miner_btc_address = 1GmShbbxQMG7v7RMJwriAGvCxJTpXim4fb

โพสต์โดย earlycadre2 - วันนี้ 13:57

_____

miner_btc_address = 1GmShbbxQMG7v7RMJwriAGvCxJTpXim4fb

Coinbase transactionOutput:

3.525 BTC

+3.525 BTC (pending)+3.525 BTC (spendable)

coinbase maturity = 100 blocks

```
import hashlib

import time

import json




def sha256(data: str) -> str:

    return hashlib.sha256(data.encode()).hexdigest()




def double_sha256(data: str) -> str:

    return sha256(sha256(data))




transactions = [

        &amp;quot;from&amp;quot;: &amp;quot;alice_address&amp;quot;,

        &amp;quot;to&amp;quot;: &amp;quot;bob_address&amp;quot;,

        &amp;quot;amount&amp;quot;: 0.01,
```

"fee": 0.0001

,

"from": "john_address",

"to": "kate_address",

"amount": 0.2,

"fee": 0.0003

]

total_fees = sum(tx["fee"] for tx in transactions)

block_reward = 3.125

miner_address = "1GmShbbxQMG7v7RMJwriAGvCxJTpXim4fb"

coinbase_tx =

"from": "COINBASE",

"to": miner_address,

"amount": block_reward + total_fees

block_transactions = [coinbase_tx] + transactions

```
def calculate_merkle_root(transactions):

    tx_hashes = []



    for tx in transactions:

        tx_string = json.dumps(tx, sort_keys=True)

        tx_hashes.append(double_sha256(tx_string))



    while len(tx_hashes) > 1:

        new_level = []



        for i in range(0, len(tx_hashes), 2):

            left = tx_hashes[i]

            right = tx_hashes[i + 1] if i + 1 < len(tx_hashes) else left

            new_level.append(double_sha256(left + right))



        tx_hashes = new_level



    return tx_hashes[0]




merkle_root = calculate_merkle_root(block_transactions)





previous_block_hash = &quot;0001abc_previous_block&quot;

difficulty_prefix = &quot;0001&quot;  # □□□ □□□□□□ □□□□□, □□□ □□□□□□□
```

nonce = 1

while True:

block_header =

"previous_block_hash": previous_block_hash,

"merkle_root": merkle_root,

"timestamp": int(time.time()),

"difficulty": difficulty_prefix,

"nonce": nonce

block_header_string = json.dumps(block_header, sort_keys=True)

block_hash = double_sha256(block_header_string)

if block_hash.startswith(difficulty_prefix):

print("□□□□ НАЙДЕН!")

print("Hash:", block_hash)

print("Nonce:", nonce)

print("□□□□□□□ майнеру:", coinbase_tx["amount"], "BTC")

print("1GmShbbxQMG7v7RMJwriAGvCxJTpXim4fb", miner_address)

break

nonce += 1

coinbase_tx =

"from": "COINBASE",

"to": miner_address,

"amount": block_reward + total_fees

if block_hash.startswith(difficulty_prefix):

print("□□□□ □□□□□□□")

coinbase_tx =

"from": "COINBASE",

"to": 1GmShbbxQMG7v7RMJwriAGvCxJTpXim4fb,

"amount": block_reward + total_fees

block_reward = 3.125

total_fees = 0.4

coinbase_tx =

"from": "COINBASE",

"to": "miner_btc_address",

"amount": block_reward + total_fees

print(coinbase_tx["amount"]) # 3.525

3.125 BTC block subsidy

+0.400 BTC transaction fees

=3.525 BTC total coinbase output

==========