Summary

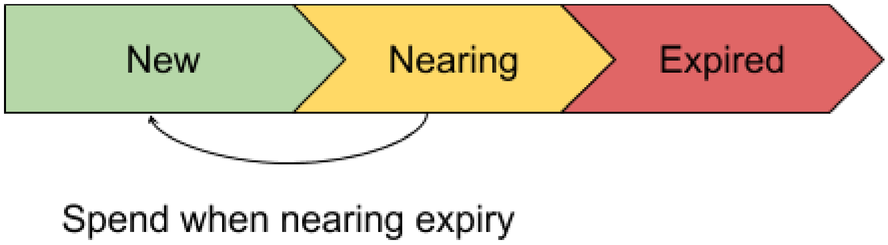
On June 25th, a Twitter user reported that a portion of the Liquid Network funds were temporarily (approximately 40 minutes) accessible by a set of emergency keys. This behavior is the result of a known inconsistency between the timeout period for the emergency keys becoming active and the transaction sweep frequency on the functionaries. Blockstream is moving to release a quick fix ahead of the original fix (DynaFed) to address this issue, and it can be deployed across the network in the next week. All funds remain safe in the Liquid Network.

Emergency Keys Explained

The Liquid Network's functionaries maintain a wallet that controls the underlying BTC that makes up the BTC to L-BTC peg. This wallet requires 11 out of the 15 functionaries to sign transactions that spend the underlying BTC. In the event that 5 functionaries are destroyed, seized, or otherwise inoperable and unable to be restored from backups, the underlying Bitcoin would not be able to be spent. To provide insurance against this scenario, a set of emergency keys exist that can be used to spend any BTC in the Liquid network that remain unspent for an extended period of time. Two of these keys are required to spend these coins. These keys are distributed across the world in secure locations, held by Blockstream in such a manner that it takes multiple employees to access sufficient numbers of keys to use.

Watchman Overview

The default script for Liquid is 11-of-15 multisig (to spend immediately) or 2-of-3 (after a timeout). The Liquid Federation automatically spends each UTXO periodically to ensure that this timeout is not reached. Any UTXO that reaches sufficient maturity could be spent by 2-of-3 of the emergency keys.



Every 25-40 minutes, the functionaries undergo a "watchman round". These rounds consist of one functionary being designated the "leader". Each functionary takes a turn being leader in a specified order, until all have completed this process and the first functionary is again the leader.

The leader of a watchman round proposes a set of Bitcoin transactions that should be broadcasted. This set is chosen from two sources:

1) Any mature peg-out in the Liquid blockchain should be processed by spending a set of UTXOs to the designated peg-out address.
2) Any UTXOs past the sweep threshold should be spent back to the Liquid Federation “change address”. This effectively resets the expiration period. An exception is UTXOs that are dust. These dust UTXOs are not re-spent, and typically represent <$10 ($0.76 as of the time of this writing) of value at any point in time and would cost more to spend than their value. These UTXOs will eventually be spent when fee rates lower to make them economical to spend.

Once the leader proposes this set of transactions, the other functionaries will ACK or NACK this request, and sign the transactions they believe are valid. If a threshold of 11 functionaries ACK each transaction, each functionary will request a signature from its HSM for the transactions. The HSMs validate that the transactions are either spent as change to the federation, or to a member of the peg-out whitelist. Signatures are then collected and the transaction is broadcast to the Bitcoin network.

In a correctly functioning network with at least 11 functionaries online, this process allows Liquid to correctly process peg-out transactions as well as to ensure that the emergency keys cannot be used to spend any of the UTXOs. The network targets 100 UTXOs as the desired number of UTXOs to maintain at all times, which can involve consolidating or splitting existing UTXOs during this process. Having 100 UTXOs ensures that a large number of peg-out transactions can be processed upon demand.

Current Network Configuration

Liquid has three different parameters related to the sweeping of UTXOs:

1) The peg-in script template defines the conditions needed for functionaries to spend peg-in transactions. This script template is used by each user attempting to peg-in Bitcoin such that it is a unique address per peg-in. This allows each peg-in transaction to commit to a script that can be used in the Liquid transaction claiming the peg-in.
2) The HSM’s expected change script for UTXOs that are spent back to the federation. The HSM will only sign transactions to whitelisted addresses as part of a peg-out or to this change address.
3) The target maturity that a functionary should target when sweeping a UTXO.

For Liquid, these values are currently as follows:

1) (11-of-15 Functionary Keys) OR (4032 blocks maturity AND 2-of-3 Emergency Keys)
2) (11-of-15 Functionary Keys) OR (2016 blocks maturity AND 2-of-3 Emergency Keys)
3) 2016 blocks

The mismatch between parameters 1 and 2 was the result of an early bug in Liquid. The timeout period was modified in one piece of software, but was left unmodified in a separate piece. This bug prevented the functionaries from receiving a signature from the HSM due to their mismatched expectations of the change address. Due to the security design of Liquid, the HSM software is designed to be considerably harder to update than the functionary software. While the ideal solution would have been to modify the HSM software to use the intended 4032 block maturity, this solution was infeasible, given it would take a physical update of each HSM in the network. An easier solution was to simply have the functionary software, which can be more easily updated, to use the HSM's change script for processing change, reducing the timeout period to 2016 blocks. Once this fix was deployed to 11 functionaries, Liquid was able to process peg-outs and sweep UTXOs. During this time period, many UTXOs were accessible by the emergency keys, however the network value of Liquid at this time was very insignificant so little actual risk was present.

However, due to this fix, the sweep behavior did not account for this adjustment and instead used the network defined timeout period of 4032 blocks with the intention to sweep funds at ½ of that timeout period. This issue was detected by Blockstream soon after deployment. However, in normal circumstances, only a small portion of the funds of Liquid are ever vulnerable, and only for a very limited time period (the time for a watchman round to complete and a block to mine the transaction). Given that there are 100 UTXOs at any point in time, the amount of funds at risk was typically small, and would have required malicious behavior from Blockstream, combined with proof of this malicious behavior.

However, several large peg-ins to the network in recent weeks have led to an uneven distribution of UTXOs. One particular UTXO contained a value of 870 BTC, representing approximately 40% of the network value, reached its maturity, before being swept and included in a block 40 minutes later. This sweeping was part of the automated process for Liquid functionaries.

Proposed Fix

While the preferred fix for this undesirable behavior was part of an existing upgrade plan of the network, Blockstream is making a fix that will reduce the risk of this happening by reducing the sweep period to 1008 blocks. This fix is being actively developed and will be deployed to a set of functionaries. As soon as a single functionary upgrades to this version, all UTXOs will be swept at this higher frequency, avoiding any possibility of the emergency keys being able to be used. It is recommended that all functionaries complete this upgrade so that the sweep process can continue regardless of which functionaries are offline or online.

As a previously planned longer term fix, the Dynamic Federations upgrade includes an update to the HSM to allow the change script to be a network parameter that can be changed while running. This can allow the federation to change the timeout period, the emergency keys used, or even whether emergency keys should be used. As confidence in the Liquid Network grows, this recovery period can be extended to a much greater time period.