II.2317 Cybersecurity (ISEP)

LAB Blockchain (Proof-of-Work)

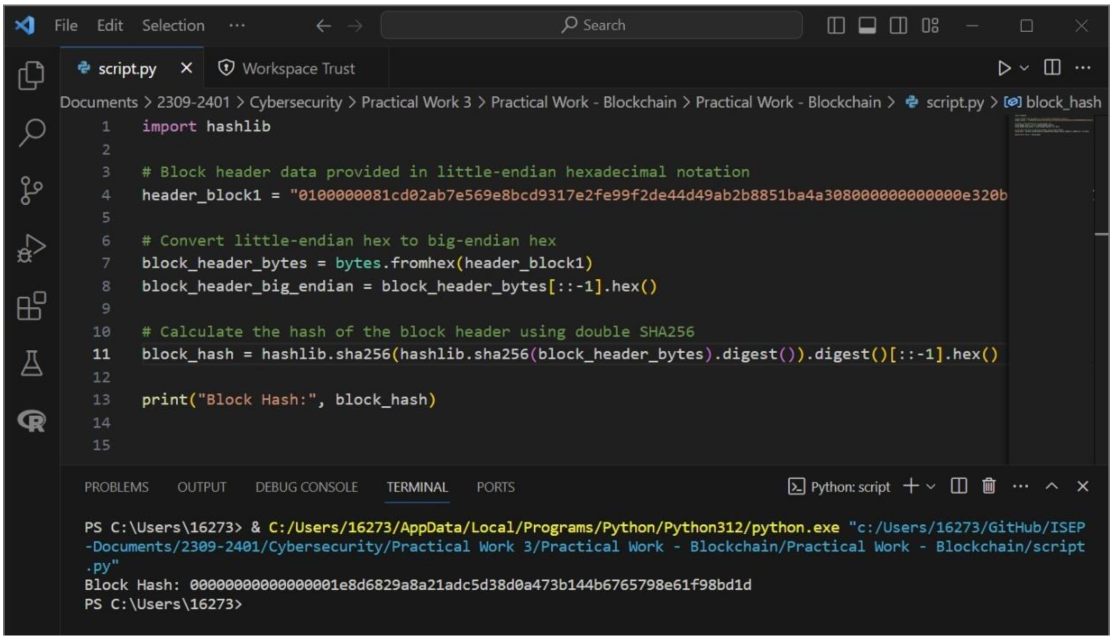
Part I: Understanding the Bitcoin Header…………2

Part 2: Implementation of a PoW…………………4

GUO Xiaofan

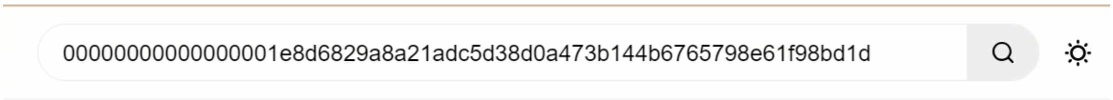
ZHAO Chao

Part I: Understanding the Bitcoin Header

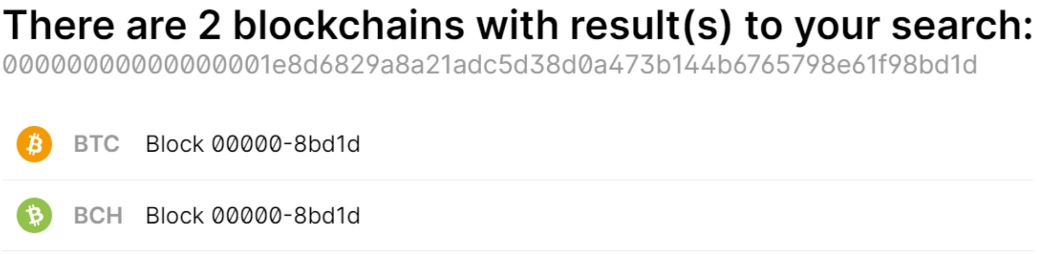

File
Edit
Selection
Search
script.py
Workspace Trust
Documents > 2309-2401 > Cybersecurity > Practical Work 3 > Practical Work - Blockchain > Practical Work - Blockchain > script.py > block_hash
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Python: script

```python
import hashlib

# Block header data provided in little-endian hexadecimal notation
header_block1 = "0100000081cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a308000000000000e320b

# Convert little-endian hex to big-endian hex
block_header_bytes = bytes.fromhex(header_block1)
block_header_big_endian = block_header_bytes[::-1].hex()

# Calculate the hash of the block header using double SHA256
block_hash = hashlib.sha256(hashlib.sha256(block_header_bytes).digest()).digest()[::-1].hex()

print("Block Hash:", block_hash)
```

```
PS C:\Users\16273> & C:/Users/16273/AppData/Local/Programs/Python/Python312/python.exe "c:/Users/16273/GitHub/ISEP
-Documents/2309-2401/Cybersecurity/Practical Work 3/Practical Work - Blockchain/Practical Work - Blockchain/script
.py"
Block Hash: 0000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
PS C:\Users\16273>
```



0000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d

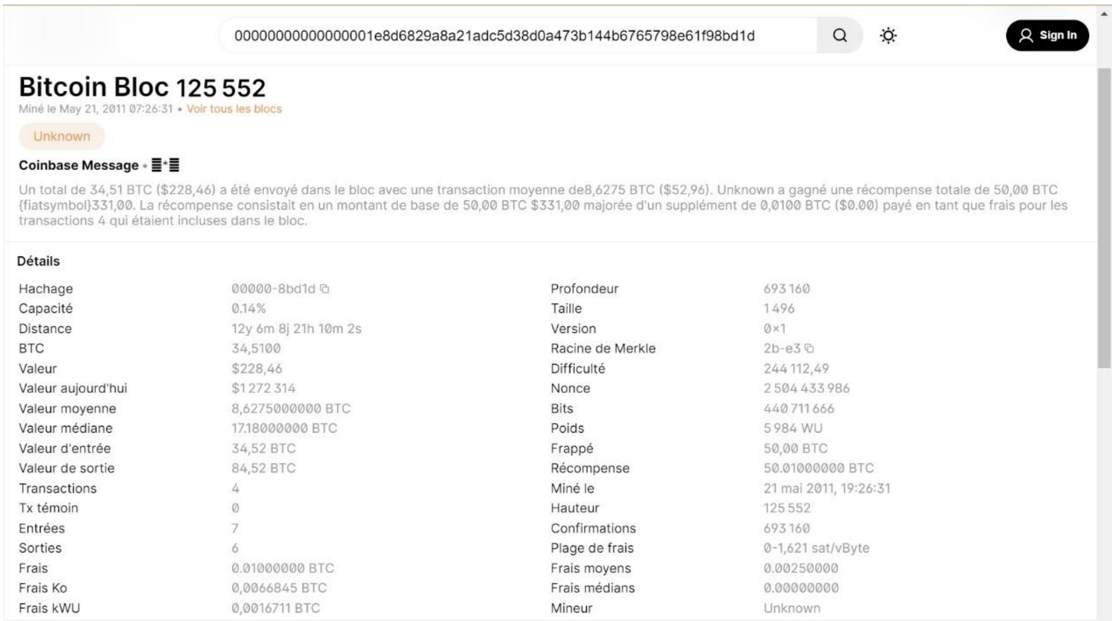


There are 2 blockchains with result(s) to your search:

0000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d

BTC Block 00000-8bd1d

BCH Block 00000-8bd1d



0000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
Sign In

Bitcoin Bloc 125 552

Miné le May 21, 2011 07:26:31 • Voir tous les blocs

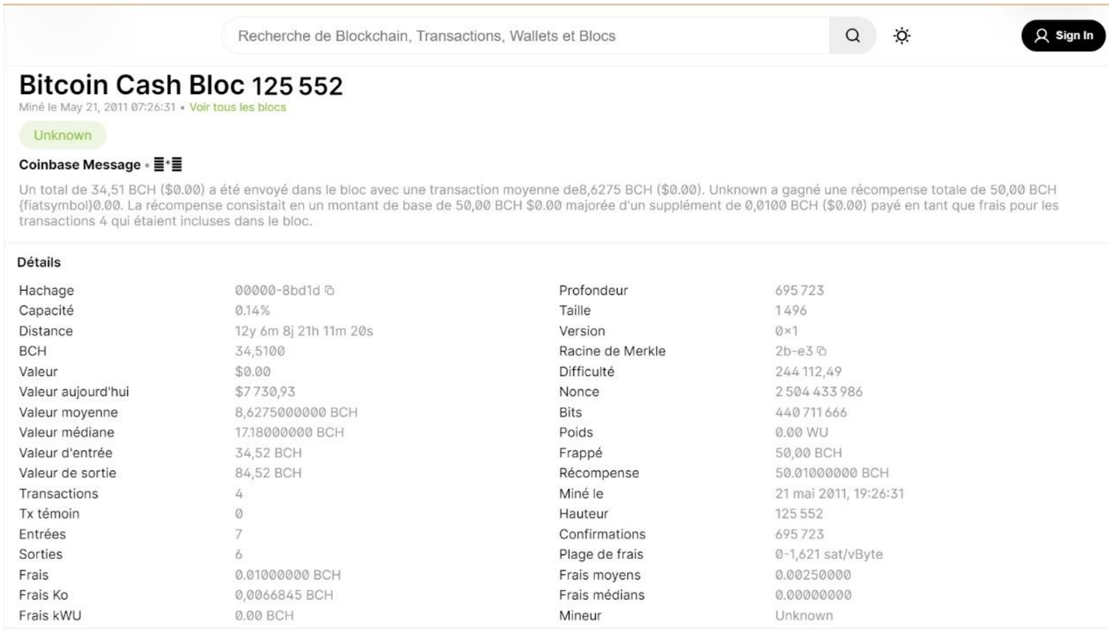
Unknown

Coinbase Message • ≣*≣

Un total de 34,51 BTC ($228,46) a été envoyé dans le bloc avec une transaction moyenne de8,6275 BTC ($52,96). Unknown a gagné une récompense totale de 50,00 BTC {fiatsymbol}331,00. La récompense consistait en un montant de base de 50,00 BTC $331,00 majorée d'un supplément de 0,0100 BTC ($0.00) payé en tant que frais pour les transactions 4 qui étaient incluses dans le bloc.

Détails

Hachage	00000-8bd1d	Profondeur	693 160
Capacité	0.14%	Taille	1 496
Distance	12y 6m 8j 21h 10m 2s	Version	0×1
BTC	34,5100	Racine de Merkle	2b-e3
Valeur	$228,46	Difficulté	244 112,49
Valeur aujourd'hui	$1 272 314	Nonce	2 504 433 986
Valeur moyenne	8,6275000000 BTC	Bits	440 711 666
Valeur médiane	17.18000000 BTC	Poids	5 984 WU
Valeur d'entrée	34,52 BTC	Frappé	50,00 BTC
Valeur de sortie	84,52 BTC	Récompense	50.01000000 BTC
Transactions	4	Miné le	21 mai 2011, 19:26:31
Tx témoin	0	Hauteur	125 552
Entrées	7	Confirmations	693 160
Sorties	6	Plage de frais	0-1,621 sat/vByte
Frais	0.01000000 BTC	Frais moyens	0.00250000
Frais Ko	0,0066845 BTC	Frais médians	0.00000000
Frais kWU	0,0016711 BTC	Mineur	Unknown



Bitcoin Cash Bloc 125 552

Miné le May 21, 2011 07:26:31 • Voir tous les blocs

Unknown

Coinbase Message • ≣*≣

Un total de 34,51 BCH ($0.00) a été envoyé dans le bloc avec une transaction moyenne de8,6275 BCH ($0.00). Unknown a gagné une récompense totale de 50,00 BCH {fiatsymbol}0.00. La récompense consistait en un montant de base de 50,00 BCH $0.00 majorée d'un supplément de 0,0100 BCH ($0.00) payé en tant que frais pour les transactions 4 qui étaient incluses dans le bloc.

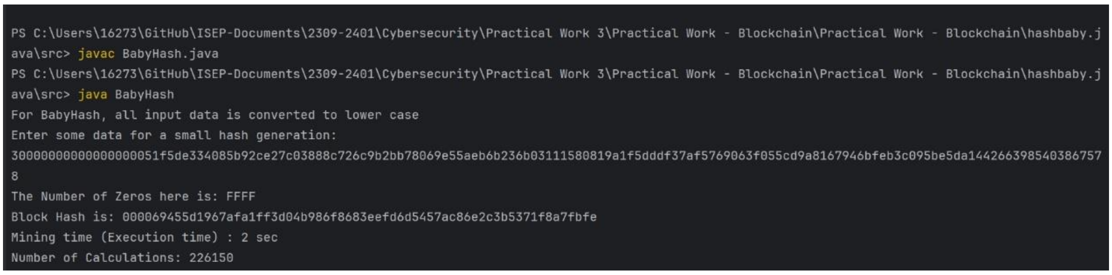
Détails

Hachage	00000-8bd1d	Profondeur	695 723
Capacité	0.14%	Taille	1 496
Distance	12y 6m 8j 21h 11m 20s	Version	0×1
BCH	34,5100	Racine de Merkle	2b-e3
Valeur	$0.00	Difficulté	244 112,49
Valeur aujourd'hui	$7 730,93	Nonce	2 504 433 986
Valeur moyenne	8,6275000000 BCH	Bits	440 711 666
Valeur médiane	17.18000000 BCH	Poids	0.00 WU
Valeur d'entrée	34,52 BCH	Frappé	50,00 BCH
Valeur de sortie	84,52 BCH	Récompense	50.01000000 BCH
Transactions	4	Miné le	21 mai 2011, 19:26:31
Tx témoin	0	Hauteur	125 552
Entrées	7	Confirmations	695 723
Sorties	6	Plage de frais	0-1,621 sat/vByte
Frais	0.01000000 BCH	Frais moyens	0.00250000
Frais Ko	0,0066845 BCH	Frais médians	0.00000000
Frais kWU	0.00 BCH	Mineur	Unknown

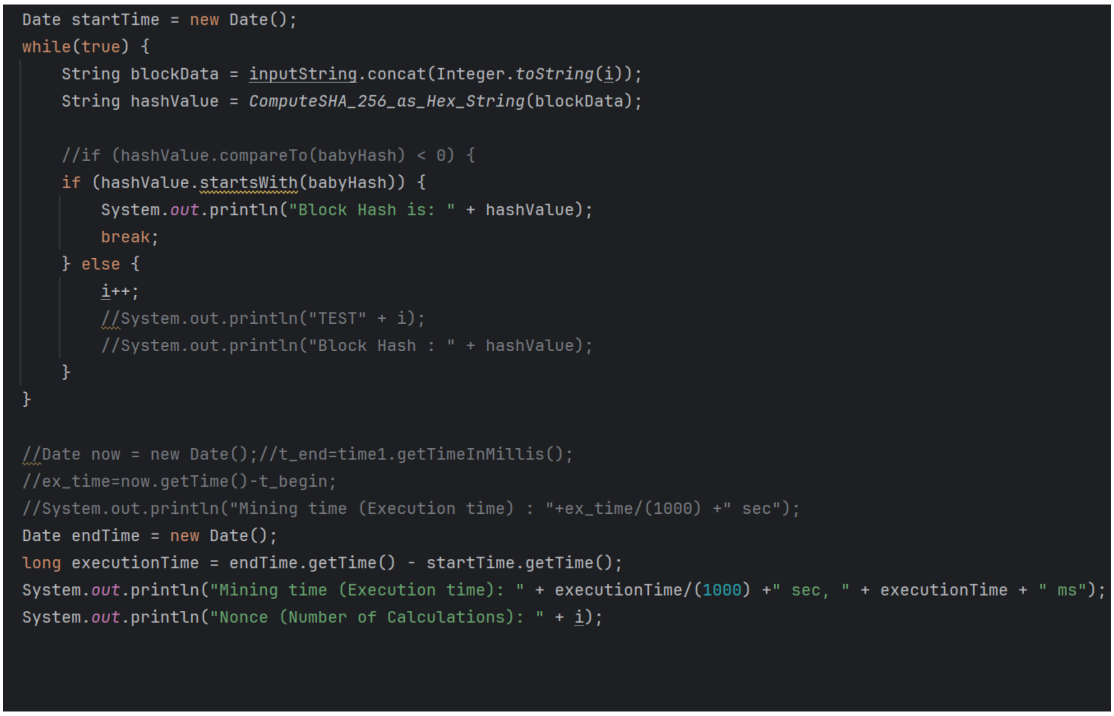
block mined: 21 may 2011, 19:26:31

the number of confirmations: 695 723

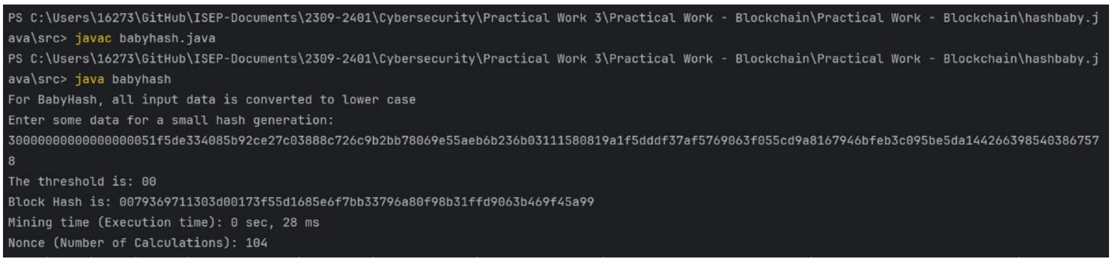
Part 2: Implementation of a PoW



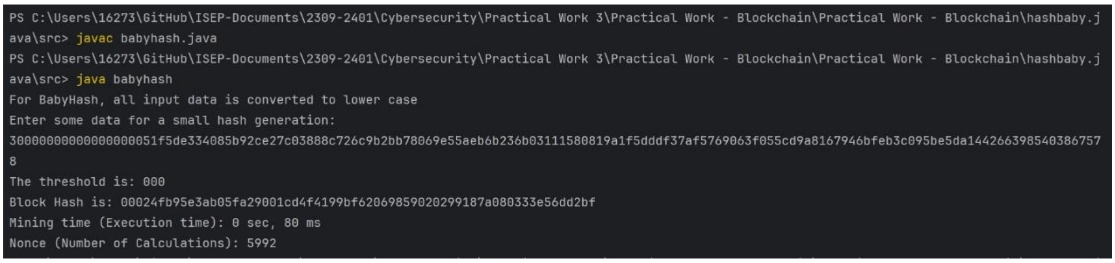
```
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> javac BabyHash.java
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> java BabyHash
For BabyHash, all input data is converted to lower case
Enter some data for a small hash generation:
30000000000000000051f5de334085b92ce27c03888c726c9b2bb78069e55aeb6b236b03111580819a1f5dddf37af5769063f055cd9a8167946bfeb3c095be5da144266398540386757
8
The Number of Zeros here is: FFFF
Block Hash is: 000069455d1967afa1ff3d04b986f8683eefd6d5457ac86e2c3b5371f8a7fbfe
Mining time (Execution time) : 2 sec
Number of Calculations: 226150
```



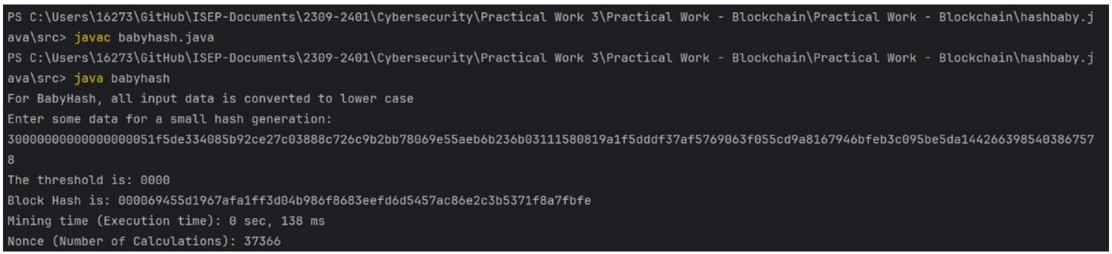
```java
Date startTime = new Date();
while(true) {
    String blockData = inputString.concat(Integer.toString(i));
    String hashValue = ComputeSHA_256_as_Hex_String(blockData);

    //if (hashValue.compareTo(babyHash) < 0) {
    if (hashValue.startsWith(babyHash)) {
        System.out.println("Block Hash is: " + hashValue);
        break;
    } else {
        i++;
        //System.out.println("TEST" + i);
        //System.out.println("Block Hash : " + hashValue);
    }
}

//Date now = new Date();//t_end=time1.getTimeInMillis();
//ex_time=now.getTime()-t_begin;
//System.out.println("Mining time (Execution time) : "+ex_time/(1000) +" sec");
Date endTime = new Date();
long executionTime = endTime.getTime() - startTime.getTime();
System.out.println("Mining time (Execution time): " + executionTime/(1000) +" sec, " + executionTime + " ms");
System.out.println("Nonce (Number of Calculations): " + i);
```



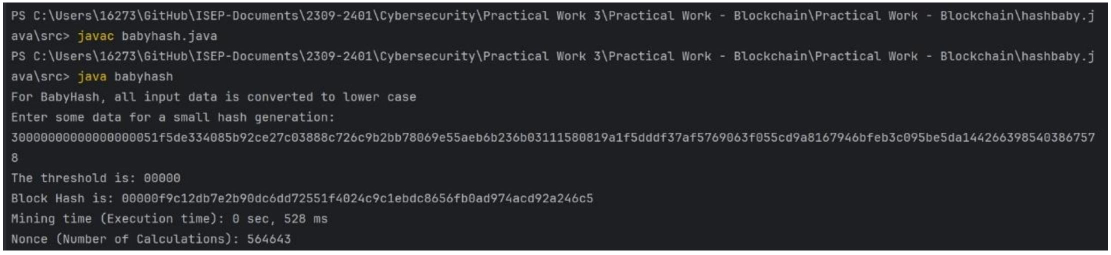
```
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> javac babyhash.java
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> java babyhash
For BabyHash, all input data is converted to lower case
Enter some data for a small hash generation:
30000000000000000051f5de334085b92ce27c03888c726c9b2bb78069e55aeb6b236b03111580819a1f5dddf37af5769063f055cd9a8167946bfeb3c095be5da144266398540386757
8
The threshold is: 00
Block Hash is: 0079369711303d00173f55d1685e6f7bb33796a80f98b31ffd9063b469f45a99
Mining time (Execution time): 0 sec, 28 ms
Nonce (Number of Calculations): 104
```



```
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> javac babyhash.java
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> java babyhash
For BabyHash, all input data is converted to lower case
Enter some data for a small hash generation:
30000000000000000051f5de334085b92ce27c03888c726c9b2bb78069e55aeb6b236b03111580819a1f5dddf37af5769063f055cd9a8167946bfeb3c095be5da144266398540386757
8
The threshold is: 000
Block Hash is: 00024fb95e3ab05fa29001cd4f4199bf62069859020299187a080333e56dd2bf
Mining time (Execution time): 0 sec, 80 ms
Nonce (Number of Calculations): 5992
```



```
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> javac babyhash.java
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> java babyhash
For BabyHash, all input data is converted to lower case
Enter some data for a small hash generation:
30000000000000000051f5de334085b92ce27c03888c726c9b2bb78069e55aeb6b236b03111580819a1f5dddf37af5769063f055cd9a8167946bfeb3c095be5da144266398540386757
8
The threshold is: 0000
Block Hash is: 000069455d1967afa1ff3d04b986f8683eefd6d5457ac86e2c3b5371f8a7fbfe
Mining time (Execution time): 0 sec, 138 ms
Nonce (Number of Calculations): 37366
```



```
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> javac babyhash.java
PS C:\Users\16273\GitHub\ISEP-Documents\2309-2401\Cybersecurity\Practical Work 3\Practical Work - Blockchain\Practical Work - Blockchain\hashbaby.j
ava\src> java babyhash
For BabyHash, all input data is converted to lower case
Enter some data for a small hash generation:
30000000000000000051f5de334085b92ce27c03888c726c9b2bb78069e55aeb6b236b03111580819a1f5dddf37af5769063f055cd9a8167946bfeb3c095be5da144266398540386757
8
The threshold is: 00000
Block Hash is: 00000f9c12db7e2b90dc6dd72551f4024c9c1ebdc8656fb0ad974acd92a246c5
Mining time (Execution time): 0 sec, 528 ms
Nonce (Number of Calculations): 564643
```

Number of Zeros	Execution Time	Number of calculations
00	28ms	104
000	80ms	5992
0000	138ms	37366
00000	528ms	564643