Bitcoin Custody

Bryan Bishop <kanzure@gmail.com>

0E4C A12B E16B E691 56F5 40C9 984F 10CC 7716 9FD2

2018-09-23

Baltic Honeybadger 2018

whoami

- Bryan Bishop
- Software development background
- Previously @ LedgerX (4 years!)
- Bitcoin Core contributor
- Biotech projects
- https://twitter.com/kanzure

What is custody? "The Custody Rule"

- 17 CFR 275.206(4)-2 https://www.law.cornell.edu/cfr/text/17/275.206%284%29-2
- Custody rule: It is forbidden to have custody, assets must be stored with a qualified custodian (bank, futures commission merchant (FCM), broker-dealer, or foreign financial institution)
- Custody is defined as:
  - possession of funds
  - authorization or permission to withdraw funds
  - legal ownership or access to funds

Bitcoin without third-parties vs. Custody Rule

- Hot and cold wallets
  - Cold wallets are "buy and hold", should that really require a bank..?
- Bitcoin was invented to operate without third-parties, so was bitcoin security
- Custodians can be considered a third-party security hole
- Custodians operate in a much more centralized regime
- Combining traditional "qualified custodians" with bitcoin technology will produce interesting new outcomes and possibilities
  - Monitoring, auditing, multisig, locktimes, MASTs, etc.

Regulation (1/2)

- Square pegs, round holes
- Unclear how to require use of bitcoin's technological ability
- Some regulations may need to be altered to take advantage of bitcoin's features
- … default behavior is to apply existing rules to bitcoin, missing out on technological developments.
- Give real examples to regulators, with actual use cases.

Lessons learned at LedgerX

- CFTC regulated bitcoin clearinghouse & options exchange
- Automation good, but sometimes not really required
- No end-to-end off-the-shelf cold storage solution with HSMs
- Be careful which backend solutions get promised to regulators

Levels of Storage and Custody

- Bitcoin Core wallet (hot wallet)
- Offline keys
- Offline wallets (cold storage)
- Hardware wallets
- Hardware security modules
- Nuclear bunker cold storage
- Paper wallets, bullion wallets- survive EMP attacks

Appropriate Custody

- What is the targeted level of security?
- What are the risks?
- Who are the potential adversaries?
- What's the threat model?
- Implementation cost vs level of security provided

You may think your wallet is simple enough for your heirs to figure out.

You're wrong.

Checklists and Documentation

- No matter the scale or scope of a bitcoin storage solution, documentation must be written
- Importance of checklists
- Make a checklist
- Make a checklist
- Check it twice.

Signing Ritual

- Signing ritual or signing ceremony
- Ceremony rooms, vaults, locks, lock boxes, etc.
- Video surveillance
- Checklists and documentation
- Training and orchestration
- The Summoning
- Rigorous logging, auditing, receipts

DNSSEC signing ceremony

- Largest publicly visible signing ceremony
- https://www.iana.org/dnssec/ceremonies
- https://www.iana.org/dnssec/dps/ksk-operator/ksk-dps.txt

Things to consider when designing a custody solution...

Risks

- Key entropy
- Cross-company interface risks
- Internal theft
- Hacking
- Wallet bug
- Blockchain bug
- ….

Threat models

- Simplified: What is the level of sophistication of an attacker that you wish to defend against?
- Examples:
  - Internal theft
  - Small-scale phishing operation
  - Local police
  - Nation state actor

Adversaries

- Bitrot
- Coercion
- Process fatigue
- Correlation
- Death and incapacitation
- Disaster
- Nation state actor
- ...

Questions for third-party custodians

- Get a copy of their standard operating procedures
- Who is on their staff? Key personnel?
- What level of technical expertise do they have available?
- What regulations do they comply with? Who are their regulators?
- Insurance policy?
- ...

Piecing together a signing ritual...

Hardware wallets

- Important component to signing rituals
- Nice-to-haves:
  - Screen verification of transaction details
  - Include amount in the transaction so the hardware wallet knows before signing
  - Backups
  - More backups
  - Consensus rules and bitcoin node on a hardware wallet

Hardware security modules

- Generally considered as:
  - More sophisticated hardware wallets
  - Distinguished from hardware wallets often by being bolted to the floor
  - Generally not consumer/retail-oriented
- But the above is a hold-over from pre-bitcoin days:
  - Hardware wallets and HSMs should really be the same thing
  - Maximum security for all customer demographics

Hot wallet hardware wallets

- Only sign transactions that increase balance
- Useful for lightning nodes (HTLCs required)
- Useful for coinjoin and joinmarket
- UTXO consolidation when fees are low
- "This allows custodial wallets to make productive use of their assets while not putting funds at risk, or for HODL'ers to help grow JoinMarket and Lightning networks without putting their nest egg at risk." - maaku

HSMs with quorums

- Single key stored on the HSM
- Multiple hardware devices required in quorum to access the HSM (authorization to access HSM)
  - Don't need to update blockchain to handle internal personnel changes or org chart changes
  - BTC fund reallocation within an organization by updating a table or data store in the HSM, without on-chain transactions
- Other possible HSM constructions

Bitcoin-specific techniques for custody....

Partially-signed bitcoin transactions (PSBT, bip174)

- https://github.com/bitcoin/bips/blob/master/bip-0174.mediawiki
- A binary transaction format which contains the information necessary for a signer to produce signatures for the transaction and holds the signatures for an input while the input does not have a complete set of signatures.

- Unsigned transactions, non-witness UTXO, witness UTXO, partial signatures, sighash type, redeemScript, witness script, bip32 child key derivation path, etc.

Pre-signed transactions

- Very useful when using airgaped, irregularly accessed hardware wallets
- After signing all transactions that you intend to broadcast, also sign other transactions that sweep to emergency destinations, but do not broadcast these alternative transactions
- Timelocks (next slide)

Pay to timelocked pre-signed transaction

- nLockTime OP_ELSE emergency super-secure master key
- Pay to timelocked signed transaction (by deleting intermediate keys after broadcasting an intermediate step, spending to a timelocked script)
  - Coins impossible to steal until the second transaction is broadcasted
  - Monitor blockchain for unexpected transactions appearing on the chain, use emergency key to move funds
  - Use MASTs or graftroot to hide complex policies in the OP_ELSE etc. etc.

Things that have gone unsaid

- Covenants
- Auditing, public keys, bip32
- MASTs, taproot, graftroot
- Schnorr multisig

Regulation (2/2)

- Everyone deserves access to a hardware wallet.
- Buy-and-hold should not require a qualified custodian
- Companies need to evaluate the regulatory risk of non-compliance- might be acceptable?
- What would we propose to the SEC for a hands-off, sandbox approach?
- Software approach to bypass regulatory requirements (next slide)

Avoiding the qualified custodian requirement using software magic

- Goal: Other than choosing to ignore the custody rule (taking on compliance risk), find a way to run a bitcoin fund where the fund manager does not have custody.
- Solution: software nodes operated by investors that participate in the fund. Fund manager proposes transactions. Nodes sign off on trades, connect to exchanges.
- Other example: New Wave (compliance risk?)

Smart Custody workshop #1
November 15th, 2018 in San Francisco
https://www.smartcustody.com/

- Smart Custody is the use of advanced cryptographic tools to improve the care, maintenance, control, and protection of digital assets.
- 1-day workshop for custodians and family offices covering topics such as:
  - custody
  - hardware wallets
  - best practices
- Optional next day "office hours"
- Organized by Christopher Allen, Angus Champion de Crespigny, Bryan Bishop
- Contact: **angus@anguschampion.com**

One more thought: Off-the-shelf custody product wish list

- Uses multiple hardware wallets
- Uses at least one offline computer
- Runs bitcoin consensus code, blockchain sync
- Handles deposits/withdrawals
- Rigorous logging
- Remote auditability
- Has training & documentation materials, videos

That's all, folks.