Bitkey

A deep dive and honest review

PRESENTED BY

Bitcoinology

Introduction to BitKey

- New self custody solution
- For the broader market (just works^{TM})
- **No seed words** means less stress
- Easy to setup and use
- But there are trade offs in its design as all products have

Requirements for setup

- Bitkey device
- Smartphone (Android/iPhone)
- Bitkey app (Google Play Store / Apple App Store)
- Google Cloud or iCloud account
- Phone number and email
- **Trust in Blocks infrastructure and discretion**

Setup flow

- Download app
- Tap device
- Register for service via Block (easy)
- Some back and forth with device
- Wallet

For those who don’t trust, verify.

- Open Source => Server, Server Infra, App, Firmware
- Verifiable Builds => Only APK
    - iOS promised with no deadline

Headline features

- Turnkey security model
- User friendly and easy to use
- Provides a lifeline for “when life happens”
- Integration with exchanges and providers
- Blend of convenience, security and safety nets

Bitkey’s security model

- Three key system
  - Bitkey device
  - Smartphone
  - Block’s servers
- Any combination of two keys can control your bitcoin
  - Provides a lifeline for losing one key at any one time
  - Ticking time bomb is better than a trigger bomb, but a bomb nonetheless
  - Steel punched backup of single key could still be more resilient over time

Bitkey’s security model

- No seed words
    - No need to worry about where and how to store a critical “password”
- Familiar
    - Uses tools and services you are probably already familiar with
- Extra lifeline
    - Resilient to losses or thefts
    - Limited: don’t let this make you complacent!

Single sig vs Bitkey

- Bitkey better prevents theft
  - Device stolen:
    - 1 key is not sufficient to steal, slow recovery path available, email and SMS under your control
  - Hot key extracted:
    - 1 key is not sufficient to steal but can start slow recovery if email and SMS also compromised, 2 keys = immediate recovery
- Single sig better prevents loss
  - Given safe living environment and not public figure
  - Stamped metal is harder to destroy
  - BUT In case of theft, race to block confirmation or race to 100% fees
- **Multi Sig:** Single backup may be easier to track/monitor

Bitkey’s recovery model

- Cloud backups for lost phone
    - Smartphone key encrypted and locked to Bitkey device
    - Smartphone key encrypted and locked to Social contact’s device
- Delay & notify for lost device (or cloud + phone)
    - Requires proof of one key
    - Relies on at least one uncompromised SMS or Email to prevent illegitimate theft

Bitkey’s recovery model

- Break glass
  - Protects against removal from app store and loss of phone in tandem
  - Break glass kit stored in cloud (user space)
  - Requires recovery app found online (independent source)
    - Can configure custom electrum server
  - Requires bitkey device
  - One flavour: not for power users, but sideloading app complex for average consumer, Block open to community solutions

Not a hardware wallet?

- https://www.zherbert.com/bitkey/
- Written by co-founder and CEO of Foundation
- Calls this “an insecure hardware wallet”:
  - *A hardware wallet's raison d'etre is to provide a trusted, offline environment for confirming transaction details before sending*
- Maybe this is a “self recoverable hot wallet”
  - Not as insecure as storing your keys in an email or using an insecure password to an account
  - My biggest fear for others is when they lose their phone or change phone without giving a second thought about their bitcoin

Security tradeoffs

- No ability to backup device for resiliency[??]
- Fingerprint lock (physical bypass)
- No screen (malicious app/device, open source, verifiable builds)
- No interoperability (limited use, less audits, trust vendor)
- Data collection (risk of data leaks, government compliance)

Privacy Considerations

- You give out your email and phone number
  - Not typically a concern for people
  - Linking your online identity to Bitcoin via Block
  - Both communication channels used to phish or target you
  - Potentially activity data leaked alongside
  - Very specific, limited uses
    - **Only used to cancel**, cannot be used to authorize*
  - Could create and use burner details?
    - High risk of losing access to burner channels
    - Not typical consumer behaviour

Privacy Considerations

- Block can see all of your wallet activity (xpub)
- Block could collect your IP addresses and other identifiers
- Block could audit and block transactions made via Server
- More convenient UX may introduce more usage and activity tracking
- All integrated exchanges require login and/or personal info (UK only?)

Recovery scenarios

- Loss of smartphone: cloud
- Loss of cloud account: phone + device
- Loss of both smartphone and cloud account: social or delay + notify

Loss of Bitkey device

- Delay + notify required
- Requires purchase of new BitKey device*
- Sweeps to one UTXO
- Transaction fees to recover

Social recovery mechanism

- What is social recovery?
    - Involves trusted contacts
    - Setting up and using Social Recovery
    - How one contact can help restore access
- Security considerations for trusted contacts
    - Uses cloud (could be same platform)
    - Requires contact to install app
    - Requires contact to coordinate in time of crisis
    - Unclear why Block involved in inter-party communications

Summary

- Social recovery optional but worth encouraging
- Lost phone key, restored by cloud and device
- Lost device, delay + notify
- Lost phone and device, restore by cloud **and contact** then delay + notify
- Lost phone key and cloud, delay + notify
- Break glass kit **requires cloud and device***

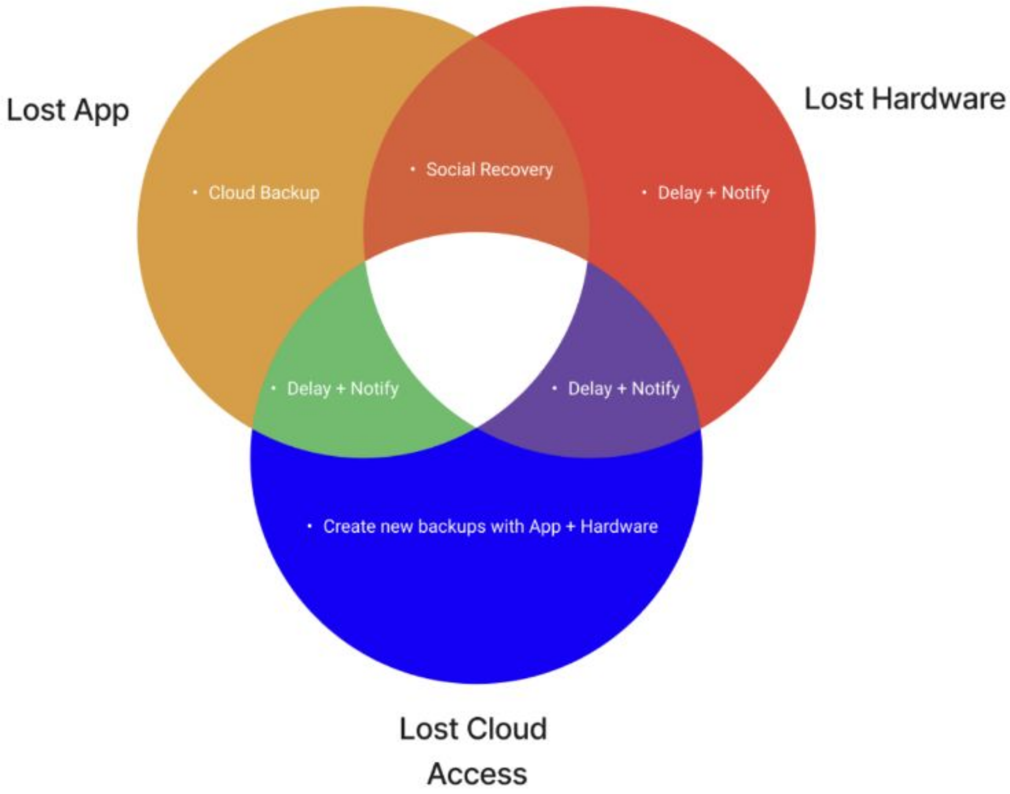


Figure 1: Recovery tools used for different loss scenarios.

What if Block disappears?

- No fault of your own
- How notify?
- Options
  - Mobile app + device
  - Break glass kit
- Need to find another wallet
- **Need to take action**
- Not “cold storage” (2 hot keys) / (1 of 2 fragile key)

How to assess the risk of losing your bitcoin

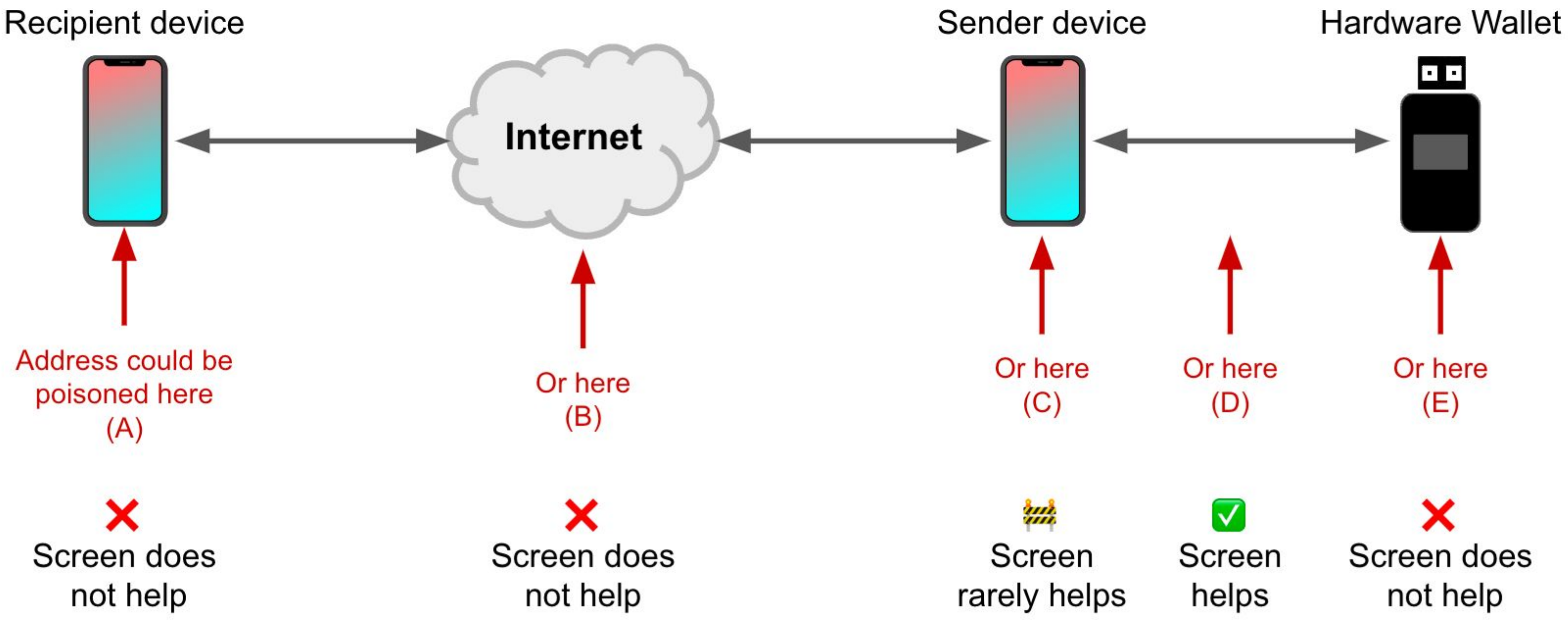
- Scenario 1:
  - > Hackers breach Block’s servers and find a key linked to your email and phone number
  - > Hackers breach your iCloud/Google Cloud account and find your app key
  - You’ll probably hear about Block’s breach, but it ain’t good
  - It is still better than putting your trust in a Coinbase where only half the work is needed
- Scenario 2:
  - > Hackers steal your Bitkey device
  - > Hackers breach your iCloud/Google Cloud account and find your app key
  - You will hopefully know if your Bitkey device is stolen, maybe not if maid attack
  - Although fingerprint is a barrier, it is probably easy to get if they can steal your bitkey
  - A local thief is unlikely to be an online hacker, you would need to be targeted, or it would likely be someone you know

To summarise

- Not for the hardcore, paranoid or technology skeptics
- Social backup is a nice touch
- It IS self custody
- It is NOT cold storage
- Smooth and familiar
- Convenient to use
- Still being developed

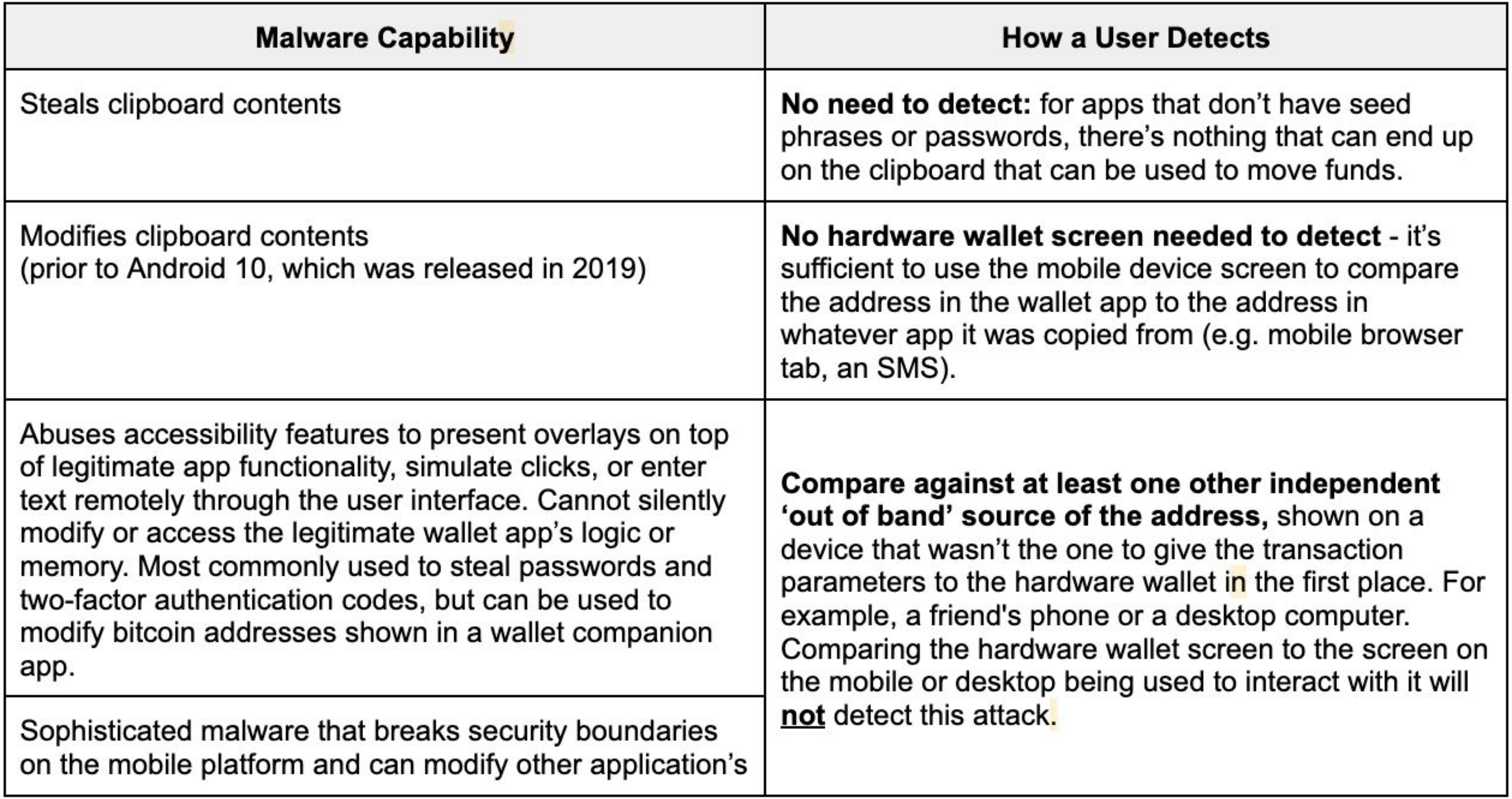
Screens are not a panacea

- https://bitkey.build/screens-are-not-a-panacea/



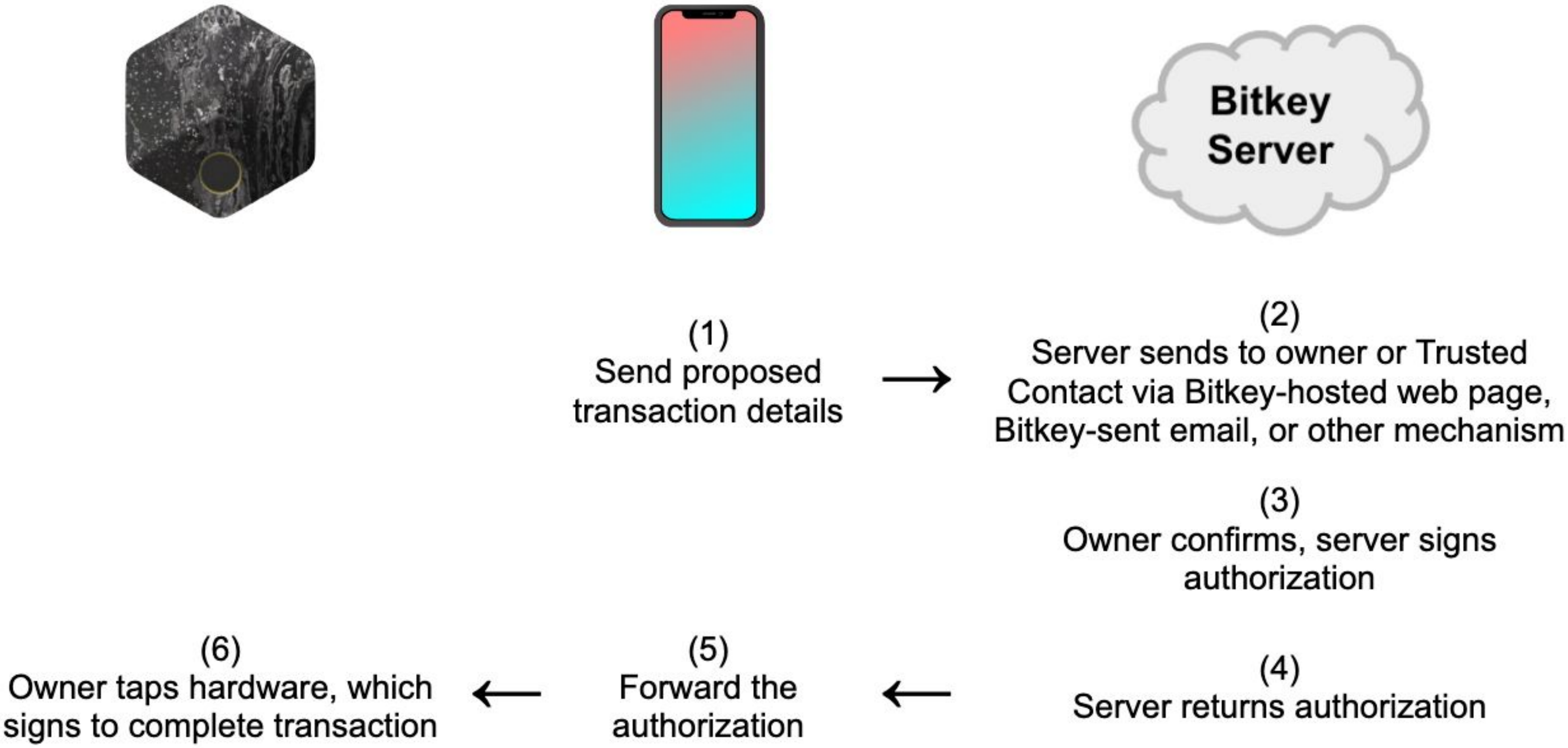
Screens are not a panacea

If the sender's internet-connected device is sufficiently compromised, then the destination address can be poisoned before it ever gets to the hardware wallet. **When that happens, comparing the address shown on the hardware wallet screen to the address shown on the sender's phone or desktop will always result in a match – because the process is comparing garbage to garbage.**



Malware Capability	How a User Detects
Steals clipboard contents	**No need to detect:** for apps that don't have seed phrases or passwords, there's nothing that can end up on the clipboard that can be used to move funds.
Modifies clipboard contents (prior to Android 10, which was released in 2019)	**No hardware wallet screen needed to detect** - it's sufficient to use the mobile device screen to compare the address in the wallet app to the address in whatever app it was copied from (e.g. mobile browser tab, an SMS).
Abuses accessibility features to present overlays on top of legitimate app functionality, simulate clicks, or enter text remotely through the user interface. Cannot silently modify or access the legitimate wallet app's logic or memory. Most commonly used to steal passwords and two-factor authentication codes, but can be used to modify bitcoin addresses shown in a wallet companion app.	**Compare against at least one other independent 'out of band' source of the address,** shown on a device that wasn't the one to give the transaction parameters to the hardware wallet in the first place. For example, a friend's phone or a desktop computer. Comparing the hardware wallet screen to the screen on the mobile or desktop being used to interact with it will **<u>not</u>** detect this attack.
Sophisticated malware that breaks security boundaries on the mobile platform and can modify other application's	

Screens are not a panacea



(1)
Send proposed transaction details →

(2)
Server sends to owner or Trusted Contact via Bitkey-hosted web page, Bitkey-sent email, or other mechanism

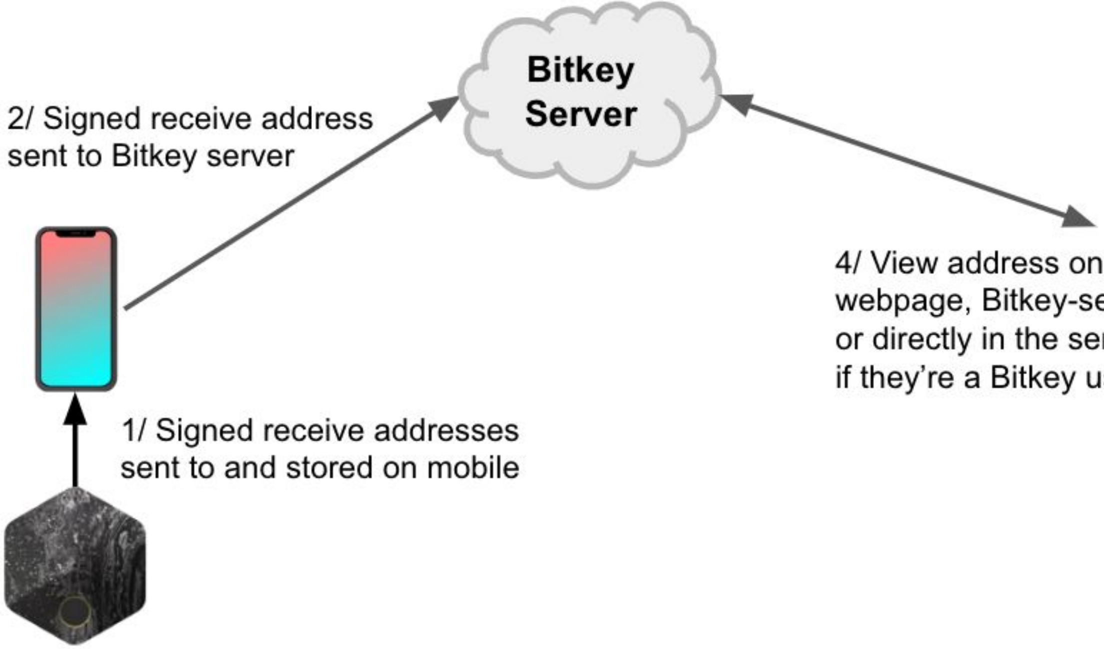
(3)
Owner confirms, server signs authorization

(4)
Server returns authorization

← (5)
Forward the authorization

← (6)
Owner taps hardware, which signs to complete transaction

Screens are not a panacea



1/ Signed receive addresses sent to and stored on mobile

2/ Signed receive address sent to Bitkey server

3/ Server verifies signed address came from hardware, before communicating it to the wallet owner or sender

4/ View address on a Bitkey-hosted webpage, Bitkey-sent email or text, or directly in the sender's Bitkey app if they're a Bitkey user

Thank you.