No category Today 7:38 PM

What is your understanding of Blockchain?

Blockchain is a system of recording information in a way that makes it difficult or impossible to change or hack or cheat the system.It is a database that is shared across the difference computer in different places. The copies of the database are same across the network. Once the block has recorded it impossible or difficult to delete or change it. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.

What is the core problem Blockchain trying to solve?

The problem trying to slove is data security and trust by making the ledger public. It mainly decentralized in network. It make the truth on individual and security.. Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.

What are the few features which Blockchain will give you?

CANNOT BE CORRUPTED:-

Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its vaidity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

DECENTRALIZED TECHNOLOGY:-

The network is decentralized meaning it doesn't have arw governing authority or a single person looking after the framework Instead, a group of nodes maintain the network making it decentralized.

ENHANCED SECURITY:-

As it eliminates the need for central authority, no one can

just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

DISTRIBUTED LEDGERS:-

The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

CONSENSUS:-

Every blockchain thrives because of the consensus algorithm, The architecture is cleverly designed and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

FASTER SETTLEMENT:-

Blockchain offers a faster settlement compared to

traditional banking system. This way a user can transfer money relatively faster, which saves a lot of tren in the long run.

What all things does a Block contain?

Each block contains, previous hash value, the current time, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle - the answer to which is unique to each block. New blocks cannot be submitted to the network without the correct answer.

--->previous hash value size depending on hash algorithm we use

--->Magic no value always 0xD9B4BEF94 bytes

--->Block_size number of bytes following up to end of

block4 bytes

--->Block_headerconsists of 6 items 80 bytes

--->Transaction counterpositive integer VI = Var_Int1 - 9 bytes

--->transactionsthe (non empty) list of transactions<Transaction counter>-many transactions

--->present hash value size depending on hash algorithm we use.

How is the verifiability of Blockchain has been attained?

As public ledgers, Bitcoin blockchain and Ethereum require transactions to be visible by default.We all know that blockchain ledger is public and maintaining anonymity is a daunting task. Thus, we consider Bitcoin pseudo-anonymous. By pseudo-anonymity, we mean that a person will be linked to a public Bitcoin address, but no

one will get to know the actual name or address. To explain this in simple words, suppose a person sends a sum of money, then the receiver will get to know that the sender is linked to a bitcoin address but will not know the actual address. Hence, we say that bitcoin or any other alt currencies are not entirely anonymous. There are various reasons for keeping everything hidden, the primary ones include :

Company-specific information

Law-enforcement related issues

Maintaining privacy

To explain this in simple words, I can say that in its system keeps on chaining the address for a given wallet. This discourages the ability to trace payments done to a particular wallet