



Relative
Locktime
BIP68:
[https://github.c](https://github.com/bitcoin/bitcoin/blob/master/doc/relative-locktime.md)

Vault Setup: V1, R1, V2, R2, E are created
Partially signed transactions are created
V1, V2 are deleted

Vault funding: A transaction sending to the mutlisig adress of V1,R1

Normal Vault Release: R1 is used to sign the first transaction
R2 is used to sign the second transaction
After 1000 blocks the funds are spendable in F

Theft assumptions: A thief has access to R1, R2 and F, but not E

Theft attempt: A thief follows the normal vault release.

Stopping the thief: Monitoring of the blockchain records that the funds have moved to F without the vault owners actions.
Before 1000 blocks have passed the vault owner can use E and R2 to spend to any address immediately.