital Asset Process

1. Draw physical assets as nodes (circles), and subassets as subnodes (smaller circles) linked to the main node.
2. Add nodes to your diagram that are part of your cryptocurrency process but were not on your physical assets list.
3. Add alternate nodes (dotted circles) for physical assets that aren't cryptocurrency or where the cryptocurrency doesn't belong to you.
4. Draw interfaces (arrows) between the nodes.
5. Draw non-physical assets as reminders (squares).



Step 4-6

Brainstorm Interface, Custody, and Non-Physical Risks

		Examples
1.	How could you lose your cryptocurrency when it moves across that interface?	a. Money sent to wrong address b. Incorrect amount of money sent to recipient c. Money lost by recipient d. Money stolen by man-in-the-middle e. Transaction scripted or timelocked wrong
2.	How could you lose your money via your keys?	a. Funds stolen by computer attacker b. Keys stolen by computer attacker c. Keys stolen in physical theft d. Keys destroyed in fire or earthquake e. PIN for hardware wallet forgotten f. Exchange goes out of business
3.	How could you lose your non-physical assets?	a. Privacy lost due to address reuse b. Privacy lost by announcing Bitcoin ownership c. Ease of use lost by complicated cold storage setup d. Ease of use lost by 2FA e. Compartmentalization lost by constantly sending funds from one account to another

Step 7

Assess Consequences & Likelihoods of Risks

Determine two values for each of the potential risks:

1. ***Consequence:*** the bad result if the risk proves true, listed as a numerical value (directly based on your asset valuation)

2. ***Likelihood:*** the chance that the risk proves true

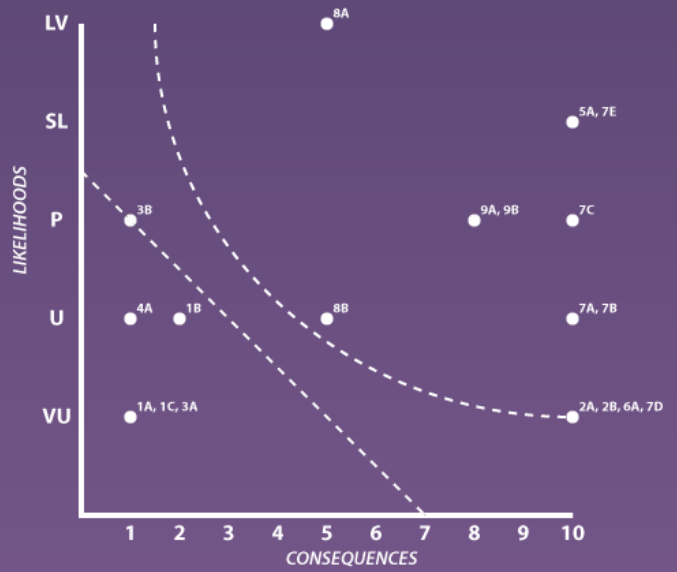
Examples of Likelihood Measures:

- A, B, C, D, F
- 1, 2, 3, 4, 5
- 25%, 20%, 15%, 10%, 5%
- Constant Problem, Frequent Problem, Occasional Problem, Rare Problem, Extremely Rare Problem
- Very Likely, Somewhat Likely, Possible, Unlikely, Very Unlikely
- Super Scary, Cold Chill, Frightening, Concerned, Not Worried
- Great, Very Good, Good, OK, Poor

Step 8

Chart Risks to Highlight True Risks

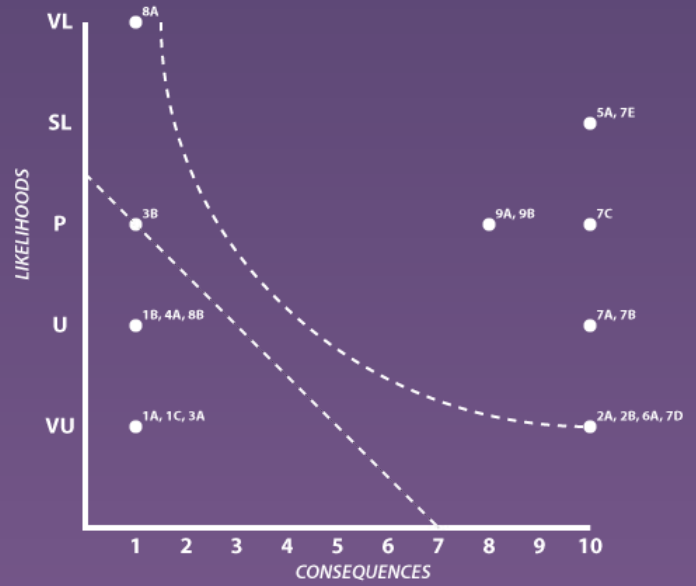
1. Label the horizontal axis. Use your consequences as the horizontal axis, running from 0 to the top consequence that you considered.
2. Label the axes. Use your likelihood as the vertical axis, running from 0 to the top likelihood that you considered.
3. Place all risks on the chart. Make a point for each risk at the intersection of its consequence and likelihood.
4. Draw a risk-tolerance line.



Step 9

Consider Asset Valuation Changes

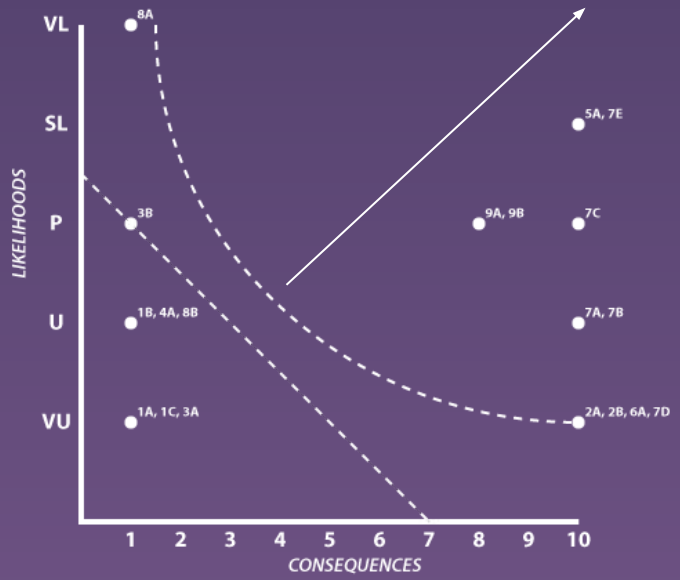
1. Consider the value of assets. Look at each of the assets that has a true risk, and consider whether their valuation could be decreased sufficiently to push the related nodal risks below the risk-tolerance line.
2. Modify consequences. Based on your asset valuation changes, modify the consequences for those assets, and also consider any linked interfaces and see if their consequences changed as well.
3. Rechart if needed



Step 10 & 11

List Your True Risks & Correlate Remaining Risks to Digital Adversaries

1. List your true risks in decreasing order.



2. Go through the list of adversaries and checkmark all adversaries that correlate with the risks you identified.

Step 12

Take Steps to Foil Adversaries

Adopt solutions as appropriate:

1. Introduce a Cold Storage Procedure.
2. Incorporate Cold Storage Solutions.
3. Add Cold Storage Optional Steps.
4. Incorporate Hot Wallet Solutions.
5. Incorporate Process Solutions.

Self-Custody Digital Risk Model

A walkthrough

Digital asset wallets and custody hardware

Live discussion

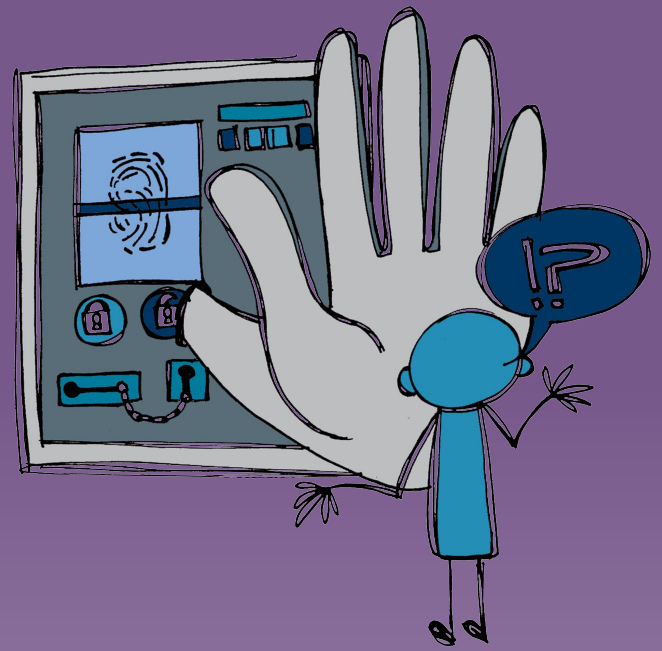
Break

Ignore beyond here

Denial of Access

“I want to control your movements, to keep you from getting to your bank or to your house. As is often the case, I have a deeper motivation, but it probably has nothing to do with your cryptocurrency. Instead, my motives likely relate to an instability in your city, state, or country. I might be a riot, a political insurgency, or a popular uprising.”

- Access to cryptocurrency is usually blocked by censorship, when someone on the internet purposefully obstructs the ability to transact funds. However, that blockage can also take physical form if access to private-key storage locations is prevented. This imagines a fairly large-scale problem that is likely only possible in a politically unstable region.



Denial of Access

Case Studies

Abstract Case Study: Blocking by Mistake. Frank is cheap, so he stores his Cryptosteel in his company's safety deposit box, which he has access to. The company goes into bankruptcy, and Judy has its assets frozen. Frank tries to recover his Cryptosteel from the safety deposit box but finds he's denied access … which wouldn't be a problem except for the fact that the dog ate the paper copy of his recovery seed at home.

Denial of Access

Risks and Controls

Risks:

1. **Key Denial.** Much as with Censorship, the user still has theoretical access to his keys, but can't actually get to them.

Process Solutions:

1. **Neutrally Store Your Funds.** Maintain funds or keys outside of the sphere of control of fascist and authoritarian nation-states.

Cold Storage Solutions:

1. **Redundantly Store Your Keys.** Maintain multiple representations of your master keys. Store encrypted keys in local storage and unencrypted keys in more protected storage, such as a safety deposit box. *Dangers: Casual Physical Theft, Institutional Theft.*
2. **Widely Separate Your Keys.** Maintain multiple physical representations of your master keys in places that are widely separated. Consider locales under different legal jurisdictions and with different physical risks.
3. ***Cold Storage Scenario Optional Steps:*** Use Redundant Metal Tiles, Use a Safety Deposit Box.

See Related — Censorship.

Systemic Key Compromise

“I lie in wait. I want you to think that your keys were generated correctly, but after you’ve turned your attention to other things, I will spring my surprise. I am the best pal of hackers and crooks, who use my exploits to steal your money.”

- A systemic problem in the generation of keys can leave them broadly vulnerable to compromise. For example, a key-generation program’s random seed might have been insufficiently random. This might be a result of an error in the key generation or purposeful malevolence on the part of the key generators. This may also be an attack on a system meant to steal all of the keys on that system or to deny access to it.
- .
- .

Systemic Key Compromise

Case Studies

Historic Case Study: Whitehatting BlockchainInfo. A mistake in an update caused 0.0002% of Blockchain.info's private keys to be generated insecurely. 250 Bitcoins quickly went missing, but it was soon revealed that a whitehat was sweeping up the funds, with the intention of returning them. *News Story*.

Historic Case Study: Trusting Libraries. Systemic compromises can arise from deep libraries used in cryptocurrency apps. JavaScript's secureRandom() function at one time generated low-entropy numbers that weren't truly random due to a type error. Unfortunately, it was used in numerous cryptocurrency products for many years before this was discovered. *Security Alert*, *News Story*.

Systemic Key Compromise

Risks and Controls

Risks:

1. **Funds Loss.** A sophisticated attacker could use the compromise to discover private keys. This would most likely occur in aggregate, rather than the asset holder being individually targeted.
2. **Cascade: Censorship.** One of the possible results of a systemic key compromise is the censorship of the system.

Process Solutions:

1. **Maintain Emergency Procedure.** Write a procedure that describes what to do if your security has been compromised. Follow it quickly and precisely. Generally, move funds if their keys have any possibility of compromise. *Dangers: Process Fatigue.*
2. **Monitor the Industry.** Be aware of happenings in the Bitcoin industry, particularly security compromises.
3. **Rotate Your Keys.** Regularly change the keys being used to protect funds by sending those funds on to new addresses. *Dangers: Key Fragility.*

Hot Wallet Solutions:

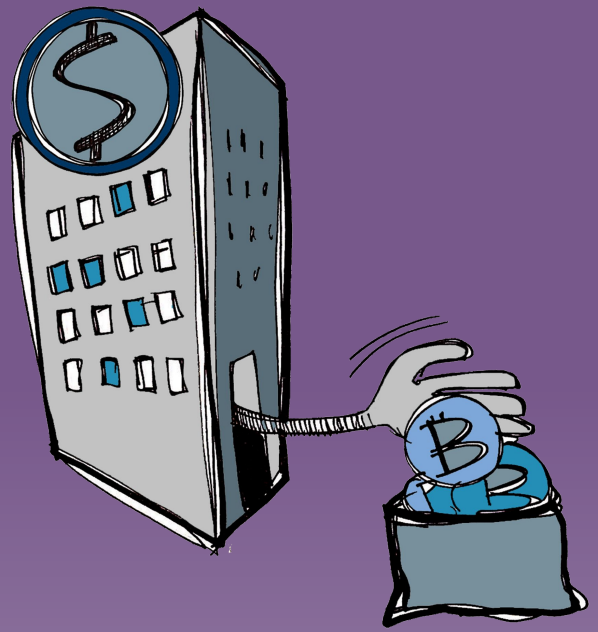
1. **Question Policies & Procedures.** Know the security policies and procedures of any company that you're working with; be sure that they have rigorous, well-documented security procedures that they follow religiously, and that they treat any variance from their procedure as a problem that must be investigated. Also, be sure that there are no negative policies that might affect your usage of its services.

Institutional Theft

“I pretend to be a good employee, but I’m always waiting for my chance for a great score. I want to sift through the goods entrusted to my company and to take the best for myself. However, I don’t want to be caught, so I need to be cautious in my larceny.”

A networked attack against a specific person or company’s cryptocurrency holdings.

- Keys could be stolen by the staff members at a trusted institution such as a bank or a Bitcoin exchange. This could be a bank employee violating dual-access-key protocol and illicitly accessing a safety deposit box or it could be an engineer stealing private keys out of a database. Unlike casual or sophisticated theft, the physical representation of the key might not be stolen, just the data, making it harder for the victim to realize that a theft has occurred at all!
-
- In rare cases, a whole institution might be corrupt. They might steal the coins or some of their customers, they might falsely claim that a hacker had made off with funds, or they might just disappear quietly, never to be heard from again.
-



Institutional Theft

Case Studies

Abstract Case Study: Backdooring the System. Mallory always plans for the future. While working at an exchange as their security expert he builds several backdoors into the system. Years later, when the value of bitcoin has skyrocketed, he utilizes them, and the exchange finds their funds suddenly missing.

Historic Case Study: Blocking Hackers. Sometimes an Internal Theft might actually be a purposeful choice on the part of a company to retrieve stolen goods! When coins were stolen from the OzCoin mining consortium they were moved to a StrongCoin Wallet. This was obvious due to a correlation danger at StrongCoin: every time funds are spent at StrongCoin, a small fee is paid to a specific address. OzCoin alerted StrongCoin who recovered the funds by creating a new version of their JavaScript wallet especially for the hackers; as soon as they tried to access the funds, the coins were sent to another address, so that StrongCoin could then return them to OzCoin.

Institutional Theft

Risks and Controls

Risks:

1. **Funds Loss.** Though it's certainly possible that an institutional thief at a bank doesn't know what he's getting, most likely he is a sophisticated thief who is looking for private keys in order to steal the funds.

Process Solutions:

1. **Monitor the Industry.** Be aware of happenings in the Bitcoin industry and the hardware devices you uses, particularly concerning security compromises.
2. **Monitor Your Funds.** Regularly monitor funds to make sure they're not disappearing. Make sure that alarms are obtrusive. Have a plan in place to quickly save remaining funds if some disappear.

Cold Storage Solutions:

1. **Create Tamper Evidence.** Store keys or other secret materials in tamper-evident bags; place padlocks on your Cryptosteel. *Dangers: Process Fatigue*.
2. **Obscure or Protect Your Keys.** Store keys in an obscured way that would be readily obvious to the asset holder, but not to a thief. Alternatively, protect keys with a PIN or other code. *Dangers: Key Fragility*.
3. ***Cold Storage Scenario* Optional Steps:** Use Bags (Tamper Evident), Use Redundant Metal Tiles.

Hot Wallet Solutions:

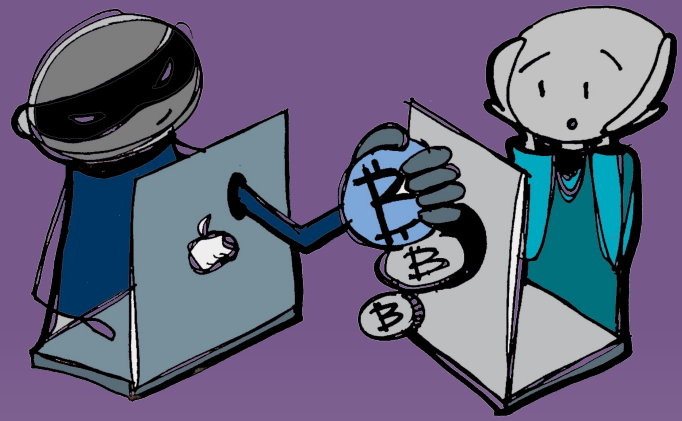
1. **Create Cold Storage Procedure.** Adapt a Cold Storage Procedure that moves some or all of your funds off of your hot wallet. Only keep keys on an exchange or brokerage for the minimum amount of time required to make a transaction. *Dangers: Disaster, Casual Physical Theft*.
2. **Question Policies & Procedures.** Know the security policies and procedures of any company that you're working with; be sure that they have rigorous, well-documented security procedures that they follow religiously, and that they treat any variance from their procedure as a problem that must be investigated. Also, be sure that there are no negative policies that might affect your usage of its services.

Network attack, personal

"I know you personally have cryptocurrency, and I want to steal it. I will use my expertise with programming or with hacking to attack you on the internet, and then your bitcoin will be mine."

A networked attack against a specific person or company's cryptocurrency holdings.

- A hacker may eavesdrop or change data on a site or *en route* to a site.
- For Bitcoin transactions, they might try to change the recipient of a transaction or they might try to access the credentials of the asset holder, so that they can generate a transaction as they see fit.
- They could try to hack into the site where the private keys are held or simply phish the target with a fake login page.



Network attack, personal

Case Studies

Abstract Case Study: Eavesdropping on Wifi.

Historic Case Study: Spoofing Bitcointalk.

Spearphishing Bitpay. An attacker contacting the CFO pretending to be an associate to convince them to login to a phishing page where the CFO revealed his Bitpay credentials. These credentials were then used to contact the CEO of Bitpay and convince him to transfer 5,000 Bitcoins.

Hacking Coinbase Accounts. A Coinbase account was linked to a Gmail account, itself protected with 2FA linked to his cell phone. Hackers moved the cell phone number to a different device, used that to retrieve Google's two-factor authentication messages, and used that to break into Coinbase.

Network attack, personal

Risks and Controls

Risks:

1. **Funds Loss.** The ultimate goal of an active network attack is usually funds theft, but that can occur via several means.
    a. **Account Compromise.** In a masquerade attack, an active network attacker might take control of your account at a Bitcoin brokerage or exchange, giving them access to any keys and any records or logs stored there.
    b. **Transaction Corruption.** In an en-route attack, an active network attacker might corrupt a transaction that you have in process, misdirecting it.
2. **Cascade: Correlation.** If an attacker gains access to logs or records, they can probably trace an asset holder's usage of funds.
3. **Cascade: Transaction Error.** If an attacker manages to substitute a recipient address, the user will send funds to the wrong place.

Process Solutions:

1. **Maintain Emergency Procedure.** Write a procedure that describes what to do if your security has been compromised. Follow it quickly and precisely. Generally, move funds if their keys have any possibility of compromise. *Dangers: Process Fatigue*.
2. **Monitor Your Funds.** Regularly monitor funds to make sure they're not disappearing. Make sure that alarms are obtrusive. Have a plan in place to quickly save remaining funds if some disappear.
3. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.

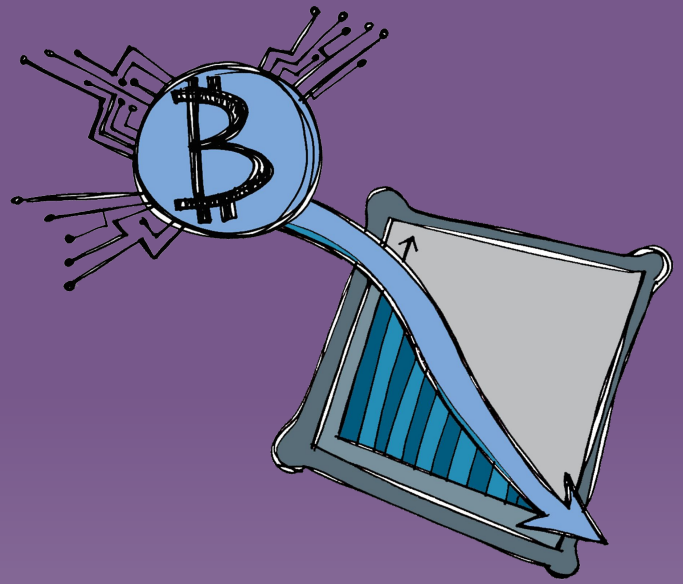
Hot Wallet Solutions:

1. **Create Cold Storage Procedure.** Adapt a Cold Storage Procedure that moves some or all of your funds off of your hot wallet. Only keep keys on an exchange or brokerage for the minimum amount of time required to make a transaction. *Dangers: Disaster, Theft, Casual*.
2. **Maintain Account Security.** Be sure that all online accounts have very robust passwords and that the companies have high security ratings.
3. **Practice Session Security.** Ensure that all online communications are encrypted.

Network attack, systemic

“I’m a big kahuna among hackers. I don’t go after your little bitcoin wallets, I go after the exchanges or other bitcoin sites instead. Nonetheless, you might just find yourself at a literal loss when I bankrupt the company holding your wallet.”

- Users are usually most concerned about Personal Network Attacks which target them directly; due to the decentralized nature of Bitcoin, each user is their own last line of defense. However, hackers might instead decide to go after the companies that users are working with. This is both a bigger danger, because it’s been a prime source for Bitcoin instruisions, and a big problem, because the user doesn’t have any control over this level of infrastructure.



Network attack, systemic

Case Studies

Historic Case Study: Unsigning the Transactions. In the early days of Bitcoin, there were sites that processed transactions, but which had bugs in their code. It was possible to send some of them invalid, unsigned transactions, and they would still think they had gotten paid. Some of these early sites were advantage of and their customers lost money.

Historic Case Study: Bankrupting Bitcoin Dice. Hackers took over Ghash.io, giving them about 25-30% of network hashing power. They mined a block that gave Ghash's funds to themselves, but before they announced it, they made a bunch of bets at Betcoin Dice. Some paid out, then Ghash announced the block that reversed the bets, effectively creating a double spend. Betcoin dice lost 1000 bitcoins. *Forum Post*.

Historic Case Study: Filling the Graveyard. Many other blockchains has suffered systemic network attacks over the years. *Blockchain Graveyard*.

Network attack, systemic

Risks and Controls

Risks:

1. **Funds Loss.** Though it's a company being attacked, if they lose their cash, and can't recover it through insurance claims, this directly impacts the users.
2. **Key Denial or Key Loss.** Attackers might deny users temporary or permanent access to their online keys, even if they're not able to access those keys themselves.
3. **Cascade: Correlation.** Attackers who have taken over a site can do all kinds of nefarious things, such as spy upon users and correlate their various addresses.

Process Solutions:

1. **Maintain Emergency Procedure.** Write a procedure that describes what to do if your security has been compromised. Follow it quickly and precisely. Generally, move funds if their keys have any possibility of compromise. *Dangers: Process Fatigue.*
2. **Monitor the Industry.** Be aware of happenings in the Bitcoin industry and the hardware devices you uses, particularly concerning security compromises.

Hot Wallet Solutions:

1. **Create Cold Storage Procedure.** Adapt a Cold Storage Procedure that moves some or all of your funds off of your hot wallet. Only keep keys on an exchange or brokerage for the minimum amount of time required to make a transaction. *Dangers: Disaster, Casual Physical Theft.*
2. **Maintain Account Security.** Be sure that all online accounts have very robust passwords and that the companies have high security ratings.
3. **Question Policies & Procedures.** Know the security policies and procedures of any company that you're working with; be sure that they have rigorous, well-documented security procedures that they follow religiously, and that they treat any variance from their procedure as a problem that must be investigated. Also, be sure that there are no negative policies that might affect your usage of its services.
1.

Physical Theft, Casual

“I just want an easy score, and your house looks like it. Obviously, I’m taking your jewelry and your electronics. But, if you got a safe, I’ll try to take that too. I have no idea what I’ll do with it, or with the contents if I can get it open. If I see some weird numbers, I’ll probably just trash them.”

- An entirely opportunistic real-world theft could, by chance, scoop up private keys. This is typically a burglary or a robbery that results in the acquisition of a computer device or safe that happens to have private keys on them, but which weren’t the motivation for the theft. Casual Theft often results in denial rather than loss.

Physical Theft, Casual

Case Studies

Abstract Case Study: Waiting for the Other Shoe. Dan's house is broken into. His electronics are stolen, including his laptop. Though his bitcoin keys are on the laptop, and his procedure says he should now move his funds as soon as possible, he doesn't worry about it because the whole hard drive is encrypted. A few months later, his bitcoins all disappear in the night.

Abstract Case Study: Losing a Phone. Bob accidently leaves his phone in his car, and a thief breaks the window and steals it. The phone contains Bob's old Bitcoin wallet; it used to only have "play" money, but due to the increase in the value of Bitcoin it is now worth $50 thousand dollars. Bob can't remember where he kept his recovery phrase.

Physical Theft, Casual

Risks and Controls

Risks:

1. **Key Loss.** Because the physical representation of the key has been taken, it will no longer be available to the asset holder.
2. **Cascade: Sophisticated Theft.** A casual theft could lead to Sophisticated Theft if the thief realizes what he has and how to use it.

Solutions:

1. **Maintain Emergency Procedure.** Write a procedure that describes what to do if your security has been compromised. Follow it quickly and precisely. Generally, move funds if their keys have any possibility of compromise. *Dangers: Process Fatigue.*

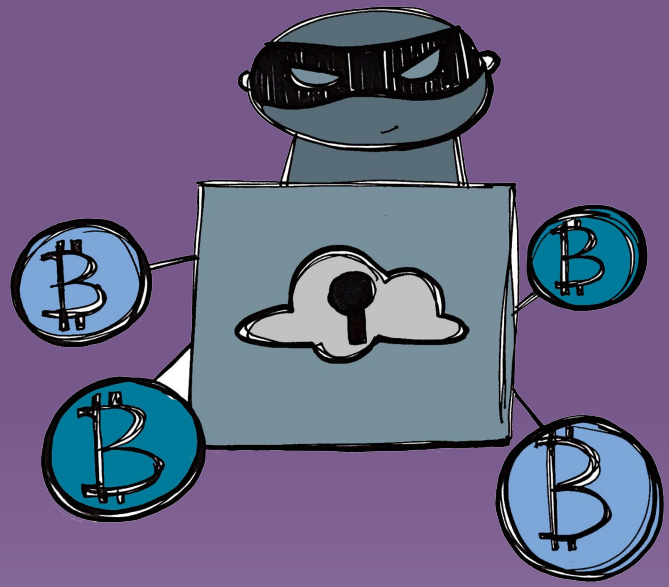
Cold Storage Solutions:

1. **Obscure or Protect Your Keys.** Store keys in an obscured way that would be readily obvious to the asset holder, but not to a thief. Alternatively, protect keys with a PIN or other code. *Dangers: Key Fragility.*
2. **Redundantly Store Your Keys.** Maintain multiple representations of your master keys. Store encrypted keys in local storage and unencrypted keys in more protected storage, such as a safety deposit box. *Dangers: Casual Physical Theft, Institutional Theft.*
3. ***Cold Storage Scenario Optional Steps:*** Use a Safety Deposit Box.

Physical Theft, Sophisticated

“I know you have cryptocurrency and I want to steal your keys. I’m not a fancy hacker or email spoofer. Instead, I’m someone who can successfully stage a real-world crime. I’ll break into your house or your safety deposit box. Cut the music for my heist scene.”

- Unlike a Casual Theft, a Sophisticated Theft is a real-world crime that specifically targets cryptocurrency keys. They could be going after computers, hardware wallets, Cryptosteels, or some other storage that contains a key. However, these thieves aren’t necessarily a second-story man or other robber; they also could be a confidence man or someone else who wins your trust.



Physical Theft, Sophisticated

Case Studies

Abstract Case Study: Staging a BitCON. Mallory befriends Carol and convinces her to demonstrate how Bitcoin works. Mallory is able to spy out enough specifics about Carol's Bitcoin accounts that she's later able to break into them.

Abstract Case Study: Listening In. Mallory rents a suite next to a Bitcoin bank. He then sets up listening devices to engage in an EMI side channel attack, extracting crucial information from electromagnetic leaks.

Physical Theft, Sophisticated

Risks and Controls

Risks:

1. **Funds Loss.** The goal of the thief is to acquire private keys so that he can then steal the funds associated with them.
2. **Key Loss.** Technically a thief might physically steal private keys. However, that's really the least of the problems with a sophisticated theft. Because the private keys were purposefully stolen, the goal of the attacker is to acquire the related funds as soon as possible. Thus, the fact that the asset holder no longer has access to a key becomes quickly irrelevant.

Process Solutions:

1. **Maintain Emergency Procedure.** Write a procedure that describes what to do if your security has been compromised. Follow it quickly and precisely. Generally, move funds if their keys have any possibility of compromise. *Dangers: Process Fatigue.*
2. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.
3. **Use Paranoid Key Procedures.** Take extreme protective methods when generating keys or when accessing accounts. Turn off phones. Remove cell phones. Unplug electronics. Cover windows. Tape your computer's camera and muffle your microphone. Do not work in rooms adjacent to property that you don't own. In extreme cases, rent a random car in a far remote location to serve both as a faraday cage and as protection against observation. *Dangers: Process Fatigue.*

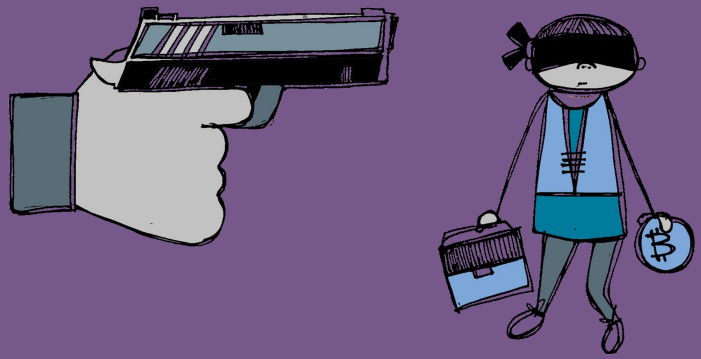
Cold Storage Solutions:

1. **Create Tamper Evidence.** Store keys or other secret materials in tamper-evident bags; place padlocks on your Cryptosteel. *Dangers: Process Fatigue.*
2. **Obscure or Protect Your Keys.** Store keys in an obscured way that would be readily obvious to the asset holder, but not to a thief. Alternatively, protect keys with a PIN or other code. *Dangers: Key Fragility.*
3. ***Cold Storage Scenario Optional Steps:*** Use Bags (Tamper Evident), Use Redundant Metal Tiles, Use a Safety Deposit Box.

Coercion

“I know you have cryptocurrency. Well, I’ve got power in the real world. I can threaten you, your family, your friends, your home, or your business — and, I can follow through on those threats! I want to get what you have, and I’m going to force you to give it to me by any means necessary.”

- An entity, whether it be a nation-state, a terrorist group, the mob, or a smart mugger, can threaten a cryptocurrency holder with the goal of forcing them to give away their funds (or in some other way corrupt the cryptocurrency market). Though there are solutions that absolutely prevent this sort of coercion from succeeding, they also place the victim in danger of the risks being carried out anyway, especially if the activated solutions are not understood by the public beforehand and are not provably activated. Often the best solution is to cooperate, or at least to seem to cooperate, in order to avoid severe consequences.



Coercion

Case Studies

Abstract Case Study: SWATing. Over the course of a month, Dan's power and his DSL line are turned off. He contacts the utilities and is told that these occurred at his request. He then receives an email that says, "we know where you live, send us half your bitcoins or next time we swat you and maybe you end up dead." A picture of his house from Google Street View is included.

Historical Case Study: Kidnapping. Ukranian cryptocurrency exchange executive Pavel Lerner was grabbed off the street outside his office, and held in an undisclosed location. He was told that he would not be released unless he paid $1 million dollars in bitcoins. *News Story*

Coercion

Risks and Controls

Risks:

1. **Death.** An asset holder's life could be threatened if they do not comply.
2. **Funds Loss.** The goal of coercion is usually to steal funds.
3. **Physical Damage.** An asset holder could be threatened with torture or permanent disability if they do not comply.
4. **Physical Detention.** An asset holder could be kidnapped and held until they comply.

Solutions:

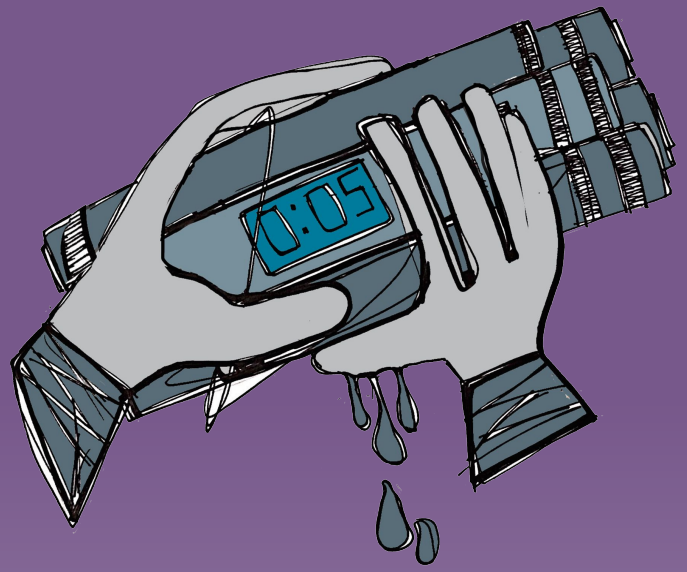
1. **Create False Funds.** Create a lesser cache of funds to be given over in case of coercion. Some hardware wallets support this with a "plausible deniability" or "alternate passphrase" function.
2. **Limit Funds Spending.** Use smart custody options to limit what funds can be spent at one time. *Dangers: User Error.*
3. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.
4. **Use Funds Multisignatures.** Lock funds with a multisignature, which requires two or more people (possibly from a larger group of people) to sign off for use of funds. *Dangers: Internal Theft, User Error.*
5. **Use Funds Timelocks.** Lock funds with a timelock, which doesn't allow a specific person to access the funds until a specific time. Create a regular procedure to update the timelock as it nears expiration. *Dangers: User Error.*
6. **Require Public Interaction.** Cross thresholds that put an adversary at risk. Store one of the necessary keys at a physical location where interactions with other people can be judged for signs of coercion. Include the presence or status of your loved ones in the judgements. Establish code words that actually mean, "Help"! Make the procedure slow enough that help could arrive. *Dangers: Process Fatigue.*

See Related — Nation-State Actor, Terrorist / Mob

Terrorist/Mob

“I want your money and I am willing to kill, maim, or destroy to get it. Plus, I’ve got a reputation to uphold. If you force me to, I will have to do bad stuff. I ain’t worried about the legal repercussions, because I’m already subverting the whole system.”

- In large part, a terrorist or mob adversary is a special case of the “coercion” adversary. A terrorist organization or an organized crime organization is likely to use coercion to acquire cryptocurrency funds, but they’re more likely than most to carry through on mortal threats if they are foiled via various Smart Custody solutions that can be used to protect cryptocurrency from coercive threats. On the flip-side, since they’re innately criminal organizations, a nation-state might offer protection against them.



Terrorist/Mob

Case Studies

Abstract Case Study: Killing Uncle Bob. Alice is too open about her bitcoin holdings, and the local mob finds out. Mallory, a representative of the mob, tells her that they'll kill her Uncle Bob if she doesn't make a payment of 10 bitcoins to a specific address. She refuses and they kill Uncle Bob.

Terrorist/Mob

Risks and Controls

Risks:

1. **Cascade: Coercion.** The threats of a criminal adversary are almost entirely coercive.

Process Solutions:

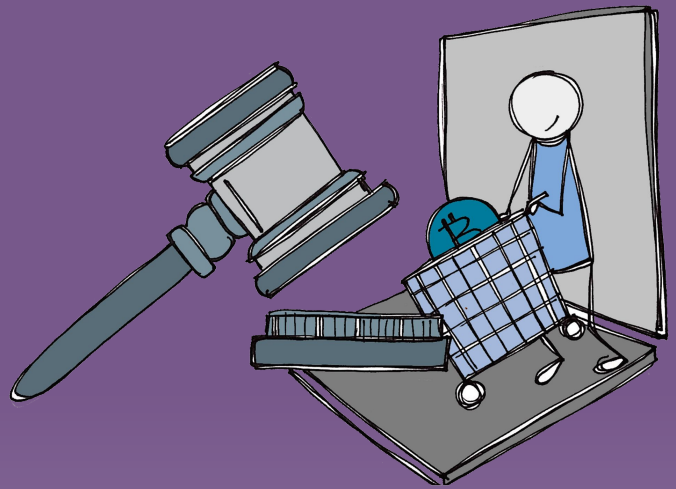
1. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.
2. **Register Your Funds.** Register and document your funds fully with your nation-state to maximize legal protections. *Dangers: Legal Forfeiture, Nation-State Actor.*

See Related — Coercion

Legal Forfeiture

“I desire your funds, please, but only because I am rightfully owed them. You violated a contract, neglected to pay a bill, or were held liable for a tort. So, pay up.”

- Just like any other asset, cryptocurrency can be subject to legal forfeiture. This is usually not considered an issue, under the assumption that forfeiture as part of a civic lawsuit or state action is legal. However, it becomes very problematic if a nation-state is corrupt and has been bribed by a party to a lawsuit or is attacking the asset holder illegally, for its own self-interest. Even a legitimate nation-state might allow its citizens to fall prey to fraudulent lawsuits.



Legal Forfeiture

Case Studies

Abstract Case Study: Extorting Legally. Mallory discovers that Carol has bitcoins. She walks up to her door on an cold day where there's ice on the ground and *whoops* falls down. She soon has a doctor proclaiming that she's been crippled for life. Mallory then uses the legal system to seize Carol's bitcoins.

Legal Forfeiture

Risks and Controls

Risks:

1. **Funds Loss.** Obviously the danger of legal forfeiture is the loss of the funds themselves.
2. **Cascade: Denial of Access.** A legal forfeiture can sometimes cause a purposeful denial of access to a house, safe, or safety deposit box.

Process Solutions:

1. **Neutrally Store Your Funds.** Maintain funds or keys outside of the sphere of control of fascist and authoritarian nation-states.
2. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.

Transaction Error

“I am the slightest error in a transaction. I’m the script that can’t complete, the address that goes to the wrong place, or even the fee that wasn’t big enough. I want your transaction to do something that you don’t expect. I am startling results that are ultimately detrimental to you.”

- Errors introduced into a transaction can lead to the loss of some or all funds. Though it is hard to simply mistype an address in Bitcoin, due to error-checking, there are other potential threats. A Transaction Error could be due to an Personal Network Attack (where an attacker substituted an address), or it could be due to system error (where a system produced an incorrect address).
- There can be other transaction issues too, such as sending the wrong type of transaction (e.g., a P2PKH when a multisig or smart contract was intended) or paying too high of a fee or paying to a cryptocurrency fork.
- The fundamental issue is lack of transparency in the address itself and in the overall transaction, both of which are natively represented as somewhat intimidating sets of letters and numbers. Anything that improves that transparency, or that tests those computer values, addresses this adversary.
-
-

Transaction Error

Case Studies

users' wallets. Later, Frank moves some money. He intends to send it to one of his wallet own addresses, but when he's looking at his wallet, he accidentally copies Mallory's sender address rather than his own recipient address. The money transfer goes to Mallory.

Abstract Case Study: Waiting Out the Clock. Bob writes a script with a Timelock for a time of 1609459200, so that the transaction will unlock on January 1, 2021. Except he forgets the last digit, and instead sets it to 160945920. Since the lock time is less than 500 million it's interpreted as a blockheight; at a block every 10 minutes, those funds will become available again in a bit more than 3,000 years.

Abstract Case Study: Paying the Miners. Carol sends $100 (.01 BTC) from an old 1 BTC transaction that she got in the early days of the technology. She remembers to send the remainder to a change address, but is confused over the value of the original transaction and only sends herself .48 rather than the .98 BTC that she intended. She doesn't double-check her math, nor does she use an interface that does so. The happy miner of her transaction earns about $5,000 from her.

Historic Case Study: Hacking the CoinDash ICO. While CoinDash was conducting an ICO, hackers broke into their web site and replaced the funding address with one of their own. $7 million dollars in Ethereum were sent to the hackers instead of CoinDash. *News Story*.

Transaction Error

Risks and Controls

Risks:

1. **Funds Delay.** The least problematic sorts of transaction error just lead to delayed funds, where you have to resend them when you realize that you messed up.
2. **Funds Loss.** In the worst cases, all of the funds could be lost due to sending it away or due to theft after not locking it with the intended sort of signature.
3. **Funds Vulnerability.** Locking a transaction with the wrong sort of signature can alternatively just make the funds more vulnerable: now, a single person can sign for them rather than multiple people.
4. **Partial Funds Loss.** A fee-related transaction error is an example of partial funds lost: Perhaps you paid $100 instead of $10 or $1 — though this is a situation where most interfaces have gotten better at preventing errors over time.

Process Solutions:

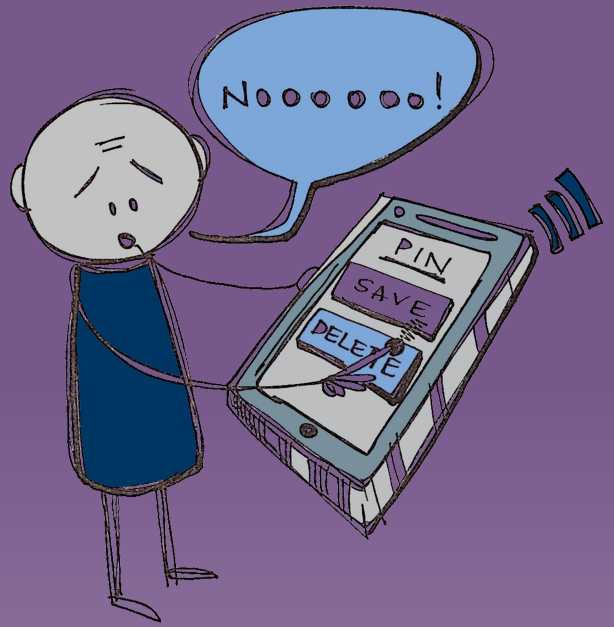
1. **Check Your Work.** Double-check your work; even better, have someone else double-check your work; even better, have an official procedure requiring someone else to double-check your work.
2. **Create Checklists**. Create simple checklists and print many copies. Physically check each box as you work down your list of procedures.
3. **Take the Time.** Be very careful when you're working. Double-check everything. Don't take transferring large amounts of funds lightly, ever.
4. **Verify Your Scripts.** Double-check that your script has valid responses. For large-scale funds held by a script, you may want to first test them with smaller amounts of funds. *Dangers: Correlation*.
5. **Verify Your Transactions.** Double-check the recipient addresses for any transactions. Make sure the change address really belongs to you. Make sure that the fee looks rational. Validate the transaction on testnet to verify it.

See Related — Key Fragility, User Error .

User Error

“I’m that niggling mistake that wouldn’t be a major problem in most financial situations. I want you to make a typo or to use the wrong address, so that you don’t get your money or send it to the wrong place. I want you to lose your keys, so that you can’t recover your funds. I am all the anxieties you have about Bitcoin made real.”

- Funds could be lost due to a user mistake. This can overlap with Key Fragility if the asset holder doesn’t correctly record his key; or with Transaction Error if the asset holder doesn’t correctly record an address. However, there are other possible errors in the Bitcoin ecosystem such as falling for a phishing attempt or forgetting to pay for a safety deposit box. Many other adversaries can cascade from user errors, so be careful..
-
-



User Error

Case Studies

Abstract Case Study: Forgetting the PIN. Alice has heard of other people losing their PINs, but knows it can't happen to her. But then she types in the wrong PIN three times to her Ledger, and it erases her keys.

Abstract Case Study: Forgetting to Pay for a Safety Deposit Box: Dan has put his recovery phrase on a piece of paper that is located in his safe deposit box. He forgets to notify his bank of an address change, and they seize the contents of the box, shredding its paper contents as there are no valuables. Unclaimed Property Article.

User Error

Risks and Controls

Risks:

1. **Funds Loss.** There's no arbiter on the Bitcoin network, so if an asset holder makes a mistake, funds can be irretrievably lost.
2. **Cascade: Key Fragility.** A User Error can cause incorrect key recording.
3. **Cascade: Transaction Error.** A User Error can cause incorrect address recording, or foul up other elements of a transaction.

Process Solutions:

1. **Check Your Work.** Double-check your work; even better, have someone else double-check your work; even better, have an official procedure requiring someone else to double-check your work.
2. **Create Checklists**. Create simple checklists and print many copies. Physically check each box as you work down your list of procedures.
3. **Take the Time.** Be very careful when you're working. Double-check everything. Don't take transferring large amounts of funds lightly, ever.
4. **Verify Your Keys.** Test that your key is correct by signing and verifying a test message using your key. If you're really paranoid, create a test transaction using your private key or create and send a small transaction from your funds. *Dangers: Correlation.*
5. **Verify Your Transactions.** Double-check the recipient addresses for any transactions. Make sure the change address really belongs to you. Make sure that the fee looks rational. Validate the transaction on testnet to verify it.

***Cold Storage Scenario* Optional Steps:** None.

See Related — Key Fragility, Transaction Error

Censorship

“I don’t want your money, I just want to make sure you can’t have it. But, I have a deeper motivation than that. Maybe I’m threatening you, maybe I’m blackmailing you, and maybe I’m getting my revenge. Whatever the case, I personally know you, I know you have cryptocurrency, and I’m making sure that you can’t use it.”

- An entity or a consortium of entities can potentially prevent an asset holder from transacting their cryptocurrency. This may be a simple denial-of-service (DOS) attack on the asset holder or on their ISP. Alternatively, it could be a more nefarious agreement among miners or block signers to not include the asset holder’s transactions in blocks. This can be a very expensive problem to resolve, which means that the best solution is to make sure that no one knows who you are, and thus doesn’t know who to censor.

Censorship

Case Studies

Abstract Case Study: Extorting Funds. Frank is open about his bitcoin wealth and freely posts his contact info on bitcoin forums. He gets an email saying that his transactions will no longer be processed if he doesn't pay a consortium 1% of his bitcoin funds. Indeed, his transactions stop going through.

Historic Case Study: Blocking WikiLeaks. WikiLeaks was blockaded by several traditional financial institutions such as Mastercard, VISA, and PayPal in December 2010. Afterward, Satoshi Nakamoto is reputed to have asked WikiLeaks not to use bitcoins for donations, and some miners were reluctant to process WikiLeaks transactions. However, there wasn't sufficient consensus to extend the financial blockade to bitcoin. *News Story*, *Another New Story*.

Censorship

Risks and Controls

Risks:

1. **Funds Denial.** Though the asset holder still has complete access to his key and thus exclusive access to his funds, he can't actually use them, so they might as well be lost (until something is done to clear up the censorship).

Process Solutions:

1. **Practice Anonymity.** Do not let people know you have bitcoins; ensure that you in no way ever link your key to your real persona.
2. **Practice Key Hygiene.** Follow the best practices of using different addresses for every transaction that you conduct. Each time you make a transaction with the same address, you are leaking information to your counterparty, which could be used to identify and either censor or correlate future transactions.
3. **Request Preferential Mining or Mine Your Own Blocks.** Gain control of some portion of the block creation infrastructure, most likely by purchasing enough mining power that you can occasionally generate a block. Of, more simply, pay a miner directly to mine your transaction.

Hot Wallet Solutions:

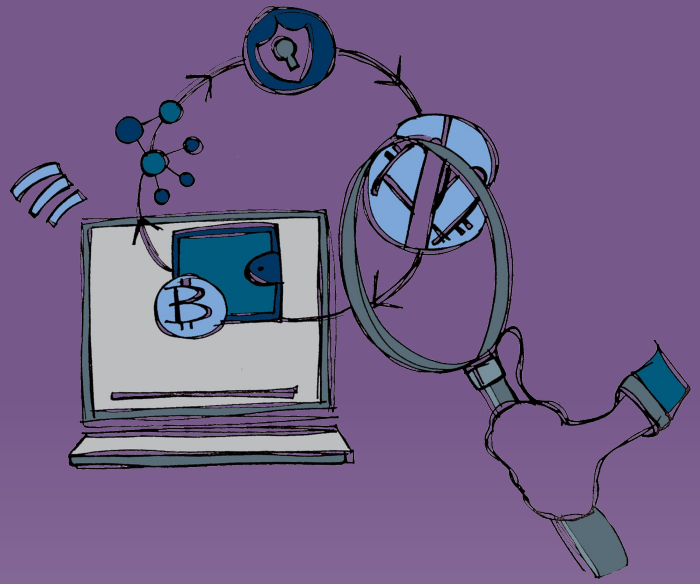
1. **Question Policies & Procedures.** Know the security policies and procedures of any company that you're working with; be sure that they have rigorous, well-documented security procedures that they follow religiously, and that they treat any variance from their procedure as a problem that must be investigated. Also, be sure that there are no negative policies that might affect your usage of its services.

See Related – Correlation.

Loss of Fungibility

"I want to figure out how your cryptocurrency has been used in the past. That way, I can decide whether to accept your funds based on their history. Maybe they were used for criminal activities or maybe they were stolen; I don't want to accept those tainted funds. Or maybe they were owned by someone I don't like, and I'm trying to punish people for transacting with them. Whatever the reason, it's vital that I be able to backtrack the history of your coins."

- Fungibility presumes that all bitcoins (or other cryptocurrency units) are indistinguishable and interchangeable.
- This ensures that all currency has the same value: a bitcoin doesn't become more valuable because (for example) it was held by Satoshi or less valuable because (for example) it was used to pay for illegal activities. Unfortunately, the fungibility of Bitcoin is in danger because some exchanges and wallet services have begun using tracing services; worse, they have begun freezing accounts where they don't like their activities.



Loss of Fungibility

Case Studies

Abstract Case Study: Gambling with Funds. Dan stores his funds at an exchange. He uses some of them to try out a Bitcoin gambling site, and the next time he returns to the exchange he finds his account locked because he's violated a no-gambling policy that was created by the exchange to pacify the US Department of Justice.

Loss of Fungibility

Risks and Controls

Risks:

1. **Funds Denial.** The big problem with loss of fungibility is that the entire cryptocurrency ecosystem might become unwilling to accept a coin with a bad history.
2. **Key Loss.** More trivially, if you find your account locked by a particular exchange, you might lose access to key stored there for a while.

Process Solutions:

1. **Practice Anonymizing Your Funds.** Occasionally use methods like CoinJoin, SendShared, or Zerocoin to anonymize your transactions. On Blockstream's Liquid, always make use of Confidential Transactions.

Hot Wallet Solutions:

1. **Create Cold Storage Procedure.** Adapt a Cold Storage Procedure that moves some or all of your funds off of your hot wallet. Only keep keys on an exchange or brokerage for the minimum amount of time required to make a transaction. *Dangers: Disaster, Casual Physical Theft*.
2. **Question Policies & Procedures.** Know the security policies and procedures of any company that you're working with; be sure that they have rigorous, well-documented security procedures that they follow religiously, and that they treat any variance from their procedure as a problem that must be investigated. Also, be sure that there are no negative policies that might affect your usage of its services.

Step 1
Set up Safe

Step 2
Set up live operating system

1. Setup Safes
    a. Install Home Safe

       Ideally it should be physically secured by mounting it to floor or wall joists, or even more securely, directly to a foundation.

    b. Order Safe Deposit Box

       Recommendations:

        i. Associate it with a joint bank account with at least one of your heirs.
        ii. Have sufficient funds in the joint bank account for several years of bank fees and box fees.
        iii. Have the safety deposit box be in both person's names.

2. Setup Computer on USB Drive
    a. Create a new bootable operating system on a USB Memory Stick (or USB hard drive)
    b. Format the external USB device
    c. Download the installer for your OS
    d. Install the OS to the external USB drive
    e. Boot drive from USB (This will be very slow! It is ok.)

Step 3 Create Master HD Seed on Ledger

1. Start Up Ledger Live
2. Initialize Your Ledger
3. Create Your PIN
4. Write the PIN and the Date that the key was generated using permanent marker on waterproof paper page
5. Hit “Continue” in Ledger Live to get the next instructions, then follow along on screen or below.
6. View Recovery Phrase
7. Write down Recovery Phrase, adding it to the waterproof paper page
8. Finish setting up your Ledger in Ledger Live
9. Upgrade Ledger (if Needed)
10. Prepare Ledger Live for Bitcoin usage
11. Write the date the key was generated, the Ledger firmware version number, and the Bitcoin app version number on waterproof paper.)

Step 3 Create Master HD Seed on Ledger

1. Start Up Ledger Live
2. Initialize Your Ledger
3. Create Your PIN
4. Write the PIN and the Date that the key was generated using permanent marker on waterproof paper page
5. Hit “Continue” in Ledger Live to get the next instructions, then follow along on screen or below.
6. View Recovery Phrase
7. Write down Recovery Phrase, adding it to the waterproof paper page
8. Finish setting up your Ledger in Ledger Live
9. Upgrade Ledger (if Needed)
10. Prepare Ledger Live for Bitcoin usage
11. Write the date the key was generated, the Ledger firmware version number, and the Bitcoin app version number on waterproof paper.)

Regulatory considerations

What are regulatory risks to keep in mind when dealing with cryptoassets?

Regulatory trends

- Regulators are increasingly scrutinizing market exchanges driven by cybersecurity hacks, unusual trading patterns and manipulative trading practices
- Regulators are beginning to crackdown on initial coin offerings (ICOs), SEC chairman called nearly all ICOs securities and exchanges that trade them will need to abide by SEC regulations
- Similar to tax-haven jurisdictions, crypto-friendly jurisdictions are beginning to emerge, e.g., Zug, Switzerland

Active Promotion	Light Touch Regulation	Strict Regulation	Aggressive Regulation
Japan	United States	South Korea	China
Singapore	Switzerland	Indonesia	
Isle of Man	United Kingdom	Russia	

Cryptoassets have unique regulatory considerations

Cryptocurrencies are never ‘held’, they are only controlled. How they are controlled raises some interesting regulatory questions.

- Sanctions and the Travel Rule: there is no geographic indicator in cryptocurrency transactions
- Mining fees: there is no way to determine the location of a bitcoin miner, and consequently, the party to whom mining fees are sent
- Multisig transactions: what are the implications when any X of Y key holders can send a transaction?
- Freely created addresses: anyone can create and control an address anonymously

Not all cryptoassets are alike

Creating assets on a publicly available blockchain means that by default, assets can be sent to anyone. Consequently there is difficulty enforcing regulations across borders.

- Securities regulations: many cryptoassets meet the Howey Test
- KYC and asset distribution: how are cryptoasset owners identified? Are they accredited?

FinCEN, SEC, IRS have found a lack of compliance in the industry

A selection of comments from an Aug. 9 speech to the Block (Legal) Tech conference at Chicago-Kent College of Law:

- FinCEN and IRS have examined over 30 percent of all registered virtual currency exchangers and administrators since 2014
- FinCEN noted money laundering controls are not put in place until a trading platform or peer-to-peer exchanger gets an investigation notice. (The government receives more than 1,500 suspicious activity reports a month involving virtual currency)
- FinCEN, on the openness of blockchain transactions: “When we say that everything is on the blockchain, I’m not so sure that’s true.”
- The SEC, regarding token sales: “It’s not sufficient to say we don’t intend to offer it to U.S. investors. What steps did you take to insure that U.S. investors cannot be part of this offering?”
- IMF: the speed and efficiency of blockchain transactions creates new openings for bad actors

There are technologies and tools available to analyze blockchains and provide compliance support

- Cryptocurrency analytics firms perform advanced analytics to identify and deanonymize activity
- Used with success in multiple cryptocurrency crime investigations
- Other tools include AML/KYC, transaction monitoring

Instructions for use

EDIT IN GOOGLE SLIDES

Click on the button under the presentation preview that says **"Use as Google Slides Theme"**.

You will get a copy of this document on your Google Drive and will be able to edit, add or delete slides.

You have to be signed in to your Google account.

EDIT IN POWERPOINT®

Click on the button under the presentation preview that says **"Download as PowerPoint template"**. You will get a .pptx file that you can edit in PowerPoint.

Remember to download and install the fonts used in this presentation (you'll find the links to the font files needed in the Presentation design slide)

More info on how to use this template at www.slidescarnival.com/help-use-presentation-template

Hello!

I AM JAYDEN SMITH

I am here because I love to give presentations.

You can find me at @username

“

Quotations are commonly printed as a means of inspiration and to invoke philosophical thoughts from the reader.

1

Transition headline

Let’s start with the first set of slides

This is a slide title

- Here you have a list of items
- And some text
- But remember not to overload your slides with content

Your audience will listen to you or read the content, but won’t do both.

Big concept

Bring the attention of your audience over a key concept using icons or illustrations

You can also split your content

White

Is the color of milk and fresh snow, the color produced by the combination of all the colors of the visible spectrum.

Black

Is the color of coal, ebony, and of outer space. It is the darkest color, the result of the absence of or complete absorption of light.

In two or three columns

Yellow

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

A picture is worth a thousand words

A complex idea can be conveyed with just a single still image, namely making it possible to absorb large amounts of data quickly.


Want big impact?
Use big image.

Use diagrams to explain your ideas

And tables to compare data

	A	B	C
Yellow	**10**	**20**	**7**
Blue	**30**	**15**	**10**
Orange	**5**	**24**	**16**

Maps

89,526,124

Whoa! That’s a big number, aren’t you proud?

89,526,124$

That’s a lot of money

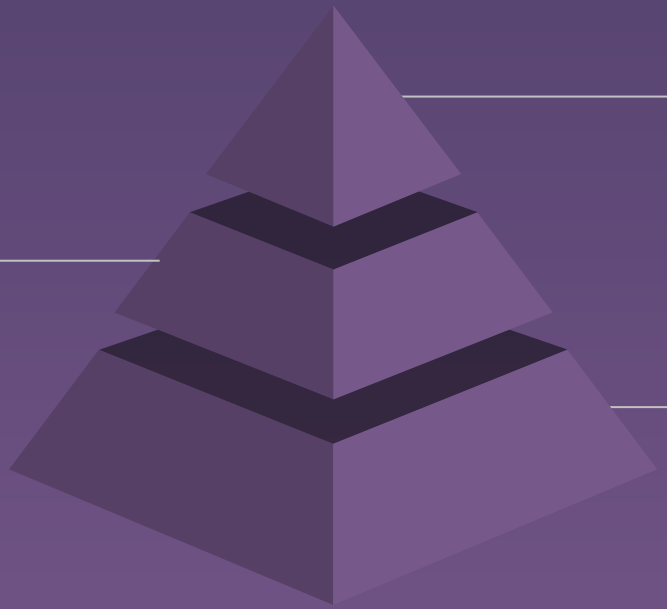
185,244 users

And a lot of users

100%

Total success!

Our process is easy



Vestibulum congue tempus

1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor. Donec facilisis lacus eget mauris.

Vestibulum congue tempus

2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor. Donec facilisis lacus eget mauris.

Vestibulum congue tempus

3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor. Donec facilisis lacus eget mauris.

Let’s review some concepts

Yellow

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

Yellow

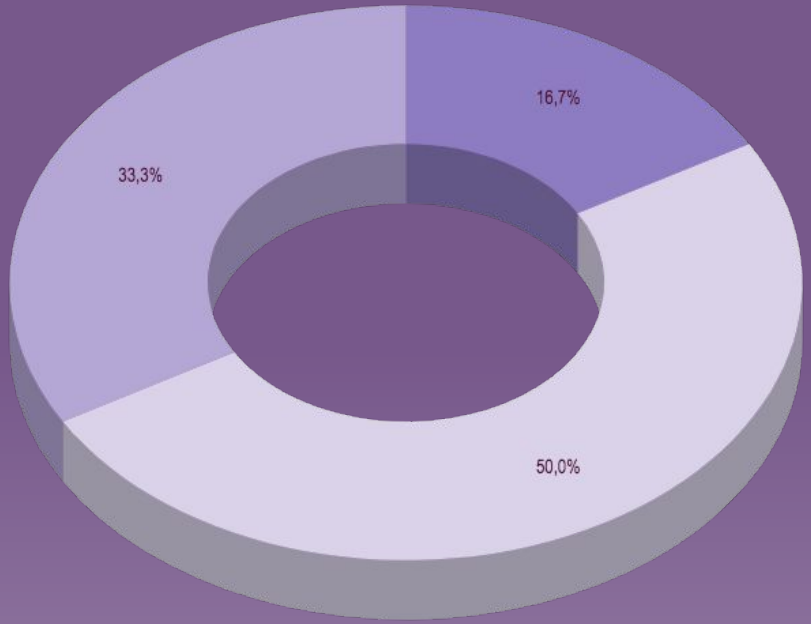
Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

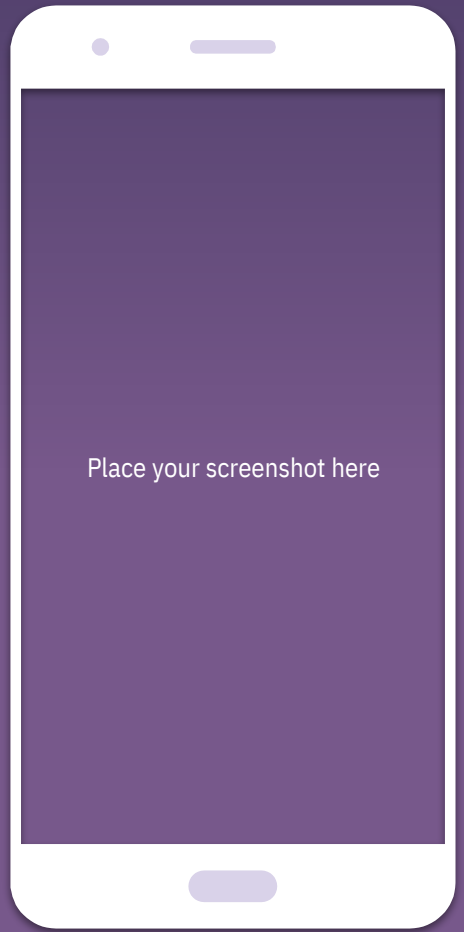
Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.



You can insert graphs from Google Sheets

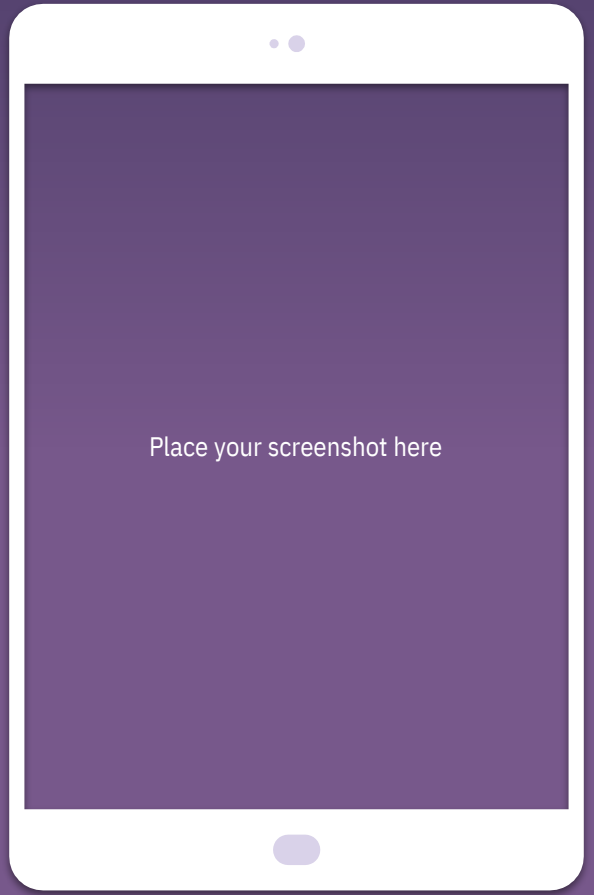
Mobile project

Show and explain your web, app or software projects using these gadget templates.



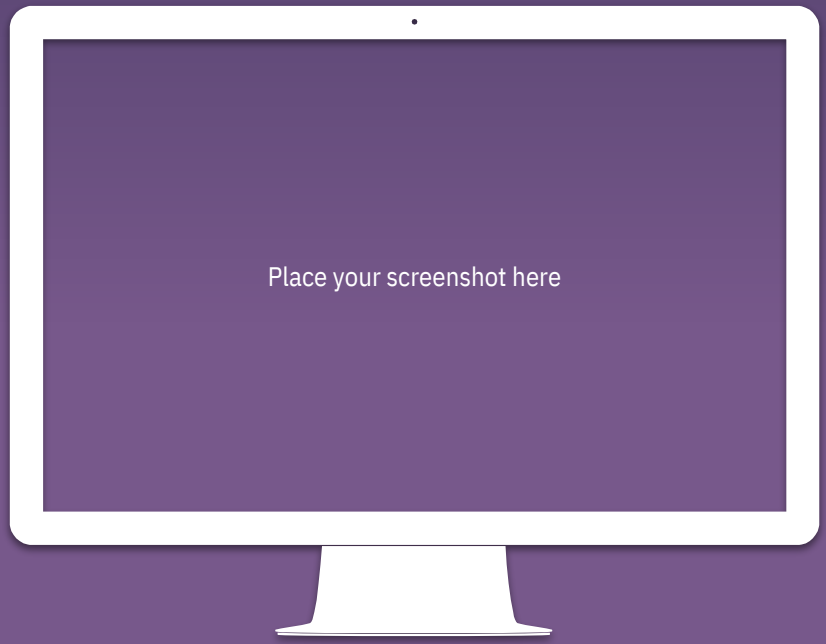
Tablet project

Show and explain your web, app or software projects using these gadget templates.



Desktop project

Show and explain your web, app or software projects using these gadget templates.



Thanks!

ANY QUESTIONS?

You can find me at

- @username
- user@mail.me

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash

Presentation design

This presentation uses the following typographies:

- Titles: IBM Plex Sans Semibold
- Body copy: IBM Plex Sans Regular

You can download the fonts on this page:

https://github.com/IBM/plex/tree/master/IBM-Plex-Sans/fonts/complete/otf

You don’t need to keep this slide in your presentation. It’s only here to serve you as a design guide if you need to create new slides or download the fonts to edit the presentation in PowerPoint®

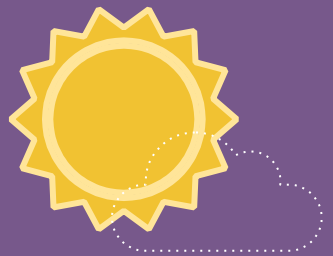
SlidesCarnival icons are editable shapes.

This means that you can:

- Resize them without losing quality.
- Change fill color and opacity.
- Change line color, width and style.

Isn't that nice? :)

Examples:



Now you can use any emoji as an icon!
And of course it resizes without losing quality and you can change the color.

How? Follow Google instructions
https://twitter.com/googledocs/status/730087240156643328