Previously: protocol, transactions, wallets & addresses, double-spending, PoW, blockchain, 51 % attack

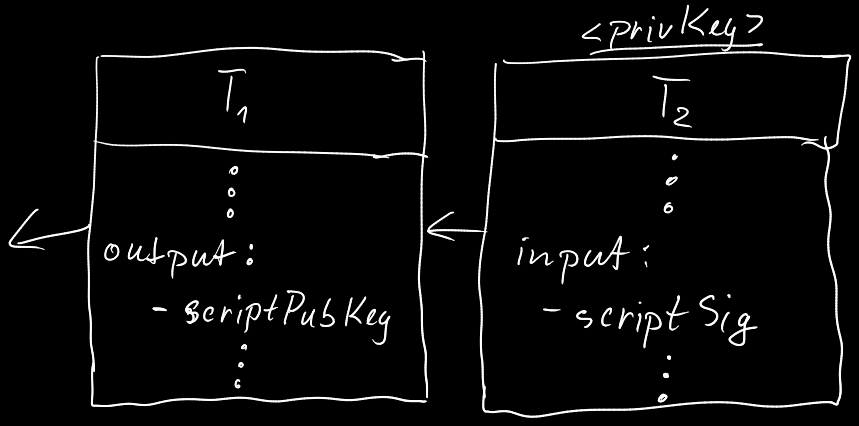
P/O

Today: Script, Merkle trees, SPV, coinbase transactions, mining pools, fees, halving

---

Script

Instruction	Input	Output
• OP_DUP	x	x, x
• OP_EQUAL	x_1, x_2	t/f
• OP_VERIFY	t/f	nothing / fail
• OP_EQUALVERIFY	x_1, x_2	nothing / fail
• OP_HASH160	x	RIPEMD-160(SHA-256(x))
• OP_CHECKSIG	<sig><pubkey>	t/f



Script is not Turing complete.

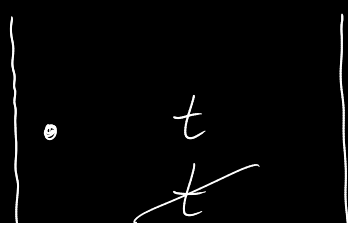
Ethereum, Solidity - Turing complete.

Owner 1 Owner 2

address

② scriptPubKey = OP_DUP, OP_HASH160, <pubKeyHash>, OP_EQUALVERIFY, OP_CHECKSIG

① scriptSig = <sig> <pubKey>

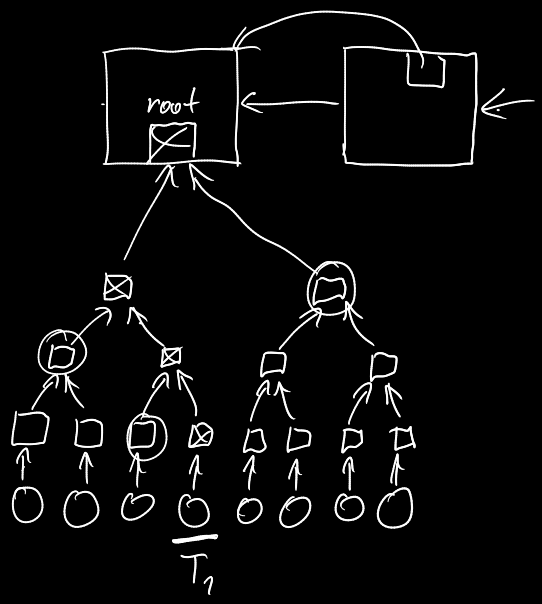


<pubKeyHash>
<H(pubKey)>
<pubKey>
<pubKey>
<pubKey>
<sig>

Merkle Trees, SPV

Block header:
- version 4B
- prev. block hash 32B
- Merkle root 32B
- time 4B
- bits 4B
- ~~nonce~~ 4B

} 80 B, 50 MB



Target

$t = m \cdot \underbrace{256^{(e-3)}}_{\text{posuv doľava o } (e-3)\,B}$

$t_n = t_p \cdot \frac{\vartheta}{2\,weeks}$ 2016

Coinbase trasactions

$1\,BTC = 10^8$ satoshi(s)

$\Sigma BTC = \frac{\sum_{i=0}^{32} 210\,000 \left\lfloor \frac{50 \cdot 10^8}{2^i} \right\rfloor}{10^8} < 21 \cdot 10^6$

```
subsidy(height, interval)
        halvings = height / interval
        if (halvings >= 64)
                return 0
        subsidy = 50 * COIN.
        subsidy >>= halvings
        return subsidy
```

interval = 210 000
COIN = 10^8

$21 \cdot 10^{14} < 2^{53}$

Mining pools → shares