SMVS
Page No.
Date : / /

Bitcoin

* What is Bitcoin and How does it work ?

=> Bitcoin is a decentralized digital currency that operates without a central authority or intermediary.

Bitcoin was created by an anonymous group of people or person using the Pseudonym Satoshi Nakamoto.

Bitcoin operates on a decentralized network of computer that maintain and verifty the blockchain.

Bitcoin transaction are digitally signed for security.

Anyone can create Bitcoin wallet by downloading the bitcoin program.

Each Bitcoin Wallet has two Things :

1) Public Key : It is like addresses which any user receive bitcoin.

2) Private Key : It is a like Digital

signature via which anyone can send bitcoin.

The Public Key can be shared with anyone but Private Key must be Know by Owner.

=> Bitcoin Transaction Work:

1 Initiate Transaction:

If User A want to send Bitcoin to the User B than User A needs User B's Public Key to send Bitcoin.

2 Transaction Creation:

User A's Bitcoin wallet software creates a transaction and specifying the amount of Bitcoin to send User B's public key.

3 Signing The Transaction:

User A's wallet signs the transaction with User A's Private Key.

The digital signature verifies that

SMVS
Page No.
Date : / /

User A is the owner of the Bitcoin.

4 Broadcasting the Transaction:

The Signed Transaction is broadcast to the Bitcoin Network and Nodes in the network receive transaction.

5 Transaction Validation:

Nodes validate by checking.

- The Digital Signature match with User A's Public Key
- User A has enough Bitcoin to send.

6 Inclusion in a Block:

Miners collect validated transaction and include them in the candidate block.

7 Mining and Proof of Work:

Miners complete to find a nonce that produces a block hash meeting the network's difficulty target.

SMVS
Page No.
Date : / /

8 Block Validation and Addition:

Nodes validate the new block, ensuring POW is correct ~~et~~ and all transaction within block is correct.

Once validated, the block is added to the Blockchain, extending it.

9 Transaction Confirmation:

User A's transaction is now confirmed and part of the Blockchain.

* How to Add and Validate the blocks in Bitcoin Network?

=> This are step to add and Validate the block in Bitcoin Network.

1 Transaction Broadcasting:

Users all the created transaction is broadcast the Bitcoin network.

SMVS
Page No.
Date : / /

2 Mining :

Miners collect the transaction along with others and start creating new block.

Miners compete to solve the PoW puzzle by Hashing the block header.

3 Finding a Valid Hash :

Miner Finds a hash that meets the difficulty target and broadcasts the new blocks in the network.

4 Validation By Nodes :

Nodes receive the block and ~~wait~~ validate :

- Block's Hash and All transaction in the Block and Block structure is correct.

5 Adding the Blockchain :

Nodes add the validated block to the blockchain and Transaction now included in the blockchain.

SMVS
Page No.
Date : / /

6 Confirmation :

As new blocks are mined and in added on top the block containg Users transaction.

* Explain Working of Double - Spending Attack.

=> This are the steps, In which Double Spending Attack is occured.

(Race Attack Example or Step)

1 Prepare Transaction :

Attacker creates Two Transaction of Bitcoin : one to a other Merchant (T-A) and one back to their own address (T-B).

2 Broadcast Transaction :

The attacker broadcast both transaction to the Bitcoin network and ~~dot~~ both transaction seen by different nodes and miners.

SMVS
Page No.
Date : / /

3 Merchant Receives Transaction A :

The Merchant seeing Transaction A, may provide goods or services to the attacker.

4 Mining :

Miner can include of the transaction in their block.

A Block containing either transaction A or B is mined and broadcast to network.

5 Resolution and Blockchain Forking :

If both transaction are included in blocks from different miners, a temporary Fork occurs.

The network follows Longest Chain Rule. The Longest chain determines with valid transaction, the other transaction is discarded.

6 Outcome :

If Transaction B is Longest chain,

SMVS
Page No.
Date : / /

the attacker successfully double-spends.

IF Transaction A is confirmed and the attack is Fail.

=> Prevent Double-Spending Attack:

1 Require Multiple Confirmation: Wait For Multiple confirmation before consider the transaction if Final.

2 Use Payment Channels: Implement payment channels like the Lightning Network For Faster transaction, with lower risk.

3 Leverage Blockchain Analysis: Use Blockchain analysis tools to trake and monitor the history of transaction and Find unusual patterns.

4 Adopt Merchant Solution: Utilize service and software designed to detect and prevent attack.

SMVS
Page No.
Date : / /

5 Educate Users and Merchants :

Ensure that users and Merchant wait for the confirmation of transaction.

6 Utilize Secure Payment Gateways :

Employ payment gateways that have built-in fraud detection.

=> Types of Double Spending Attack :

1 Finney Attack :

In this, Merchant accepts an unauthorized transaction and this transaction is performed by the attacker.

Original Block of transaction is eclipsed by the Attacker.

2 Race Attack :

In this Attack, Race is between two transaction and attacker send same money using two different merchant address.

Page No.
Date : / /

3 51 % Attack :

In this Attack, Hackers Usually take 51 % of Mining power of the blockchain.

So, Attacker can do anything with Blockchain network.

* Explain Bitcoin Transaction with Script.

=> Bitcoin Script is a Stack-based, Forth-Like Programming Language.

Script is used to define how Bitcoin transaction can be spent.

It is used to specify condition under which whole Bitcoin transaction can be occured.

Bitcoin Script Operates on a stack data structure.

Operation in Script involve pushing and poping the item From stack.

SMVS
Page No.
Date : / /

=> Script Components:

1 OpCodes : Script Instruction or operation to perform various task.

2 Push Operation : This Instruction push data onto the stack.

3 Pop Operation : This Instruction remove data from the stack and use it for further operation.

=> Script Types:

There are Three Types of Script.

1 Pay-to-PubKey (P2PK):

The Script Type is a simplest form, In which transaction script requires the recipient's public key to be provided to unlock the Bitcoin.

2 Pay-to-Pubkey-Hash:

This Script has two step:

(i) Transaction Script Requires the recipient's public key.

(iii) And This Public Key is match with hash and Unlock the Bitcoin.

3 Pay-to-Script-Hash (P2SH):

This Script is complex to be used.

This Script is used Script Hash to unlock the transaction.

=> Script Execution:

When Transaction is validated than its script is executed by Bitcoin nodes.

The Script needs to be true for the transaction considered to be valid.

ScriptPubKey: The locking Script

ScriptSig: The unlocking Script

Ex.

=>

SMVS
Page No.
Date : / /

Ex. ScriptPubKey :

'OP_DUP OP_HASH160 <PubKeyHash>
OP_EQUALVERIFY OP_CHCKSIG'

ScriptSig : '<Signature><PublicKey>'

=> ScriptPubKey : Here, Transaction is required public key that hash to '<PubKeyHash>' and vaild signature.

ScriptSig : For unlock script, required public key and signature.