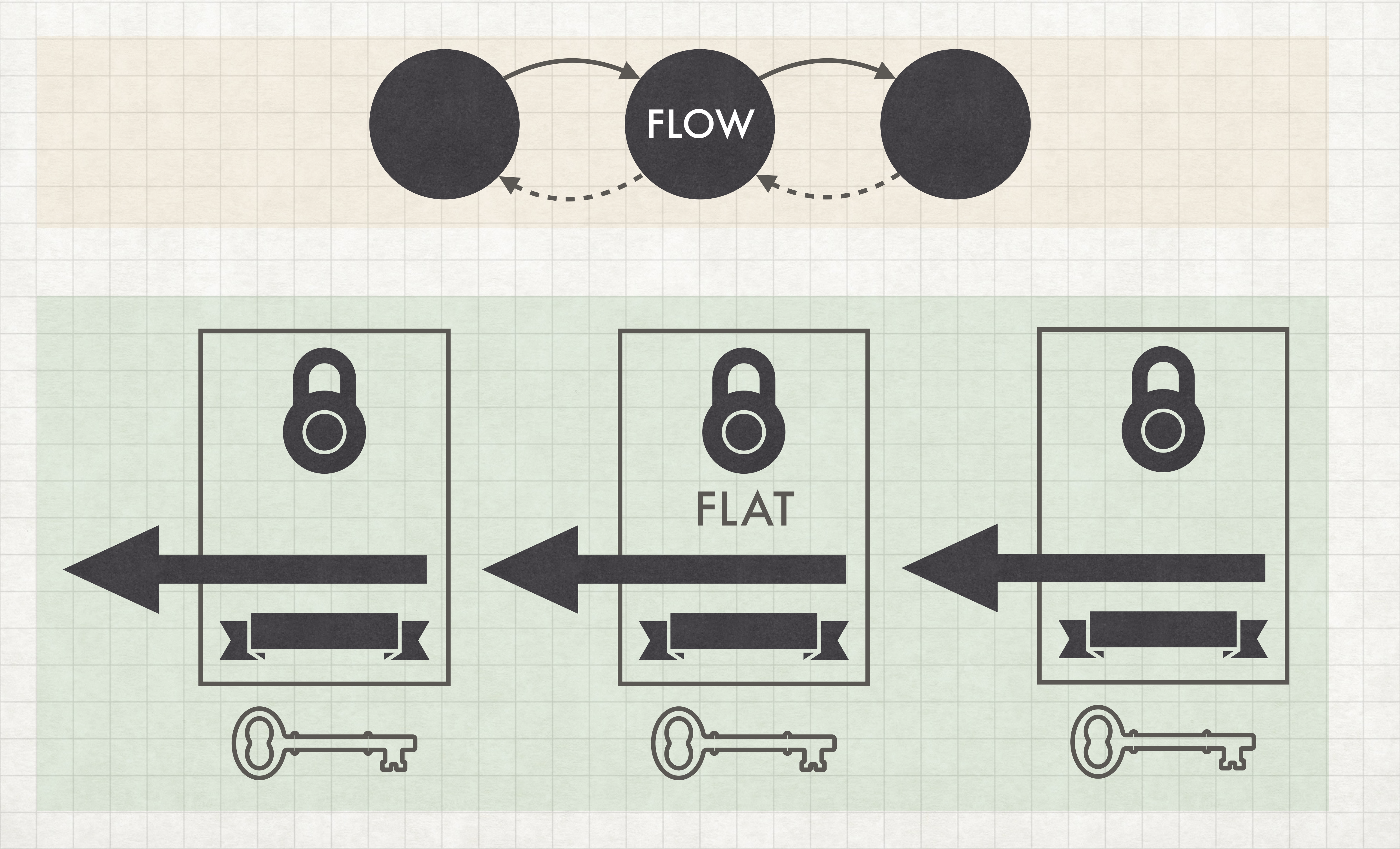
LIGHTNING NETWORK

SUBMARINE SWAPS AND LOOP

BITCOIN

ONE CURRENCY MULTIPLE SETTLEMENT NETWORKS



SUBMARINE SWAP

WITNESS PROGRAM

```
OP_HASH160 PREIMAGE OP_EQUAL
OP_IF
    ALICE PUBKEY
OP_ELSE
    CLTV_HEIGHT OP_CLTV OP_DROP
    BOB PUBKEY
OP_ENDIF
OP_CHECKSIG
```

+19 VBYTES OF KEYS, CODES

SUBMARINE SWAP

EXECUTION FLOW

SUCCESS

OP_HASH160 PREIMAGE OP_EQUAL

ALICE PUBKEY OP_CHECKSIG

TIMEOUT

CLTV_HEIGHT OP_CLTV OP_DROP

BOB PUBKEY OP_CHECKSIG

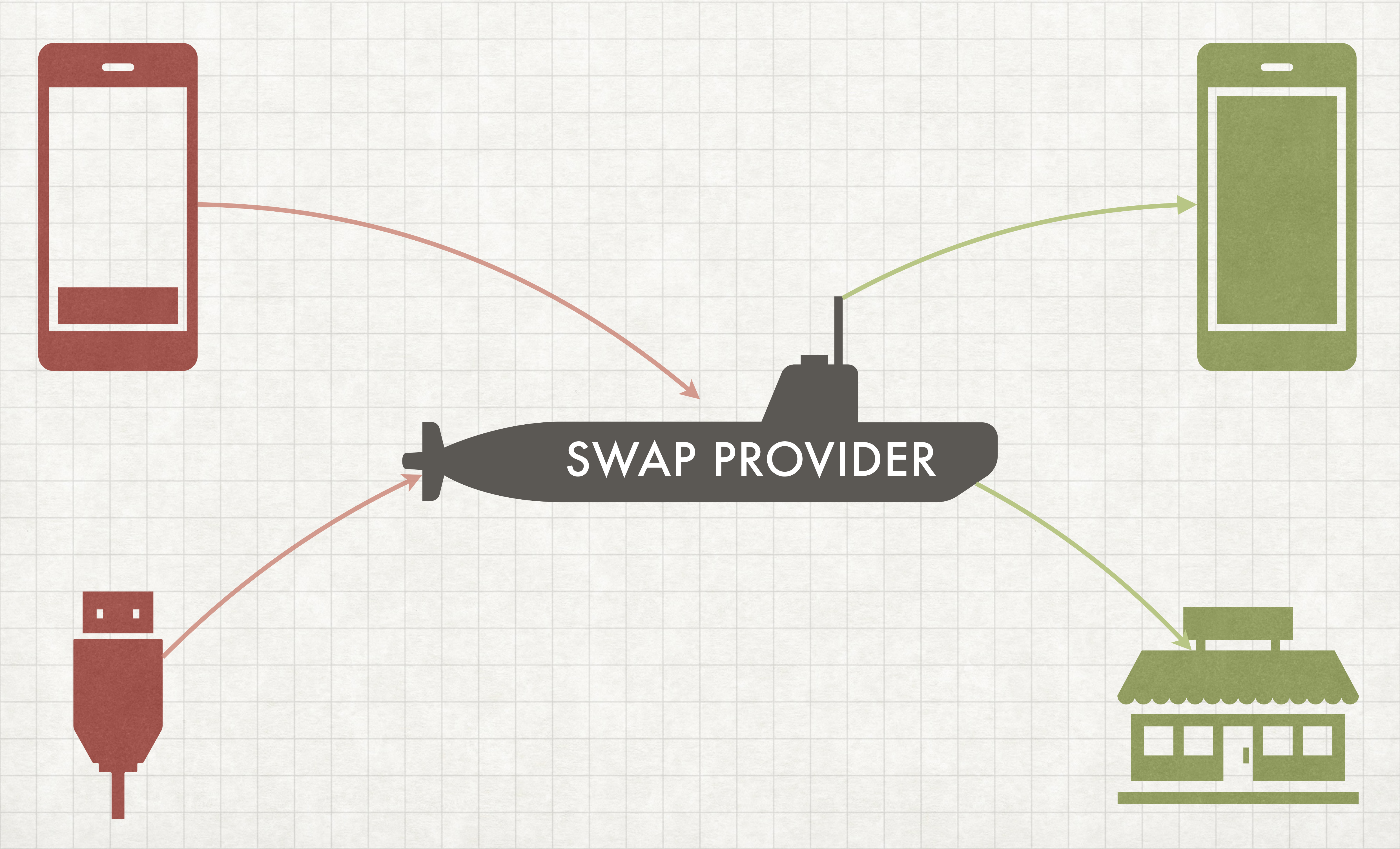
SUBMARINE SWAP

VARIATIONS IN THE WILD

OP_CSV	CSV becomes CLTV at confirmation
OP_SIZE	When are we not sure about the PREIMAGE size?
OP_HASH160	Making providing a refund key easier
OP_CHECKMULTISIG	Match the spending script

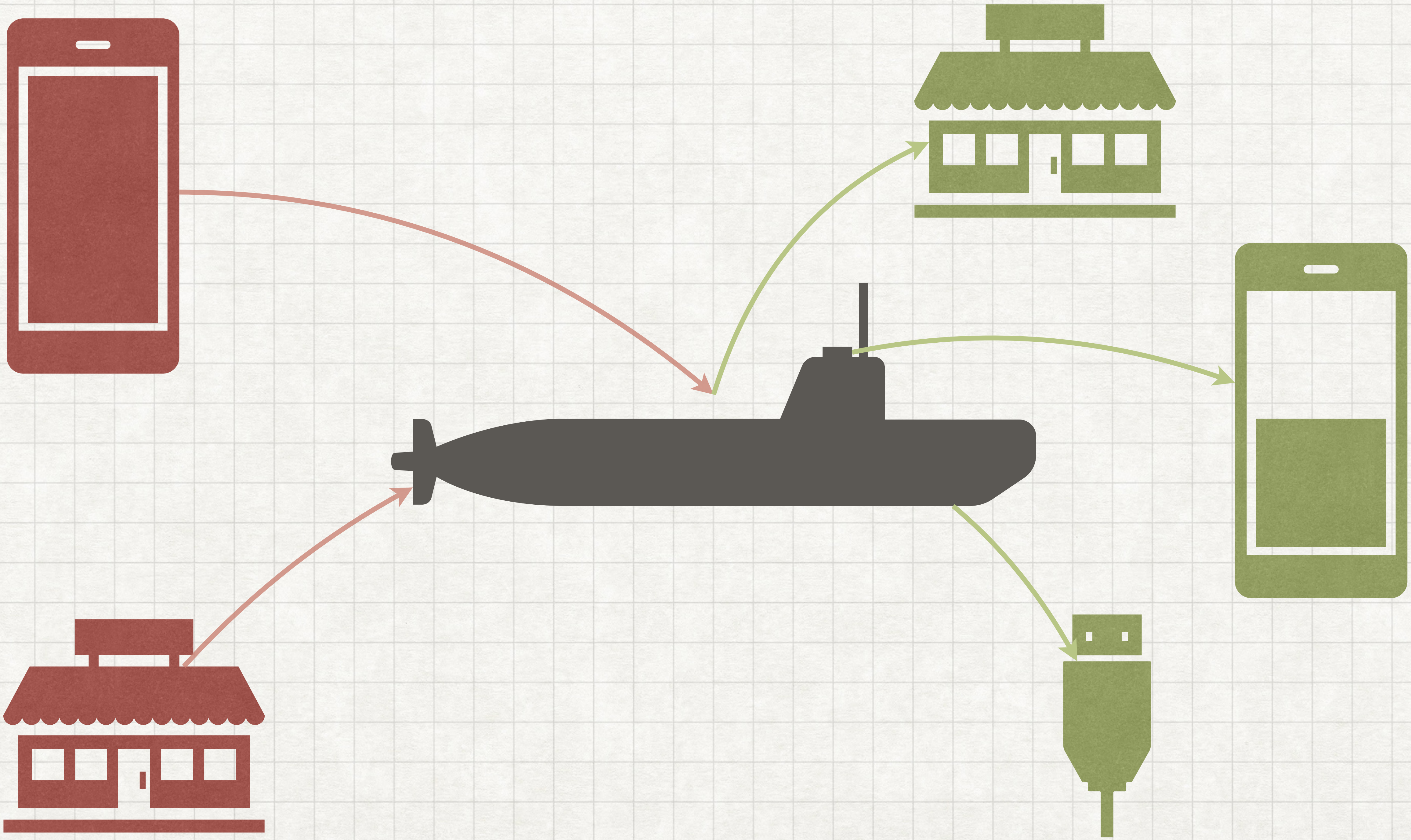
SUBMARINE SWAP

SWAP-IN USE CASES



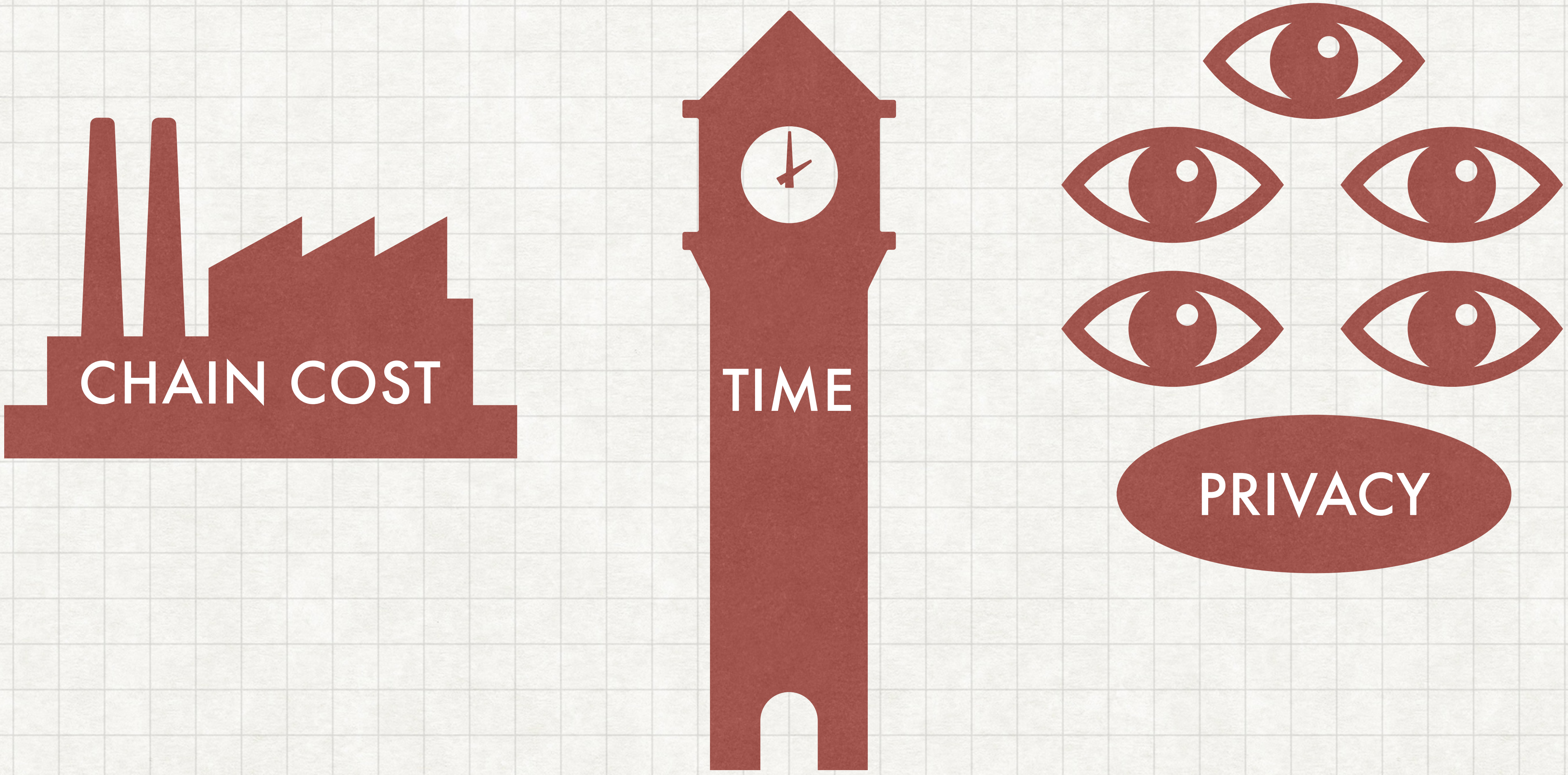
SUBMARINE SWAP

SWAP-OUT USE CASES



SUBMARINE SWAP

LIMITATIONS



CHAIN COST

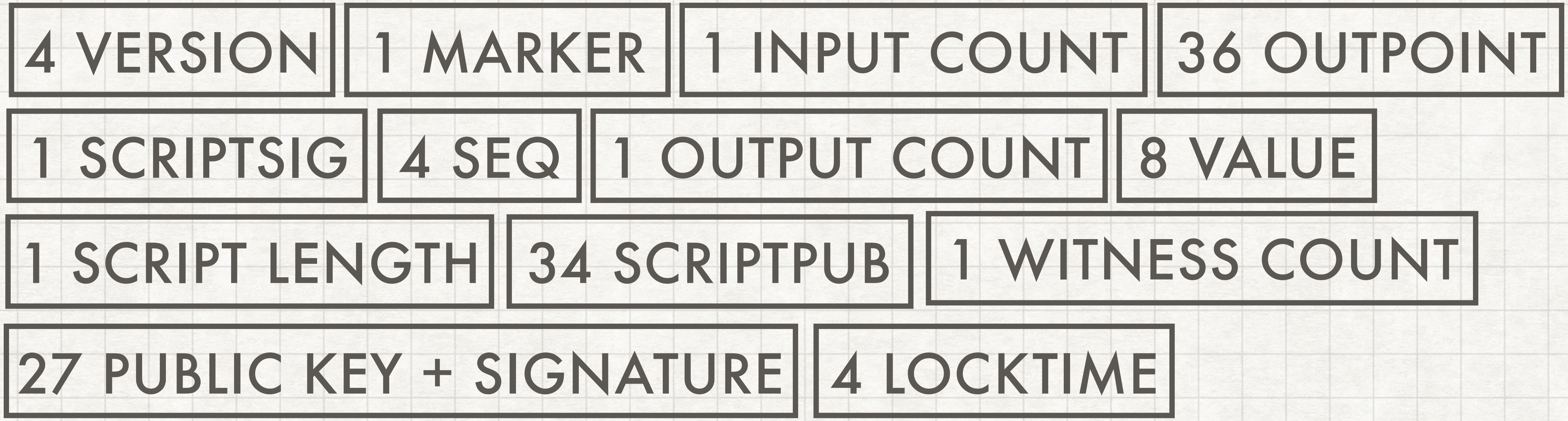
TIME

PRIVACY

SUBMARINE SWAP

CHAIN VBYTES: 260-290/SWAP

Funding Transaction: 123 vbytes (30+ if change output)



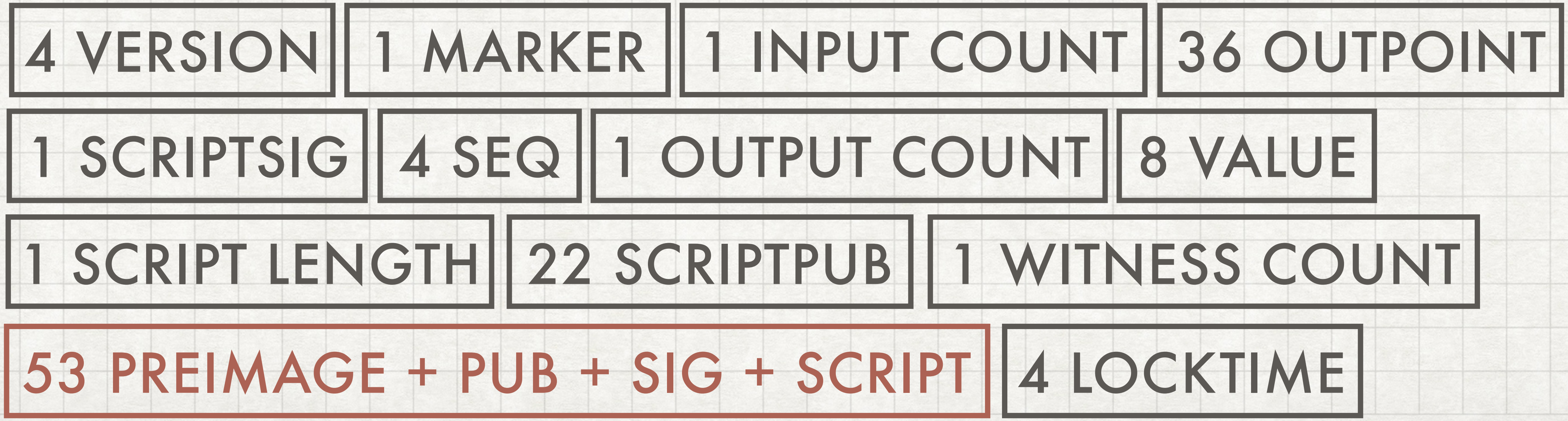
4 VERSION | 1 MARKER | 1 INPUT COUNT | 36 OUTPOINT

1 SCRIPTSIG | 4 SEQ | 1 OUTPUT COUNT | 8 VALUE

1 SCRIPT LENGTH | 34 SCRIPTPUB | 1 WITNESS COUNT

27 PUBLIC KEY + SIGNATURE | 4 LOCKTIME

Sweep Transaction: 137 vbytes



4 VERSION | 1 MARKER | 1 INPUT COUNT | 36 OUTPOINT

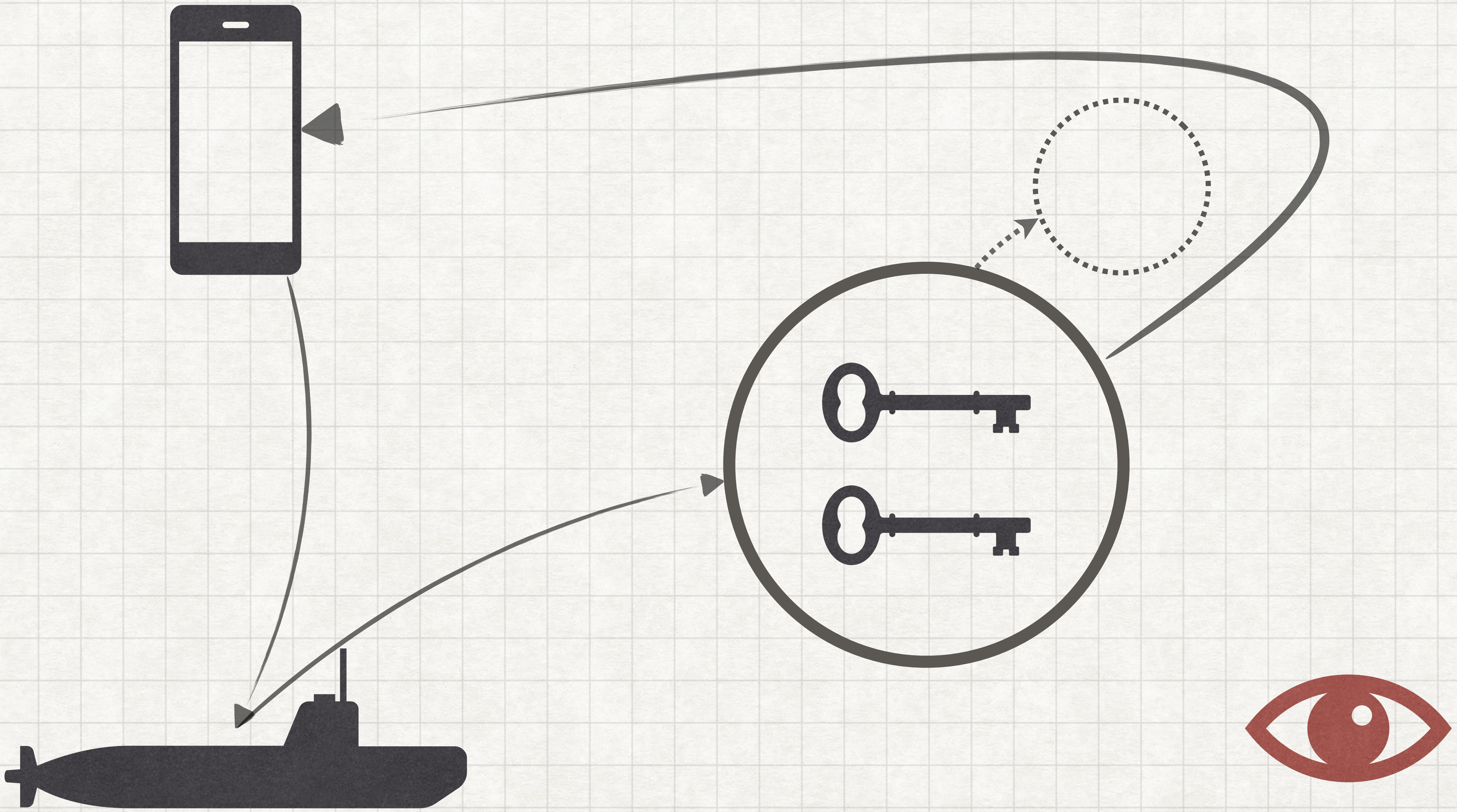
1 SCRIPTSIG | 4 SEQ | 1 OUTPUT COUNT | 8 VALUE

1 SCRIPT LENGTH | 22 SCRIPTPUB | 1 WITNESS COUNT

53 PREIMAGE + PUB + SIG + SCRIPT | 4 LOCKTIME

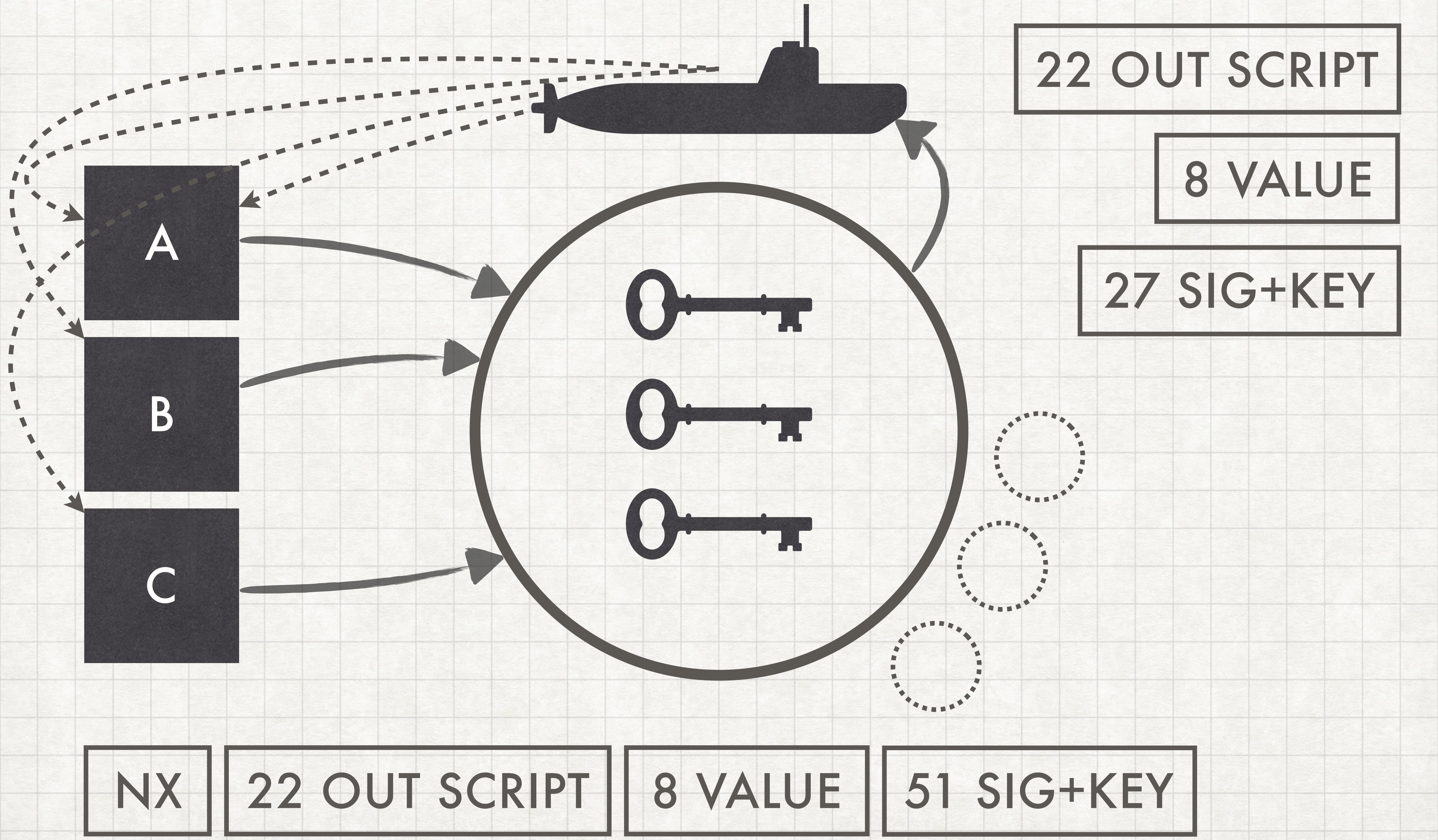
HYPERLOOP

IMPROVE PRIVACY



HYPERLOOP

REDUCE LOOP IN CHAIN FOOTPRINT



22 OUT SCRIPT

8 VALUE

27 SIG+KEY

NX

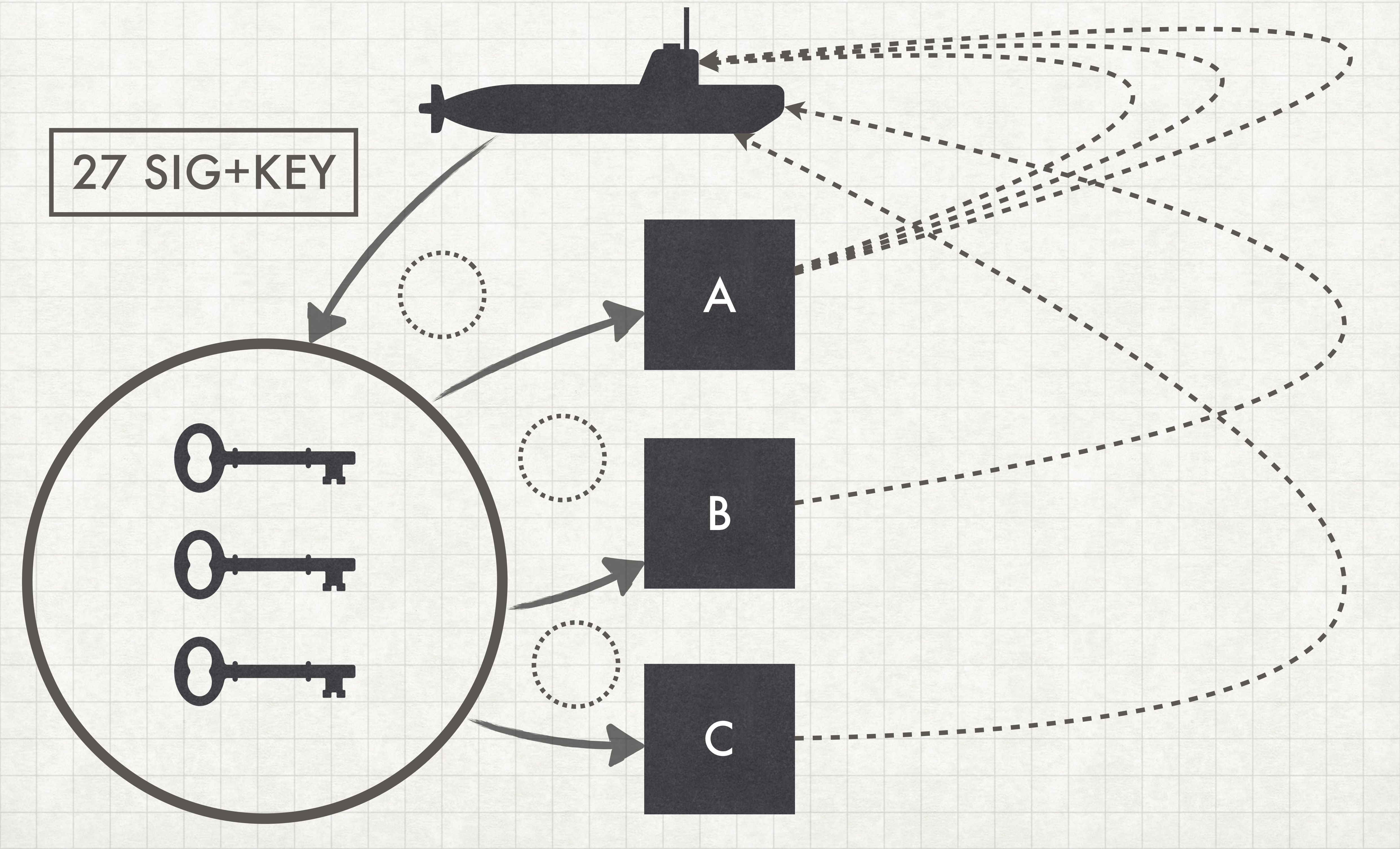
22 OUT SCRIPT

8 VALUE

51 SIG+KEY

HYPERLOOP

REDUCE LOOP OUT CHAIN FOOTPRINT



HYPERLOOP

CHAIN VBYTES: 204 + 30/SWAP

Funding Transaction: 123 vbytes

4 VERSION | 1 MARKER | 1 INPUT COUNT | 36 OUTPOINT

1 SCRIPTSIG | 4 SEQ | 1 OUTPUT COUNT | 8 VALUE

1 SCRIPT LENGTH | 34 SCRIPTPUB | 1 WITNESS COUNT

27 PUBLIC KEY + SIGNATURE | 4 LOCKTIME

Cooperative Transaction: 81 vbytes + 30/swap

4 VERSION | 1 MARKER | 1 INPUT COUNT | 36 OUTPOINT

1 SCRIPTSIG | 4 SEQ | 1 OUTPUT COUNT | 8 VALUE

1 SCRIPT LENGTH | 22 SCRIPTPUB | 1 WITNESS COUNT

27 PUBLIC KEY + SIGNATURE | 4 LOCKTIME