

**Q1: Understand the working of blockchain.**

Visit the following Link: <https://anders.com/blockchain/hash.html> to explore the complexities of blockchain.

Perform the following operations:

(A) Hash: Observe the change in hash value by varying input the data field.

Input: Hello world

## SHA256 Hash

Data:	Hello World
Hash:	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Input: Hello world!

## SHA256 Hash

Data:	Hello World!
Hash:	7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069

**(B) Block:**

1. Observe the hash value of the block. Suggest what does the unusual hash value signifies?

ANS: Hash value is randomly changes even one char or space gets change in Data.

2. Input any arbitrary data in the data field and observe the hash value of the block.

ANS: It looks unique and randomly changes. It used the SHA256 rule.

## SHA256 Hash

<b>Data:</b>	Hello Michael <u>Jacson</u> !!!! See your tomorrow! Thanks bye
<b>Hash:</b>	5ea1e4c1a0fc948df35b60bd8c465f58705d1cb9ada316d9434013e83d0d55d4

3. Mine the block and note the hash value.

# Block

Block:	# 1
Nonce:	3352
Data:	Hello <u>Tumbarika</u> , What's app?
Hash:	000026edbf2a2344ecb4c24bb0c3eabadc5334a73eaa7154f0a2727a8eb189c
<input type="button" value="Mine"/>	

## (C) Blockchain:

1. Study the blockchain
2. Try to input any information in the data field. Observe the change in hash
3. Now, try changing the information any block 2,3 or 4 and observe how the hash value changes in the subsequent blocks.

While entering input in block 1, Hash get change but Prev Hash value has all 0 that means it just started. Block 2 has Prev Hash value of Block 1. Same as, Block 3 has Prev Hash value of Block 2 and Block 4 has Prev Hash value of Block 3. This shows they all linked by Hash values.

## Blockchain

**Block:** # 1

**Nonce:** 11316

**Data:** Ram begin Transferring 1BTC to James

**Prev:** 00

**Hash:** 9f40da6ec40118c83a3309ae46a626faf64324a9e95baa3

Mine

**Block:** # 2

**Nonce:** 35230

**Data:** James transfers to Kevin 0.5 BTC

**Prev:** 9f40da6ec40118c83a3309ae46a626faf64324a9e95baa3

**Hash:** 7f3f8fe9cdf225dace67625d8e856ea0695ba1da3d3b1b7

Mine

## Blockchain

**Block:** # 3

**Nonce:** 12937

**Data:** Kevin got 0.5 BTC from James

**Prev:** 7f3f8fe9cdf225dace67625d8e856ea0695ba1da3d3b1b7

**Hash:** a982c9d427f22e2c4460b30859c6ab4c064b50d15f50e45

Mine

**Block:** # 4

**Nonce:** 35990

**Data:** Kevin bought .1 BTC worth of ETH

**Prev:** a982c9d427f22e2c4460b30859c6ab4c064b50d15f50e45

**Hash:** 95af07920ad3f31de175843ac3ae21dd519d34c1de6566c

Mine

### (D) Distributed Blockchain:

1. Study the distributed blockchain
2. Input any data in the data field of any block in peer A. Observe the change in hash value. Now mine the blocks and verify if the hash value of the blocks is same in every peer

## Distributed Blockchain

Block: # 1

Nonce: 112757

Data: distributed 0 change

Prev: 00

Hash: d8015498955cf51d06e60da2ef08669103a65dc5578875

Mine

Block: # 2

Nonce: 24025

Data: distributed 0 ---- distributed 1 Change

Prev: d8015498955cf51d06e60da2ef08669103a65dc5578875

Hash: cc8728efefc40a467231cb9454d7c8d719c1ad73eb9a35

Mine

Block: # 3

Nonce: 119561

Data: distributed 1 ---- distributed 2

Prev: cc8728efefc40a467231cb9454d7c8d719c1ad73eb9a35

Hash: 5d1e18dc683dbca52e44eb8154f10

Mine

After mining it change the Hash and subsequently changes into the Prev Hash.

[illegible]

## (E) Tokens:

## 1. Study the Tokens

## 2. Observe what happens if you try to change any value of the tokens in any of the blocks

ANS: The Hash value gets change once any value of the tokens in any of the blocks get change. Subsequently it changes into the Prev Hash in the next linked block.

## Tokens

Peer A

Block: # 1

Nonce: 139358

Tx:

\$ 25.00	From: Darcy	->	Bingley
\$ 4.27	From: Elizabeth	->	Jane
\$ 19.20	From: Wickham	->	Lydia
\$ 106.44	From: Lady Car	->	Collins
\$ 6.42	From: Charlotte	->	Elizabeth

Prev: 00

Hash: 273a0bdf3232f622aaa2940769fc2bd17f15fdf2740099

Mine

Block: # 2

Nonce: 39207

Tx:

\$ 97.67	From: Ripley	->	Lambert
\$ 48.61	From: Kane	->	Ash
\$ 6.15	From: Parker	->	Dallas
\$ 10.44	From: Hicks	->	Newt
\$ 88.31	From: Bishop	->	Burke
\$ 45.00	From: Hudson	->	Gorman
\$ 92.00	From: Vasquez	->	Apone

Prev: 273a0bdf3232f622aaa2940769fc2bd17f15fdf2740099

Hash: b20fac5a9fa302fbfb263c907113c61e06f674668181ef

Mine

Block: # 3

Nonce: 13804

Tx:

\$ 10.00	From: Emily		
\$ 5.00	From: Madis		
\$ 20.00	From: Lucas		

Prev: b20fac5a9fa302fbfb263c907113

Hash: ac9acc97b7f244e756adb8b54d69

Mine

According to above example, I understood that each block may have multiple transaction.

## (F) Coinbase

## 1. Study coinbase

## 2. What is coinbase transaction?

Coinbase transactions are the linked transactions.

## Coinbase Transactions

Peer A

Block:

#1

Nonce:

16651

Coinbase:

\$100.00

->

Anders

Tx:

Prev:

00

Hash:

0000438d7625b86a6f366545b1929975a0d3ff1f8847e5f

Mine

Block:	#	2																							
Nonce:	215458																								
Coinbase:	\$ 100.00	-> Anders																							
Tx:	<table><tr><td>\$ 10.00</td><td>From:</td><td>Anders</td><td>-&gt;</td><td>Sophia</td></tr><tr><td>\$ 20.00</td><td>From:</td><td>Anders</td><td>-&gt;</td><td>Lucas</td></tr><tr><td>\$ 15.00</td><td>From:</td><td>Anders</td><td>-&gt;</td><td>Emily</td></tr><tr><td>\$ 15.00</td><td>From:</td><td>Anders</td><td>-&gt;</td><td>Madison</td></tr></table>					\$ 10.00	From:	Anders	->	Sophia	\$ 20.00	From:	Anders	->	Lucas	\$ 15.00	From:	Anders	->	Emily	\$ 15.00	From:	Anders	->	Madison
\$ 10.00	From:	Anders	->	Sophia																					
\$ 20.00	From:	Anders	->	Lucas																					
\$ 15.00	From:	Anders	->	Emily																					
\$ 15.00	From:	Anders	->	Madison																					
Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e5																								
Hash:	0000baeab68c2a60f9a6fa56355438d97c672a15494fce																								
<div>Mine</div>																									

Block:	#	3
Nonce:	146	
Coinbase:	\$	100.00
		->
Tx:	\$	10.00
	From:	Emily
	\$	5.00
	From:	Madiso
	\$	20.00
	From:	Lucas
Prev:	0000baaab58c2a60f9a6fa5635543	
Hash:	0000df1d632b734f5a5fca126ae09e	
<input type="button" value="Mine"/>		

3. As demo shows that Anders get \$100 in coinbase transaction. Now he transfers some money to 5 people. Observe whether the transferred money is less than or equivalent to \$100

ANS: Transfer money is less than \$100.

5. Further, the people who received the money transfers some amount to other people's account. Check if they have money in their account to transfer.

ANS: Yes, they all have got the balance from previous block to transfer to another people's account.