CHECKSIG

Custody Protocol

Introduction

Bitcoin is a “bearer instrument” and, as such, it can only be spent by using private (secret) keys; if they are lost or stolen, there is no way to recover the associated Bitcoins. Safe management of the private keys is therefore of paramount importance for Bitcoin holders, but such activity requires sophisticated technical skills and domain knowledge.

Private keys are usually stored in “wallets”; however, “hot” (online, internet connected) wallets can be hacked, “cold” (offline, internet disconnected) wallets can be lost or stolen, and the PINs/passwords needed to gain access to wallets can simply be forgotten.

Consequently, individuals may be uncomfortable dealing with their Bitcoin holdings; even more if they consider issues such as inheritance (how to ensure that children will inherit Bitcoin without having to share private keys with them) and personal safety (how to avoid violence and coercion aimed at stealing Bitcoin). Institutions too, they have the above security issues; moreover, they are often required by law and/or internal regulation to entrust the management of Bitcoin holdings to a specialized service provider. That’s why there are companies offering professional Bitcoin custody services.

Unfortunately, many Bitcoin custodians offer unsatisfactory solutions

- Insufficient disclosure about their technology and process, often with the excuse that this is needed for "security" reasons (the so-called security-by-obscurity paradigm, rejected by all reputable cryptography and cyber-security experts).
- Customers have no way to check that their Bitcoins are, in fact, really held by the custodian and have not "disappeared" for one reason or another.
- Customers remain in charge of technical duties or risk management responsibilities.
- Conflicts of interest arise for custodians that also provide trading services, as trading favours availability instead of security.

This is why CheckSig has decided to undertake a totally different approach designing its transparent open protocol for Bitcoin custody. The protocol includes patent-pending inventions, pledged to the Crypto Open Patent Alliance.

A new standard of transparency and security, by design

- Avoid reliance on security-by-obscurity and, instead, defines a public standard that can be audited and reviewed by anybody
- Provide periodic evidence of Bitcoin holdings to clients, so that they can be certain that their assets are where they are supposed to be

Our guiding principles:

- no hot wallets, i.e., assets are never internet-exposed, neither remotely accessible, to make remote attacks unfeasible
- minimize the risk of loss of funds through theft, error, or other mishaps
- rely on the Bitcoin protocol for security wherever possible, rather than inventing new functionality or procedures

- remain as "neutral" as possible regarding future changes to the Bitcoin protocol, working with the existing Bitcoin protocol functionality "as is".

How it works

There are four main events happening in our custody process: deposit, withdrawal, proof-of-reserves, and disaster recovery. Before describing them in detail, it is important to know that three main parties are involved:

- Clients: the actual owners of the Bitcoins, who have decided to place their assets in CheckSig custody.

- CheckSig: the entity which has the legal custody of the assets on behalf of the Clients. Inside CheckSig there are different kind of agents; as of November 2021:

  - three authorization agents

  - three custodian agents

  - three Frozen Wallet recovery agents

  - three Cold Wallet recovery agents

- Federation: external legal entities, independent from CheckSig; as of January 2023, there are five Federation agents:

  - Intesi Group: a Certification Authority with deep Bitcoin knowledge

  - SZA an Italian law firm that assists crypto companies

  - Tinkl.it: a Bitcoin payment company

  - Studio Avella: a chartered accountant with in-depth understanding of crypto assets

  - Two, so far, undisclosed dormant (i.e., inactive) agents

Furthermore, CheckSig custody process uses two layers/wallets:

- the Frozen Wallet, where Bitcoins are stored, managed by the Federation

- the Cold Wallet, which is mostly empty (except during withdrawals), directly managed by CheckSig

Both wallets are comprised of professional-grade hardware security module (HSM) devices, provided by leading manufacturers: currently, Ledger (the most reputable specialized vendor) and CryptoAdvance/Specter (the most technically advanced one).

HSM devices are used to provide the digital signatures required for a Bitcoin transaction. A HSM device contains a secure element that perform the signatures using the secret keys without exposing them outside its own boundaries, so preventing the stealing of the keys even if the device is used in an unsecure or compromised environment.

1. Deposit process

In essence, deposit is very straightforward: the Client moves Bitcoins to an "address" belonging to the Frozen Wallet and notified to the Client by CheckSig.

2. Withdrawal process

The withdrawal process cannot be performed by CheckSig without involving the Federation, to reduce the risk of internal CheckSig wrongdoings. At the same time, the Federation cannot initiate a withdrawal process, only CheckSig can.

The withdrawal consists of two distinct Bitcoin transactions:

1. Bitcoins are moved from the Frozen Wallet to the Cold Wallet. This first "unlock and/or redeposit" transaction requires two steps:

- CheckSig authorization agents must pre-authorize the transaction. This is accomplished when the digital signatures of two out of three (2-of-3) authorization agents are obtained. Each authorization agent provides its digital signature using a HSM device.

- Then, the transaction must obtain the approval of three out of six (3-of-6) Federation agents. Each Federation agent provides its digital signature using a HSM device, customized (i.e., locked-down) to ensure that the signature can be produced only if:

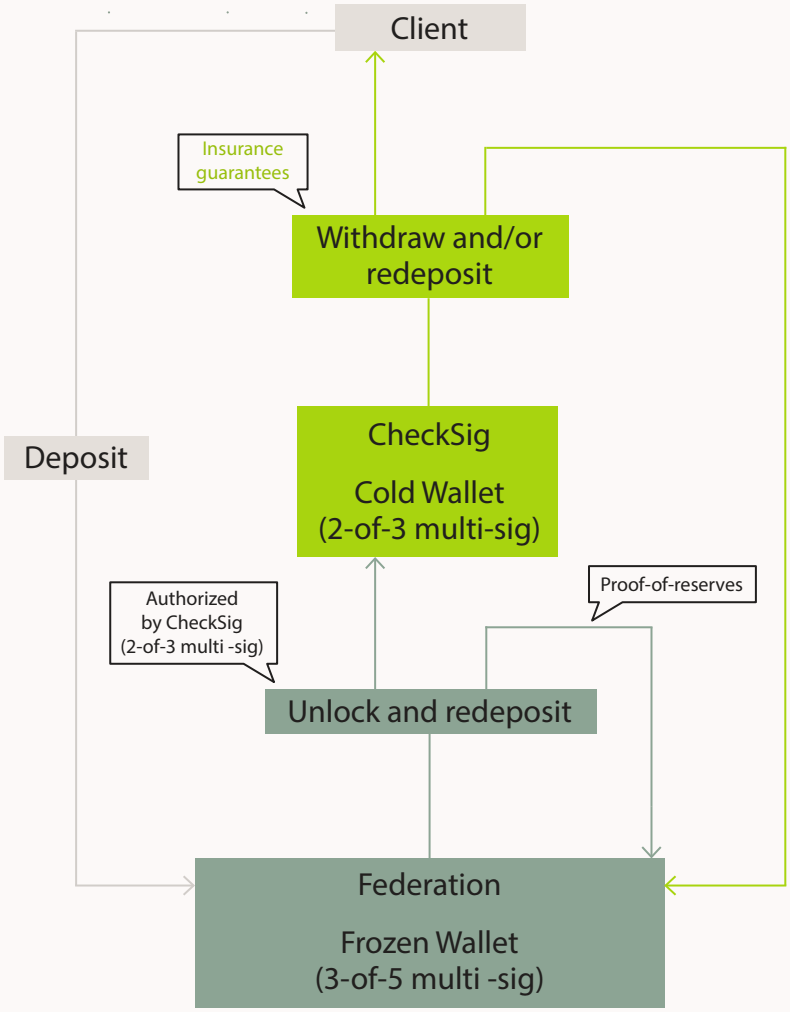
- The transaction has been pre-authorized by CheckSig authorization agents

- The transaction unlocks Bitcoins to destination addresses included in a previously approved list of addresses belonging to the Cold Wallet (and/or redeposits Bitcoins to destination addresses included in a previously approved list of addresses belonging to the Frozen Wallet itself, see "4. Proof-of-reserves" later on).

At this stage, Bitcoin can only be moved to a previously approved list of addresses: it is technically impossible to move them to any other arbitrary address and this prevents any chance of Federation agents stealing Bitcoins away from the CheckSig custody.

2. Bitcoins are moved from the Cold Wallet to the Client(s). This second "withdraw and/or redeposit" transaction requires the digital signatures of two out of three (2-of-3) CheckSig custodian agents, each signature involving a distinct HSM device held in a different safety box in a different bank in a different city. It is with this second transaction that Bitcoins are effectively withdrawn from CheckSig and returned to the Client. Furthermore, the withdraw transaction can only be performed with a four days (more precisely 4*144=576 blocks) "fixed time delay" after the previous unlock transaction has been confirmed by the Bitcoin network; this is to allow for security checks (see "4. Disaster Recovery" later on): in the case of any problem, Bitcoins can be redeposited back to the Frozen Wallet.

The act of spending from the Frozen or Cold Wallet reveals the (pre-image of the P2WSH) locking script that protects the Bitcoins under custody. Since these transactions happens at least monthly, the scripts protecting the Bitcoins under custody are public on the blockchain, making CheckSig custody really transparent: everything documented here can be independently verified, avoiding any kind of security-by-obscurity (see also "4. Disaster Recovery" later on).



Differently from all other custodians that have access to all the assets all the time, CheckSig has direct access to Bitcoins only during the withdrawal process and only for the amounts being withdrawn. This being the only residual attack surface of the custody process, the withdrawal is covered by insurance guarantees.

3. Proof-of-reserves

On a periodic (at least monthly) basis, an "unlock and/or redeposit" transaction is confirmed by the Bitcoin network, publicly documented on the blockchain and published on the CheckSig website. The Bitcoins that are not unlocked to satisfy withdrawal requests are redeposited from the Frozen Wallet back to the Frozen Wallet itself. This is the "proof-of-reserves" provided periodically to clients and auditors as evidence of the amount under custody and, crucially, to prove that CheckSig has not lost control of the Bitcoins held in the Frozen Wallet.

4. Disaster recovery

A disaster recovery procedure is activated when:

1. The authorization quorum is lost, i.e., using the current 2-of-3 set-up, less than two out of the three HSM devices held by CheckSig authorization agents are functional/available. In this case, the risk is to lose control of the assets in the Frozen Wallet, usually representing all funds under custody.

2. The federation quorum is lost, i.e., using the current 3-of-6 set-up, less than three out of the five HSM devices held by Federation agents are functional/available. In this case, the risk is to lose control of the assets in the Frozen Wallet, usually representing all funds under custody.

3. The custodian quorum is lost, i.e., using the current 2-of-3 set-up, less than two out of the three HSM devices held by CheckSig custodian agents are functional/available. In this case, the risk is to lose control of the assets in the Cold Wallet, usually just pocket money allocated to the Cold Wallet to cover for transaction fees, possibly larger amounts during a withdrawal process.

4. a malicious withdraw process has been initiated by CheckSig authorization agents and approved by Federation agents; if the custodian agents are suspected of colluding in an attempt to steal funds, the withdraw process must be reverted before the expiration of the "fixed time delay" that would make the Bitcoins (just moved from the Frozen Wallet to the Cold Wallet) available to the custodian agents. In this case, the risk is not being able to stop the malicious withdraw process, losing the involved funds.

More specifically, there are two different kind of disaster recovery transactions.

1. Cases 1 and 2 above: the disaster recovery transaction requires the digital signatures of two out of three (2-of-3) CheckSig Frozen Wallet recovery agents, provided using Frozen Wallet recovery HSM devices, each held in a different safety box in a different bank in a different city. These HSM devices are accessible to the CheckSig agents only with the informed explicit approval of a notary, after an independent audit of the disaster scenario. The disaster scenario is evident when the Bitcoins in the Frozen Wallet have not been moved on the Bitcoin network for more than 36 days (more precisely 36*144=5184 blocks), i.e., a proof-of-reserves has not been timely provided. In this case, the Frozen Wallet recovery HSM devices can be used to sweep those Bitcoins anywhere (e.g., to a new custody set-up). The disaster recovery facility, along with the regular Federation control facility, is evident when

an “unlock and/or redeposit” (i.e., proof-of-reserves) transaction spends from a Frozen Wallet address revealing the (pre-image of the P2WSH) locking script:

```
OP_IF
    OP_PUSHNUM_3 <F1> <F2> <F3> <F4> <F5> <F6> OP_PUSHNUM_6 OP_
CHECKMULTISIG
OP_ELSE
   5184 OP_CSV OP_DROP OP_PUSHNUM_2 <F-R1> <F-R2> <F-R3> OP_
PUSHNUM_3 OP_CHECKMULTISIG
OP_ENDIF
```

2. Cases 3 and 4 above: the disaster recovery transaction requires the digital signatures of two out of three (2-of-3) CheckSig Cold Wallet recovery agents, provided using Cold Wallet recovery HSM devices. These devices are customized (i.e., locked-down) to ensure that the signature can be produced only if the transaction spends Bitcoins to destination addresses included in a previously approved list of Frozen Wallet addresses. At any time, the Cold Wallet recovery HSM devices can sweep the Bitcoin in the Cold Wallet, redepositing them back to the Frozen Wallet. The Cold Wallet four days “fixed time delay” does not apply here, as it only concerns custodian HSM devices. The disaster recovery facility, along with the regular custodian control facility, is evident when a “withdraw and/or redeposit” transaction spend from a Cold Wallet address revealing the (pre-image of the P2WSH) locking script:

```
OP_IF
    576 OP_CSV OP_DROP OP_PUSHNUM_2 <C1> <C2> <C3> OP_PUSHNUM_3
OP_CHECKMULTISIG
OP_ELSE
  OP_PUSHNUM_2 <C-R1> <C-R2> <C-R3> OP_PUSHNUM_3 OP_CHECKMULTISIG
OP_ENDIF
```

CHECKSIG S.R.L.
Via G.B. Pirelli 11, 20124 Milano (MI) - ITALY
email: info@checksig.com