



Understanding basics of Blockchain

Creating a simple **BlockChain** in Python

1.5 Hours session*

S. Joshi

shivgan3@gmail.com

*Last 30 minutes for understanding the code / Audience can open the websites
and play with the tools

Four parts of the session

Introduction - 5 minutes

1. Visually Look at the tool (10-15 minutes)*
2. Come back to the term (10-15 minutes)
3. Understanding Bitcoin Blockchain (5-10 minutes)*
4. Understanding the Implement it in using Python (25-35 minutes)*

* (Audience can open the page)



Part 1 - Looking at the online GUI Tool

Practice using the GUI Tool

Blockchain Demo

Hash

Block

Blockchain

Distributed

Tokens

Coinbase

Blockchain

3

37

012fa9b916eb9078f8d98a7864e697ae83

0b9015ce2a08b61216ba5a0778545bf4d

Mine

Block: # 4

Nonce: 35990

Data:

Prev: 0000b9015ce2a08b61216ba5a0778545bf4d

Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c4f

Mine

Block: # 5

Nonce: 56265

Data:

Prev: 0000ae8bbc96cf89c68be6e10a865cc47c6c4f

Hash: 0000e4b9052fd8aae92a8afda42e2ea0f17972

Mine



Part 2 - Learning more about the terms

Components of block in a Blockchain

Index

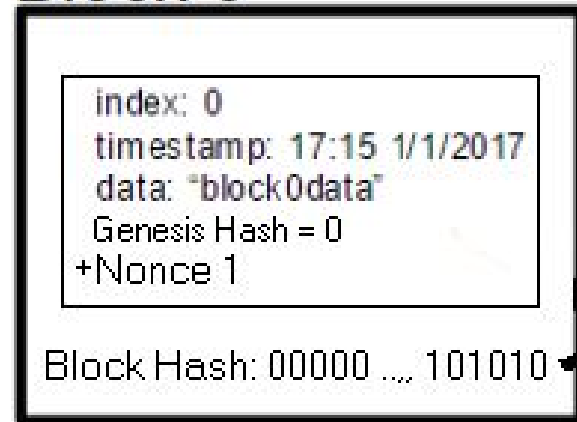
Timestamp

Data

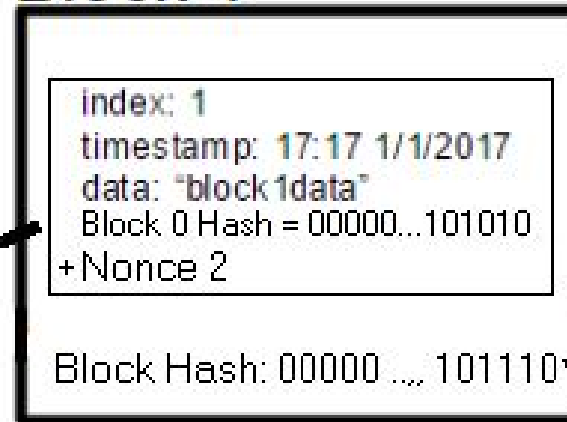
Referring to last block

Hash

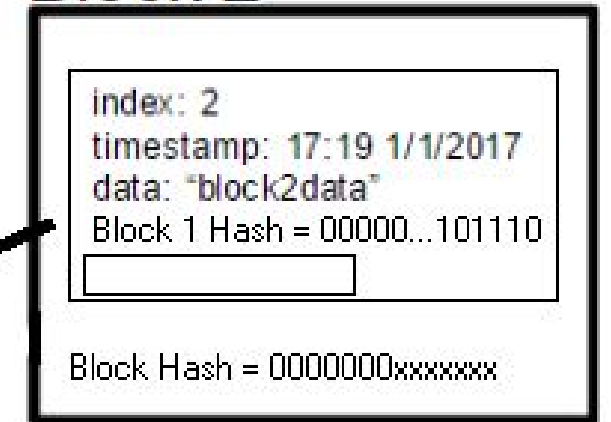
Block 0



Block 1

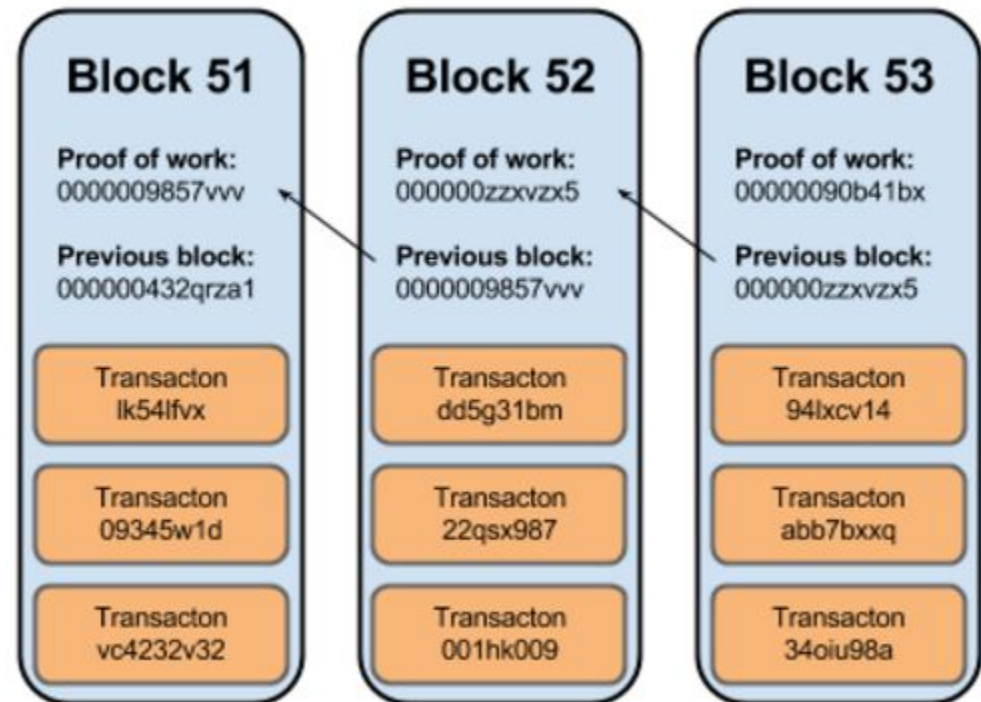


Block 2



Sample Blockchain - Four things about the Block

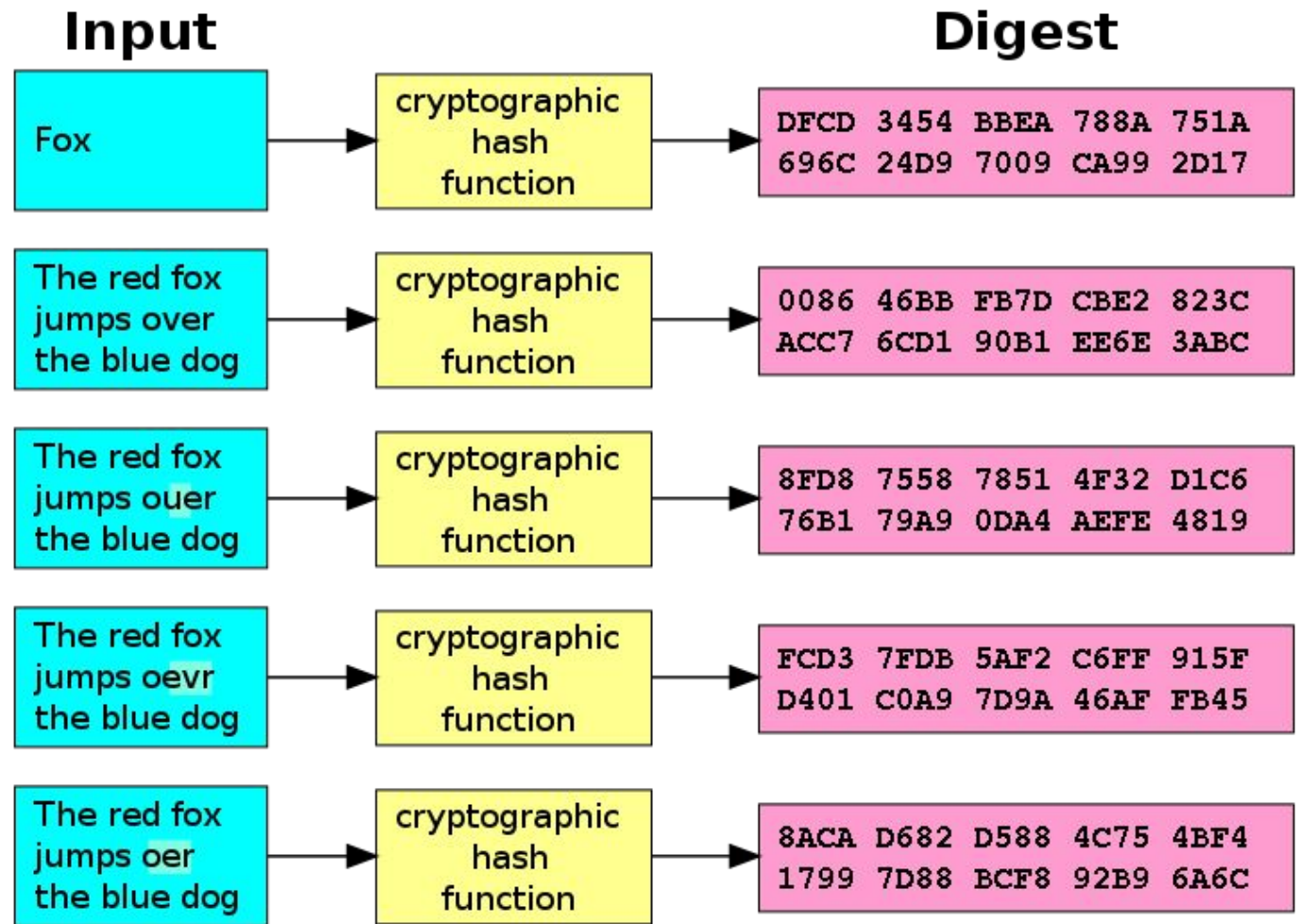
1. A block can have one or many transactions
2. Proof of work is nothing but the same as Hash
3. Each hash is used to link the previous block
4. Any change in value will require us to rehash it



<https://qph.ec.quoracdn.net/main-qimg-83c9a9555372d25d2a6be9d0cb3369df>

Hashing

Different Methods used in hashing



Mining


- The difficulty of mining a block is astounding. At the current difficulty, the chance of a hash succeeding is a bit less than one in 10^{19} .

Example in GUI Tool & Python



Part 3 - Applying what we learned to Bitcoins

Hash in a block of Bitcoin

 **BLOCKCHAIN**
info

HomeChartsStatsMarketsAPIWallet

Search

English

Transaction

View information about a bitcoin transaction

ad41c723258c0f7da48aad01191c8c77015483c4fa700a87395ff041d2509eed


18e55pf66kGYsSMBclAF4vW6TtHSHw0TE
16kKavdcbXwWS7Wazkrcg6VLJbVDG4Xzs9

→

1BBxZrr6Qqf6gkrzTWEAgkETPZYMzEhVSq
13YcacVVyo5J7HEkiPtcJKa3pAxWAF2xpG

0.0150049 BTC
0.03345953 BTC

16 Confirmations0.04846443 BTC

Summary	
Size	373 (bytes)
Received Time	2016-11-18 17:00:00
Lock Time	Block: 439497
Included In Blocks	439546 (2016-11-18 17:06:20 + 6 minutes)
Confirmations	16 Confirmations
Relayed by IP 	37.187.119.41 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.04865143 BTC
Total Output	0.04846443 BTC
Fees	0.000187 BTC
Estimated BTC Transacted	0.03345953 BTC
Scripts	Show scripts & coinbase



Part 4 - Python Implementation

```
import hashlib as hasher
```

```
class Block:
```

```
    def __init__(self, index, timestamp, data, previous_hash):
```

```
        self.index = index
```

```
        self.timestamp = timestamp
```

```
        self.data = data
```

```
        self.previous_hash = previous_hash
```

```
        self.hash = self.hash_block()
```

```
    def hash_block(self):
```

```
        sha = hasher.sha256()
```

```
        sha.update(str(self.index) +
```

```
                    str(self.timestamp) +
```

```
                    str(self.data) +
```

```
                    str(self.previous_hash))
```

```
        return sha.hexdigest()
```