BÁO CÁO TUẦN 1

Chuyên đề: ĐÀO MỘ BITCOIN

HV: Nguyễn Duy Minh

Công việc 1: Tìm hiểu cấu trúc của một block trong Bitcoin

Cấu trúc của một block:

Trường	Mô tả	Kích thước (bytes)
Magic No	Giá trị luôn luôn là 0xD9B4BEF9	4
Blocksize	Số bytes của một block	4
Block Header	Gồm 6 thành phần	80
Transaction counter	VarInt	1-9
Transactions	Danh sách các transactions	

Cấu trúc của một Block Header:

Trường	Mô tả	Cập nhật khi...	Kích thước (bytes)
Version	Phiên bản của block	Cập nhật phần mềm	4
hashPrevBlock	Giá trị hash của block header block liền trước		32
hashMerklRoot	Giá trị hash dựa trên tất cả các transaction bên trong block	Một transaction được accept	32
Time	Current timestamp	Thay đổi mỗi giây	4
Bits	Current Target (Cách tính sẽ được trình bày bên dưới)	Độ khó được điều chỉnh	4
Nonce	Số 32-bits		4

Cấu trúc của một Transaction:

Trường	Mô tả	Kích thước (bytes)
Version		4
In-counter	Số lượng inputs (VarInt)	1-9
list of inputs	Danh sách các input	
Out-Counter	Số lượng output (VarInt)	1-9
list of Output	Danh sách các output	
lock_time		4

Cấu trúc của một input:

Trường	Mô tả	Kích thước (bytes)
Previous Transaction hash	double hash của trans trước	32
Previous Txout-index	index của output được dùng trong transaction	4
Txin-script length	VarInt	1-9
Txin-script / scriptSig	Script	
sequence_no	thông thường là 0xFFFFFFFF	4

Cấu trúc của một output:

Trường	Mô tả	Kích thước (bytes)
Value	Số nguyên không âm, số lượng Satoshis	8
Txout-script length	VarInt	1-9
Txout-script / scriptPubKey	Script	

Công việc 2: Hiện thực simple code để parse data của 2048 bytes đầu tiên của file blk00000.dat

Trong 2048 bytes đầu tiên, chứa data của 9 block nhưng chỉ có 8 block là đủ data, block thứ 9 bị thiếu (**cụ thể thiếu 29 bytes**)

Dữ liệu của 8 block đầu tiên như sau:

Height	Data

#0	{
	"block_header": {
	"bits": "1d00ffff",
	"hash_merkel_root":
	"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
	"hash_prev_block":
	"0000000000000000000000000000000000000000000000000000000000000000",
	"none": 2083236893,
	"time": "2009-01-03 18:15:05",
	"version": 1
	},
	"block_size": 285,
	"magic_no": "f9beb4d9",
	"transaction_counter": 1,
	"transactions": [
	{
	"in_counter": 1,
	"inputs": [
	{
	"prev_trans_hash":
	"0000000000000000000000000000000000000000000000000000000000000000",
	"prev_txout_index": "ffffffff",
	"sequence_no": "ffffffff",
	"txin_script":
	"04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436861696e636
	56c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722
	062616e6b73",
	"txin_script_length": 77
	}
	],
	"lock_time": "00000000",

```
            "out_counter": 1,
            "outputs": [
                {
                    "txout_script":
"4104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f
6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac",
                    "txout_script_length": 67,
                    "value": "5000000000 Satoshi (50.0 BTC)"
                }
            ],
            "version": 1
        }
```


#1


```
{
   "block_header": {
       "bits": "1d00ffff",
       "hash_merkel_root":
"0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098",
       "hash_prev_block":
"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
       "none": 2573394689,
       "time": "2009-01-09 02:54:25",
       "version": 1
   },
   "block_size": 215,
   "magic_no": "f9beb4d9",
   "transaction_counter": 1,
   "transactions": [
       {
           "in_counter": 1,
           "inputs": [
               {
                   "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000000000",
                   "prev_txout_index": "ffffffff",
                   "sequence_no": "ffffffff",
                   "txin_script": "04ffff001d0104",
                   "txin_script_length": 7
               }
           ],
```

<table>
<tr><td></td><td><pre>
            "lock_time": "00000000",
            "out_counter": 1,
            "outputs": [
                {
                    "txout_script":
"410496b538e853519c726a2c91e61ec11600ae1390813a627c66fb8be7947be63c52da7
589379515d4e0a604f8141781e62294721166bf621e73a82cbf2342c858eeac",
                    "txout_script_length": 67,
                    "value": "5000000000 Satoshi (50.0 BTC)"
                }
            ],
            "version": 1
        }
    ]
}
</pre></td></tr>
<tr><td>#2</td><td><pre>
{
    "block_header": {
        "bits": "1d00ffff",
        "hash_merkel_root":
"9b0fc92260312ce44e74ef369f5c66bbb85848f2eddd5a7a1cde251e54ccfdd5",
        "hash_prev_block":
"00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048",
        "none": 1639830024,
        "time": "2009-01-09 02:55:44",
        "version": 1
    },
    "block_size": 215,
    "magic_no": "f9beb4d9",
    "transaction_counter": 1,
    "transactions": [
        {
            "in_counter": 1,
            "inputs": [
                {
                    "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000000000",
                    "prev_txout_index": "ffffffff",
                    "sequence_no": "ffffffff",
                    "txin_script": "04ffff001d010b",
                    "txin_script_length": 7
</pre></td></tr>
</table>

<table>
<tr><td></td><td><pre>
                }
            ],
            "lock_time": "00000000",
            "out_counter": 1,
            "outputs": [
                {
                    "txout_script":
"41047211a824f55b505228e4c3d5194c1fcfaa15a456abdf37f9b9d97a4040afc073dee
6c89064984f03385237d92167c13e236446b417ab79a0fcae412ae3316b77ac",
                    "txout_script_length": 67,
                    "value": "5000000000 Satoshi (50.0 BTC)"
                }
            ],
            "version": 1
        }
    ]
}
</pre></td></tr>
<tr><td>#3</td><td><pre>
{
   "block_header": {
       "bits": "1d00ffff",
       "hash_merkel_root":
"999e1c837c76a1b7fbb7e57baf87b309960f5ffefbf2a9b95dd890602272f644",
       "hash_prev_block":
"000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd",
       "none": 1844305925,
       "time": "2009-01-09 03:02:53",
       "version": 1
   },
   "block_size": 215,
   "magic_no": "f9beb4d9",
   "transaction_counter": 1,
   "transactions": [
       {
           "in_counter": 1,
           "inputs": [
               {
                   "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000000000",
                   "prev_txout_index": "ffffffff",
                   "sequence_no": "ffffffff",
</pre></td></tr>
</table>

<table>
<tr><td></td><td><pre>
                    "txin_script": "04ffff001d010e",
                    "txin_script_length": 7
                }
            ],
            "lock_time": "00000000",
            "out_counter": 1,
            "outputs": [
                {
                    "txout_script":
"410494b9d3e76c5b1629ecf97fff95d7a4bbdac87cc26099ada28066c6ff1eb9191223c
d897194a08d0c2726c5747f1db49e8cf90e75dc3e3550ae9b30086f3cd5aaac",
                    "txout_script_length": 67,
                    "value": "5000000000 Satoshi (50.0 BTC)"
                }
            ],
            "version": 1
        }
    ]
}
</pre></td></tr>
<tr><td>#4</td><td><pre>
{
    "block_header": {
        "bits": "1d00ffff",
        "hash_merkel_root":
"df2b060fa2e5e9c8ed5eaf6a45c13753ec8c63282b2688322eba40cd98ea
067a",
        "hash_prev_block":
"0000000082b5015589a3fdf2d4baff403e6f0be035a5d9742c1cae629546
4449",
        "none": 2850094635,
        "time": "2009-01-09 03:16:28",
        "version": 1
    },
    "block_size": 215,
    "magic_no": "f9beb4d9",
    "transaction_counter": 1,
    "transactions": [
        {
            "in_counter": 1,
            "inputs": [
</pre></td></tr>
</table>

<table>
<tr><td></td><td><pre>
                {
                    "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000000000",
                    "prev_txout_index": "ffffffff",
                    "sequence_no": "ffffffff",
                    "txin_script": "04ffff001d011a",
                    "txin_script_length": 7
                }
            ],
            "lock_time": "00000000",
            "out_counter": 1,
            "outputs": [
                {
                    "txout_script":
"4104184f32b212815c6e522e66686324030ff7e5bf08efb21f8b00614fb7
690e19131dd31304c54f37baa40db231c918106bb9fd43373e37ae31a0bef
c6ecaefb867ac",
                    "txout_script_length": 67,
                    "value": "5000000000 Satoshi (50.0 BTC)"
                }
            ],
            "version": 1
        }
    ]
}
</pre></td></tr>
<tr><td>#5</td><td><pre>
{
    "block_header": {
        "bits": "1d00ffff",
        "hash_merkel_root":
"63522845d294ee9b0188ae5cac91bf389a0c3723f084ca1025e7d9cdfe48
1ce1",
        "hash_prev_block":
"000000004ebadb55ee9096c9a2f8880e09da59c0d68b1c228da88e48844a
1485",
        "none": 2011431709,
        "time": "2009-01-09 03:23:48",
        "version": 1
</pre></td></tr>
</table>

<table>
<tr><td></td><td><pre>
   },
   "block_size": 215,
   "magic_no": "f9beb4d9",
   "transaction_counter": 1,
   "transactions": [
       {
           "in_counter": 1,
           "inputs": [
               {
                   "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000000000",
                   "prev_txout_index": "ffffffff",
                   "sequence_no": "ffffffff",
                   "txin_script": "04ffff001d0120",
                   "txin_script_length": 7
               }
           ],
           "lock_time": "00000000",
           "out_counter": 1,
           "outputs": [
               {
                   "txout_script":
"410456579536d150fbce94ee62b47db2ca43af0a730a0467ba55c79e2a7e
c9ce4ad297e35cdbb8e42a4643a60eef7c9abee2f5822f86b1da242d9c230
1c431facfd8ac",
                   "txout_script_length": 67,
                   "value": "5000000000 Satoshi (50.0 BTC)"
               }
           ],
           "version": 1
       }
   ]
}
</pre></td></tr>
<tr><td>#6</td><td><pre>
{
   "block_header": {
       "bits": "1d00ffff",
       "hash_merkel_root":
</pre></td></tr>
</table>

```
"20251a76e64e920e58291a30d4b212939aae976baca40e70818ceaa596fb
9d37",
       "hash_prev_block":
"000000009b7262315dbf071787ad3656097b892abffd1f95a1a022f896f5
33fc",
       "none": 2538380312,
       "time": "2009-01-09 03:29:49",
       "version": 1
   },
   "block_size": 215,
   "magic_no": "f9beb4d9",
   "transaction_counter": 1,
   "transactions": [
       {
           "in_counter": 1,
           "inputs": [
               {
                   "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000
0000",
                   "prev_txout_index": "ffffffff",
                   "sequence_no": "ffffffff",
                   "txin_script": "04ffff001d0123",
                   "txin_script_length": 7
               }
           ],
           "lock_time": "00000000",
           "out_counter": 1,
           "outputs": [
               {
                   "txout_script":
"410408ce279174b34c077c7b2043e3f3d45a588b85ef4ca466740f848ead
7fb498f0a795c982552fdfa41616a7c0333a269d62108588e260fd5a48ac8
e4dbf49e2bcac",
                   "txout_script_length": 67,
                   "value": "5000000000 Satoshi (50.0 BTC)"
               }
           ],
           "version": 1
```

	}] }

#7	{
	"block_header": {
	"bits": "1d00ffff",
	"hash_merkel_root": "8aa673bc752f2851fd645d6a0a92917e967083007d9c1684f9423b100540673f",
	"hash_prev_block": "000000003031a0e73735690c5a1ff2a4be82553b2a12b776fbd3a215dc8f778d",
	"none": 2258412857,
	"time": "2009-01-09 03:39:29",
	"version": 1
	},
	"block_size": 215,
	"magic_no": "f9beb4d9",
	"transaction_counter": 1,
	"transactions": [
	{
	"in_counter": 1,
	"inputs": [
	{
	"prev_trans_hash": "0000000000000000000000000000000000000000000000000000000000000000",
	"prev_txout_index": "ffffffff",
	"sequence_no": "ffffffff",
	"txin_script": "04ffff001d012b",
	"txin_script_length": 7
	}
	],
	"lock_time": "00000000",
	"out_counter": 1,
	"outputs": [
	{
	"txout_script":

```
"4104a59e64c774923d003fae7491b2a7f75d6b7aa3f35606a8ff1cf06cd3
317d16a41aa16928b1df1f631f31f28c7da35d4edad3603adb2338c4d4dd2
68f31530555ac",
                    "txout_script_length": 67,
                    "value": "5000000000 Satoshi (50.0 BTC)"
                }
            ],
            "version": 1
        }
    ]
}
```


Công việc 3: Tính hash của block header và kiểm tra lại kết quả

Cách tính block header:

```
sha256(sha256(
      version
      + hash_prev_block
      + hash_merkle_root
      + time
      + bits
      + nonce
))
```

Ví dụ với block #0
header =


```
01000000000000000000000000000000000000000000000000000000000000000000000003
ba3edfd7a7b12b27ac72c3e67768f617fc81bc3888a51323a9fb8aa4b1e5e4a29ab5f49ffff001
d1dac2b7c
```


Sau khi double hash ta được giá trị:


```
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```


Sau khi tính được hash của block header cần kiểm tra kết quả với target (được tính từ bits)

Nói nhanh qua về target:
Các miner phải thực hiện tính hash của block header, và nếu **hash này nhỏ hơn hoặc bằng với target hiện tại** thì thì hash đó mới được chấp nhận (cũng đồng nghĩa với việc miner đó được ghi block vào blockchain và nhận phần thưởng bitcoin từ hệ thống). Từ đó nhận thấy rằng **target càng thấp thì càng khó để tạo ra một block**.

Trường **bits** chính là trường lưu trữ giá trị target của block hiện tại. Tuy nhiên, giá trị này được lưu trữ ở dạng nén (compact) vì chỉ có 4 bytes, trong khi target là một số có 32 bytes.

Để hiểu rõ hơn cách tính **target** từ **bits**, có thể xét ví dụ ngay ở block #0
bits = 0x**1d**00ffff
0x1d chuyển đổi sang hệ thập phân là 29 → Kích thước của target là 29 bytes
00ffff sẽ là 3 bytes đầu tiên của target
→ target: **00ffff**0000000000000000000000000000000000000000000000000000

Target với dạng đủ 32 bytes:
000000**00ffff**0000000000000000000000000000000000000000000000000000

So sánh với giá trị hash của block #0 đã tính ở trên:

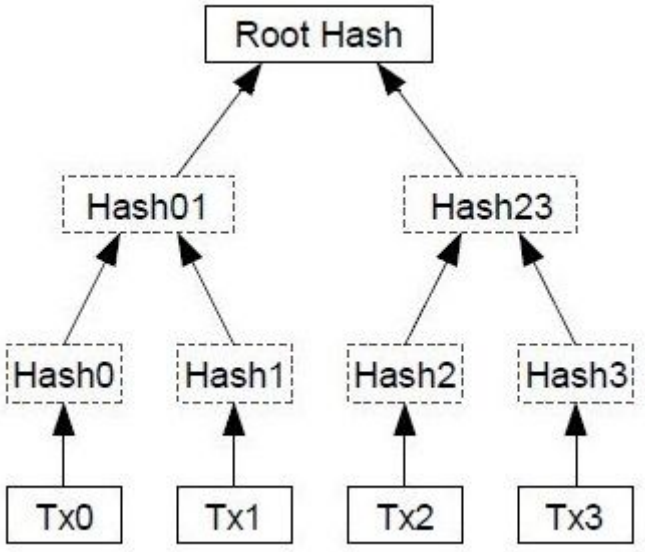
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Ta nhận thấy hash của block thỏa mãn với target!

Target của block #0 cũng chính là target gốc (original target), được sử dụng để tính độ khó (difficulty) theo công thức: **difficulty = original_target / target**

Công việc 4: Tìm hiểu cách tính Merkle Root

Cách tính Merkle Root được mô tả đơn giản như hình bên dưới:



Em có tìm hiểu cách tính trong tường hợp số transactions lẻ, thì mình duplicate node lẻ và tính toán bình thường.

Em cần thêm thời gian để tìm hiểu rõ phần này!

Sau đây là các bước em tính Merkle Root của Block #0


```
"transactions": [
       {
           "in_counter": 1,
           "inputs": [
               {
                   "prev_trans_hash":
"0000000000000000000000000000000000000000000000000000000000000000",
                   "prev_txout_index": "ffffffff",
                   "sequence_no": "ffffffff",
                   "txin_script": "04ffff001d0104",
                   "txin_script_length": 7
               }
           ],
           "lock_time": "00000000",
           "out_counter": 1,
           "outputs": [
               {
                   "txout_script":
"410496b538e853519c726a2c91e61ec11600ae1390813a627c66fb8be7947be63c52da7589379515
d4e0a604f8141781e62294721166bf621e73a82cbf2342c858eeac",
```

```
                "txout_script_length": 67,
                "value": "5000000000 Satoshi (50.0 BTC)"
            }
        ],
        "version": 1
    }
]
```


Đoạn hex string của transaction là:


```
01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff4d04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73ffffffff0100f2052a01000000434104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac00000000
```


Bước 1: **sha256** lần đầu


```
27362e66e032c731c1c8519f43063fe0e5d070db1c0c3552bb04afa18a31c6bf
```


Bước 2: **sha256** lần 2


```
3ba3edfd7a7b12b27ac72c3e67768f617fc81bc3888a51323a9fb8aa4b1e5e4a
```


Bước 3: **convert endian**


```
4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
```


Vậy **Merkle Root** là:


```
4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
```