Experiment No: 2

Aim: Writer ad-program to implement Merkle

street showing office cryptographic hash

function in Blockchain. er the blockshoin is a hash-bosed linked ali at A hash tree is also briown as Mexide Tree It is a dreamin which each leaf node is labeled with hash value of data block and each non-leaf node is labeled with the hash value of its child node labels. · Merkle Tree: ()H A Merkle tree is a binary tree formed creator Ralph Merkle. One approach can be to form a host pointerbased linked! list of transactions and store
this complete linked list in a black.

However, when we put this approach into
perspective, it does not seem practical to
store a huge list of hundreads of transactions This is of huge overhead and can reduce the efficiency of the blockchain. Now, this is where the Merkle tree comes into the picture. Merkle tree is a perblack tree doft all the transactions that are included in the block



3 hiro	It allows us tophash of all transactions
	monner: memberskip om a time - e Friched
	momer. Blockchain rannom
-	Hence, the blockchain is a hash-based linked
	list of blocks, where each blocks consists
	of a header and transactions.
Ty ee .	The stransactions vaire arranged and at thee-like
أح	fashion & knowning Merkle trees +
100	a labeled with hash value of data block
200	Merklew Treedostricturen fool-non dos
	value of its child node labels.
-	
	HC) Merkle Root.
pan	- A Mentel tree is a binger tree from
	til settle barron bor 2 restrains the leaf I Non-leaf
	node comportations.
-19+1100	dont o mit ot ad nos donnago anos -
- sket	The mit the doctor to the life both of the last of the
	. Spold pril feil bestril stylemos zitt
	- Honever, who we put this approach in
	pidong made ton 2900 to Tritogo. do
Josephann.	
sulto 9	- This is a bulge loverhood and and reflut
	ethicipacy of the blockethain.
20005	sort sideold att sight si little word
	a p si as at aldred and sign of ni
tout	2004202000 of off () No Hosh value oloold
	ave indisposariotis.



- A blackchain can portentially have thousands of blocks with thousands of transactions in intern each block of therefore is memory space and 10 computing power are two main challenges. It would be apprimate to use as dittle data as possible for verifying transactions, in which can reduce to PU = processing and in inprovide hbettern security Handonthist is exactly-downat merkle thee offerst animal tomaid Merkles treet tonsactions traine groups into pairs. The hosh is computed for each pair and this is stored in the parent + Now the parent nodes are grouped into pairs and their hash is stored in one level up in the tree. This continues till the mot of the tree. The different types of nodes in Merkle mod is stored in tree :-

- Root node! The most of Markle tree is known as the Merkle most and Merkle most and Merkle most is stored in the Leader of the block.
- 2) Leaf node! The leaf note contains the hash value of transaction data. Each transaction in the block has its data hashed and then this hash value is



a shorestoreducin ulterfinaderso sinds shold A al snothosomete to abmosunt this should 3) Non-leaf Node in The moneteaft nodes contain 13 mother hash value of transaction data, of 14+ their are expectoret ochildren luna IT data as possible for verifying tronsporters. by Bitcoln or wees of the south A-256 hash function to thosh their transactions data i continuously tilled the a Merkelala soot tole abolatored so Immote Furtherite and Merkles treelis binary the nature into paint the hash is computed for each pair and strice is stored in the parent the parent nodes are grouped into bardo si dood/ right sofoto Roof node: The root of Merkle tree known as the Merkle stot and Merkle - 70 rahad got at baguta at Leaf rode! The leaf note contains the ash value of stangardon data. Each oh attend stoold att at notionenos 21 sulpu dand sidt made hono