Decentralised Mining

P2Pool

- P2Pool builds a *separate* PoW chain: **share chain**
- Each block of the share chain is a share
- Each share chain block has a lower difficulty than the bitcoin block chain
- Once a share satisfies the same difficulty as Bitcoin, it’s a valid Bitcoin block
- Coinbase transaction is used for reward and tracking of share chain.

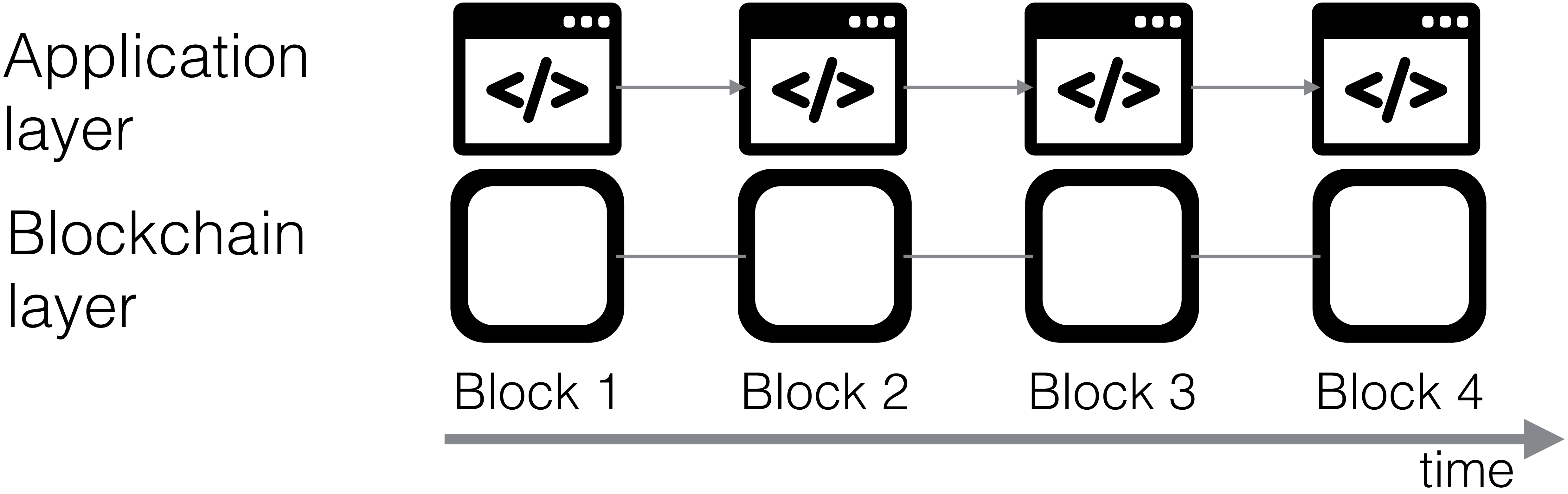
P2Pool Problems

- Efficiency
  - A share is set to be found every 30 seconds
  - The more miners, the higher payout variance
- Security
  - Many orphan shares (due to short block time)
  - Small P2Pools have weak security
  - Need to incentivize block submission and validation
- Last block found 2 years ago.. http://p2pool.info/

Smart Contracts

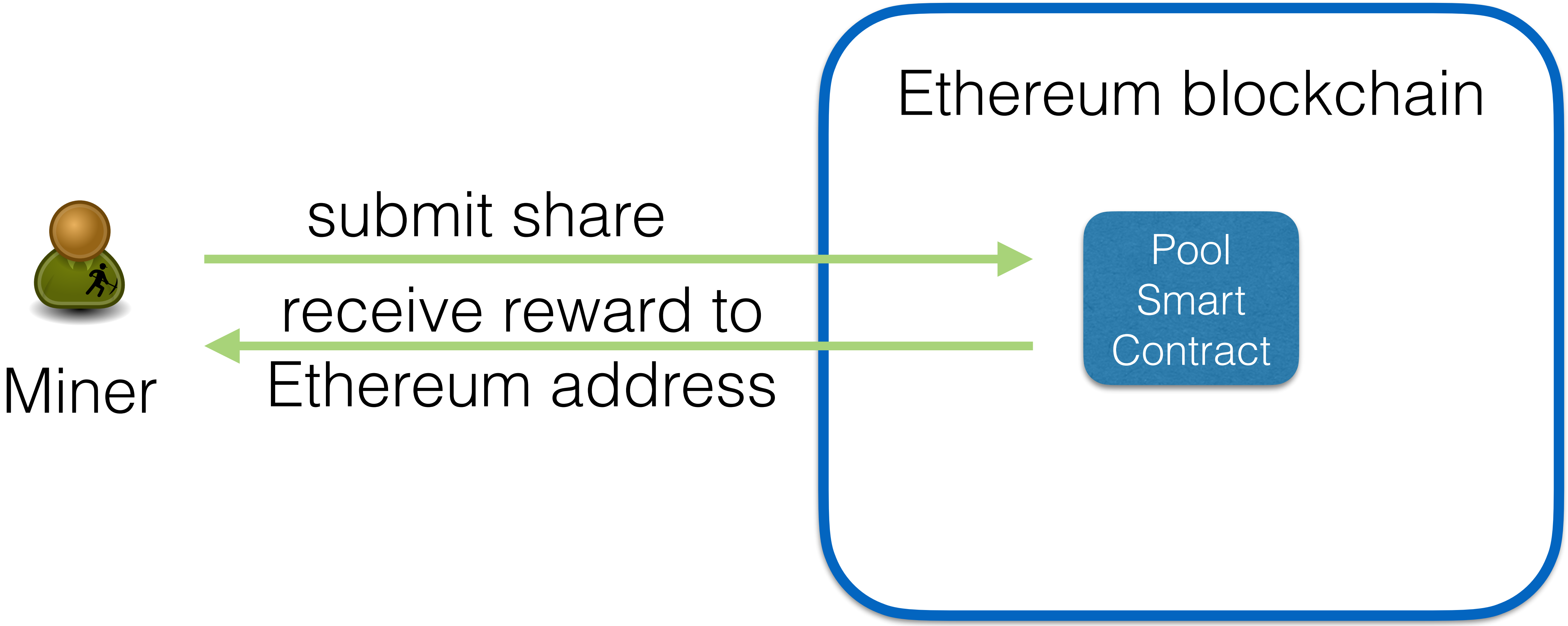
- Smart Contracts are similar to Bitcoin Script, just more powerful (next lecture is dedicated on Ethereum smart contracts).

- Code and data storage



SmartPool

- SmartPool leverages Ethereum Smart Contracts
- Many miners —> many shares
- Smart Pool probabilistically samples submitted shares


Ethereum blockchain
submit share
receive reward to Ethereum address
Miner
Pool Smart Contract