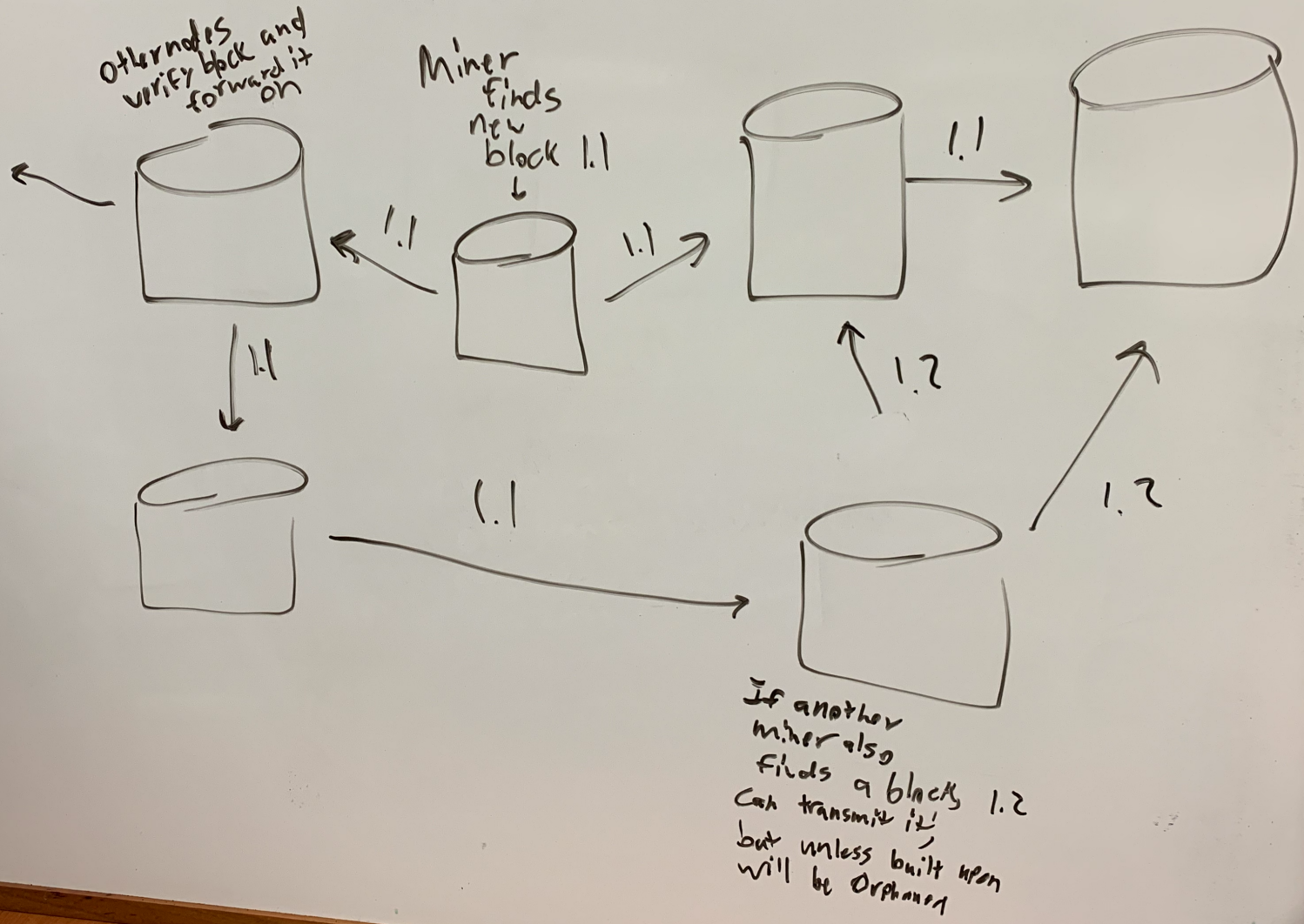
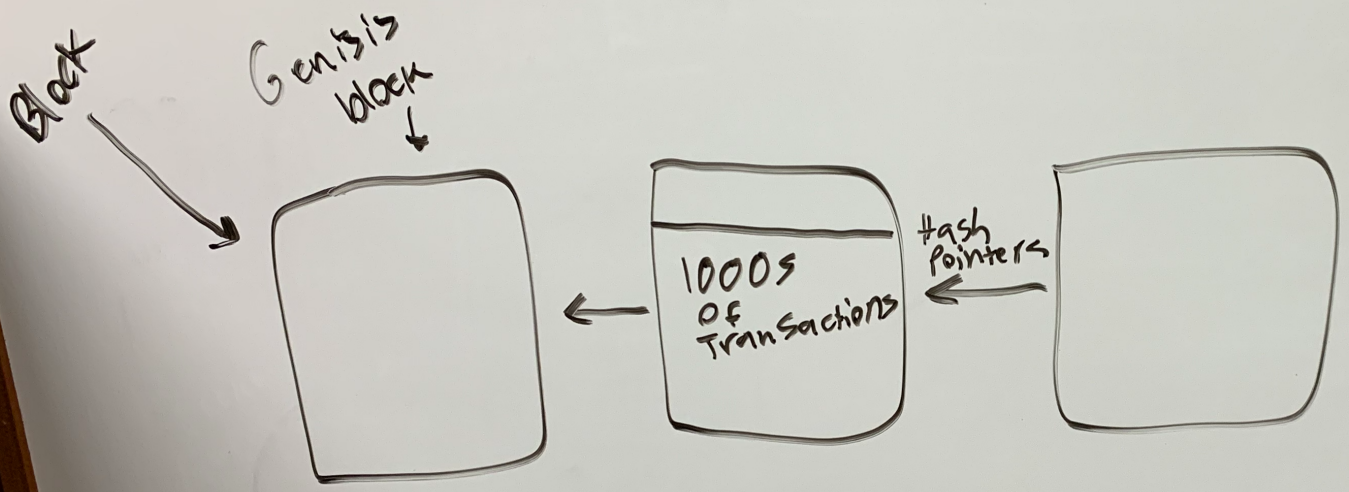
Full clients store the whole block chain,
SPV clients only store block headers to
request transactions when needed

Size goes from 20GB → 23MB
with 1000x cost
savings

How a miner broadcasts

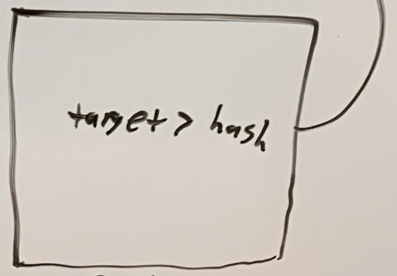


Structure

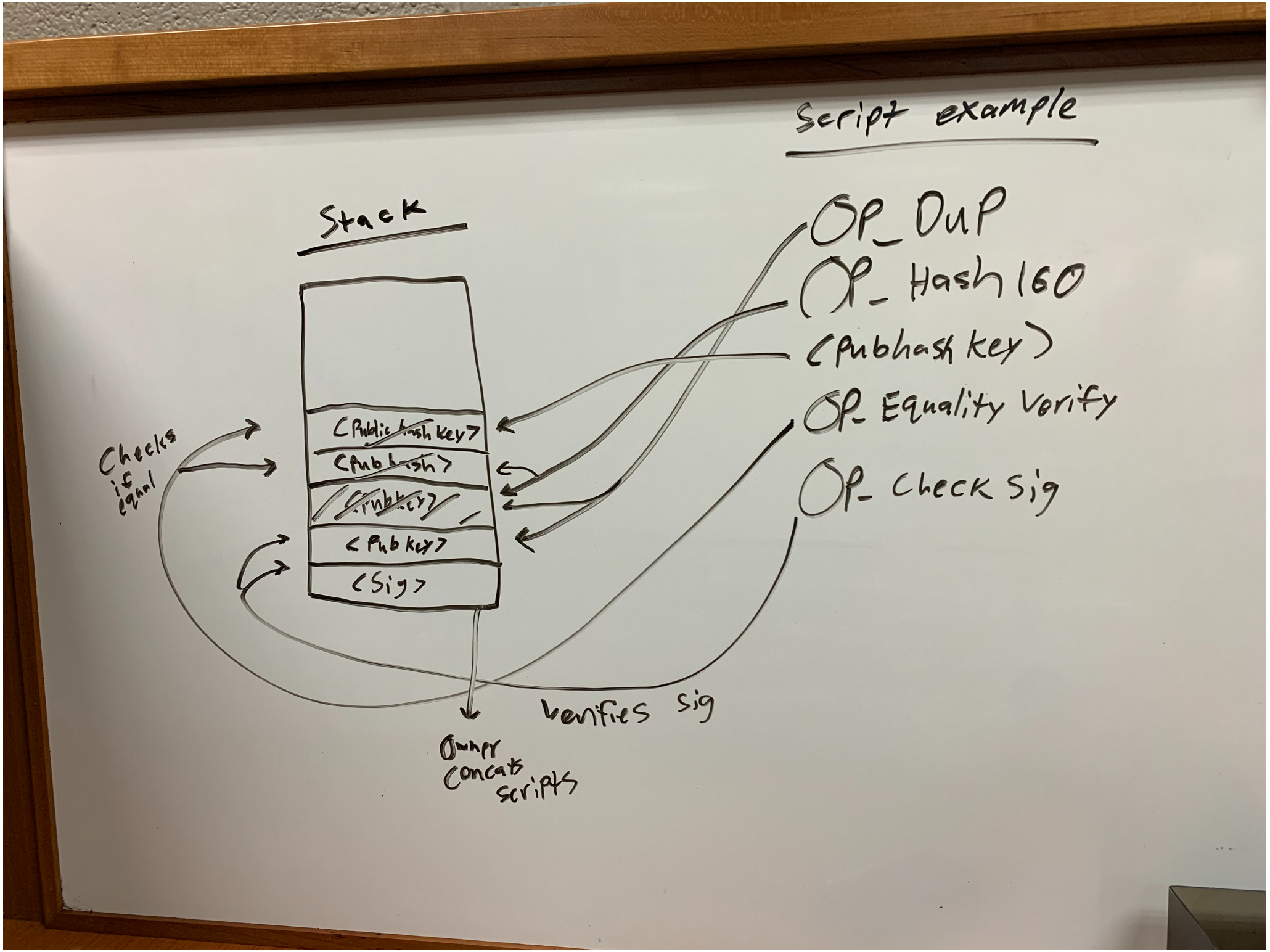


If a miner is too slow, they need to recreate a block with new transactions and a new hash pointer to the newest block

Miners → create a block of transactions and hash it until the hash is lower than target, then broadcast it to the chain

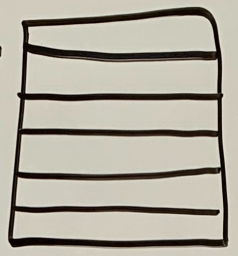


after broadcasting, they gain the mining reward


Script example
Stack
OP_DUP
OP_Hash160
<Pubhash key>
OP_Equality Verify
OP_Check Sig
Checks if equal
<Pub key>
<Sig>
verifies sig
Output
Concats
scripts

Transactions

- Each is held in a block →



- Each has inputs (signed by Owners) and Outputs
- Each input references a previous output, which is verified by a script:

<sig> <public key> OP_DUP OP_HASH160 <Pubkey hash> OP_EqualVerify OP_Checksig

<sig> <public key>: Owner (inputs)

OP_DUP OP_HASH160 <Pubkey hash> OP_EqualVerify OP_Checksig: Previous transaction Script (output)

- using stack, an Owner verifies that coin is his
- He can then reference it as an input for a new transaction
- The UTXO set is a set of all unspent transaction outputs for Owners to reference in transactions