Presentation On
Chapter 13
Bitcoin, Blockchains and Ethereum

August 11, 2022

Group Member

1. Salima Akhtar Nabila - 17701025
2. Fahmida Alam - 17701089
3. Labanti Singha - 17701055
4. Khadiza Morioum Sama - 17701084
5. Marufa Sultana - 18701008
6. Tithi Rani Das - 18701030
7. Sejuti Saha Peu - 18701067
8. Farhad Kashem - 18701073

History of Bitcoins

Bitcoins-

- What is Bitcoins?
- When Bitcoins concepts appeared?
- How block chain is related to cryptography?
- Advantages of Bitcoins.
- Disadvantages of Bitcoins.
- Who accepts Bitcoin?
- Why many Govts banned Bitcoin?

Bitcoin Transaction Types and Its Fields

There are 5 types of bitcoin transactions:

- pay-to-public-key-hash (P2PKH)
- public-key
- multi-signature (limited to 15 keys)
- pay-to-script-hash (P2SH)
- data output (OP_RETURN)

Bitcoin transaction fields

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1-9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1-9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

Bitcoin script execution (signature validation)

Script - A list of instructions recorded with each transaction that describe how the next person wanting to spend the Bitcoins being transferred can gain access to them.

Bitcoin Script - It is a stack-based programming language for locking and unlocking transactions. Bitcoin transactions contain scripts.

STACK-BASED MACHINE MODEL

- Linear structure represented by a physical stack or pile.
- Items at the top of the stack can be added (pushed) or removed (popped) in a "Last In, First Out (LIFO)" queue.

EVALUATING INPUT-OUTPUT SCRIPTS

- Execution script is the concatenation of two pieces identified in the input section of the current transaction-
  1. sig
  2. pubkey

Bitcoin script execution (signature validation)

EVALUATING INPUT-OUTPUT SCRIPTS

Instruction	Stack
$< sig >$	$< sig >$
$< pubKey >$	$< pubKey >$ $< sig >$
OP_DUP	$< pubKey >$ $< pubKey >$ $< sig >$
OP_HASH160	$< pubKeyHash >$ $< pubKey >$ $< sig >$
$< pubKeyHash? >$	$< pubKeyHash? >$ $< pubKeyHash >$ $< pubKey >$ $< sig >$
OP_EQUALVERIFY	$< pubKey >$ $< sig >$
OP_CHECKSIG	TRUE

Block structure,Merkle trees and the blockchain

Blockchain- Block structure-

- Block as data structure with transaction.
- A Bitcoin block has two main parts : a block header and an ordered set of detailed transactions each of length typically 250 to 1000 bytes.
- The merkle-root field in the header serves to incorporate the entire ordered list of transactions into the header.
- The header field identifies the previous block in the chain with a hash function, and is a hashlink specifying the hash of that previous block's header.
- The hash of its block header is used to uniquely identify each block.

Merkle tree-

- It's a mathematical data structure or a method of organizing data
- It's made up of hash number of various data blocks of transactions performed of the Blockchain Network.

Block structure, Merkle trees and the blockchain

Block Chain-

- Blocks are back-linked to form the blockchain
- Blockchain is a back-linked list of blocks ordering and integrating all transactions in time, made available as a public ledger.
- It uses secure hash algorithm or SHA

Data Integrity-

- Verifying data integrity of a given blockchain requires holding a reference to the current head block, and a trusted genesis block.
- Each block's prev-block-hash field is dereferenced to get the preceding block, this hashlink's hash field is compared to the hash of that previous block's header.
- In a full blockchain check, this process ends with a match against the hard-coded genesis block, validation failing if any integrity check fails along the way.

Block Chain Mining

Block Chain Mining: Mining is the process of creating new cryptocurrency by solving puzzles.
Mining Process: Number of transaction or capacity. **Memory Pool:** Vereified transaction(information) are kept that wait here until they are included in the block. Each transaction are hashed(T*1,T*2,T*3).Merkle tree is created to get market root. Mercal $root_blockidentify, andcontentverified$.
Candidate Blocks: $atemporaryblock$.
Block Header:
1)$asummaryofalltransationdatainthecandidateblock$,
2)$alinkofpreviousblock$,
3)$thetimeofcreationoftheblock$,
4)$avalidproofofwork$.($Blockheaderisthenhashedtogetablockidentifier$)

When the given puzzle is solved, broadcast the block, and other people in the blockchine verify the block and add it to the blockchine.

Hash Targeting

Target Hash means:

- A target hash is a number that must be greater than or equal to a hashed block header for a new block to be awarded.

Why Target Hash:

- The target hash is used to determine the difficulty of input and can be adjusted to ensure efficient processing of the blocks.

Analyzing Target Hash:

- Taking an string of any length.
- Input length doesn't matter as output always be the same length.
- Each block will contain the preceding block header hash.
- The block header contains the number of the block edition, a timestamp, the hash used in the previous block and the goal hash.
- If the hash meets the target's requirement, then add the block to the blockchain.

Building the blockchain,validation,and full nodes

Blockchain-

- Constantly growing ledger
- Keeps permanent record of all transaction
- Uses a secure chronological way

Validation-

- Transactions and blocks are validated in two different ways.
- Miner validates new transaction and store in global ledger by using Longest Chain Rule and Proof of work (pof).
- Miner gets transaction fees and block fees (new bitcoins) by confirming the transaction

Resolution of a blockchain

- If blocks A and B emerge around the same time-Miners start building on A or B, whichever they receive first.
- Now,block A‘ and B‘ may emerge at the same time but which one is the majority one. That is the majority of miners receive first(here it is B‘).
- B“ emerges, extending B‘, as most miners indicate B as main branch. So, the fork now resolved in favor of branch B.

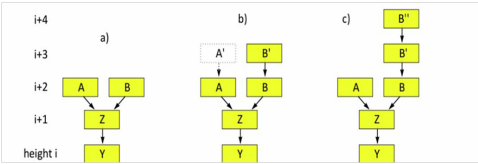

Fig: Resolution of a blockchain

The End