BLOCKCHAIN

Assignment Day 1

1. What is your understanding of Blockchain?

The words “block” and “chain” in this context, we are actually talking about digital information (the “block”) stored in a public database (the “chain”). It is combination of distributed database and cryptocurrency.

2. What is the core problem Blockchain trying to solve?

a) Currency and Transaction Support

At the moment, sending money to another either domestically or internationally requires the use of a third party, be it your local bank or PayPal account. these intermediaries usually charge hefty fees, and transactions can take an excessive amount of time.

b) Supply Chains and Item Histories

Blockchain technology can help us trace the history of any good or item back to its source in such a way that tampering with it unnoticeably would be impossible.

c) Voting

If Blockchain technology were to be used for voting purposes, there would be no question as to the results’ authenticity and legitimacy, due to the fact that all entries in a decentralized ledger are immutable and irreversible.

d) Government Operations

Government entities have budgets and responsibilities that they need to fulfill in view of their citizens. The increased transparency provided by a decentralized ledger would also help increase overall integrity.

e) Intellectual Property

The theft and illegal sharing of intellectual property such as music, movies, texts, and works of art is quite a big problem today. There are tons of great artists and authors who end up having their content leaked all over the internet and lose out on rightfully earned revenues.

f) Real Estate

There are many issues with the purchase and sale of real estate, mostly related to fraud, transparency, and errors in public records.

3.What are the few features which Blockchain will give you?

a) Cost-effective

As the blockchain is a trusted peer-to-peer network, it removes the need for a central third party. This is one of the major benefits for businesses as it completely removes the costs that are required to pay third parties.

b) Unbreakable

Once a transaction is confirmed, it is stored on the ledger and protected using cryptography. It cannot be changed or deleted without a consensus (the group agreement), which makes the blockchain unbreakable.

c) Simplifying Business to Business

Most businesses use different systems, so it is hard for them to share a database with another business. That's why it can make it very difficult for them. As a blockchain can act as a single shared database for both businesses to work from, sharing data is much easier for them on a blockchain system.

d) Availability

Blockchain is a decentralized peer-to-peer network and there is no central point of failure. Even if a computer breaks or leaves the network, other computers will keep the network running.

e) Faster operations

Let’s use a real-world example:

Imagine that you want to send a payment to someone in another country. Without the help of blockchain technology, you would normally need to pay expensive fees (to the banks) and the transaction may take 3-10 days to be processed.

Using blockchain, this can be done almost instantly and at a much cheaper cost.

f) Trust and transparency

As it is a shared database, everyone can view the full details of the transactions within it. These include the source, date, time and the destination of the transaction.

4.What all things does a Block contain?

Structure of a block

A block is a container data structure. In the Bitcoin world, a block contains more than 500 transactions on average. The average size of a block seems to be 1MB, this enables more transactions to be processed per second.

Block Header

The header contains metadata about a block.

There are three different sets of metadata:

- The previous block hash. Remember that in a blockchain, every block is inherits from the previous block because we use the previous block's hash to create the new block's hash. For every block N, we feed it the hash of the block N-1.

- Mining competition. For a block to be part of the blockchain, it needs to be given a valid hash. This contains the timestamp, the nonce and the difficulty. Mining is another crucial part of the blockchain technology, but it is outside the scope of this article.
- The third part is a merkle tree root. This is a data structure to summarize the transactions in the block. And we will leave it at that for now. More on this later.

Block identifiers

To identify a block, you have a cryptographic hash, a digital signature if you will. This is created by hashing the block header twice with the SHA256 algorithm.

Merkle Trees

The transactions in a block are contained in a structure called a merkle tree or binary hash tree.

5. How is the verifiability of Blockchain has been attained?

Verifiability is achieved by making a track over the hashing key present when the block contain is hashed.
Thus in blockchain each block contains the previous black hash key and the data , when we hash the current block it will result in new or current hash key of the block. Thus by making a track of this current hash key when can able to verify the block even when a error or modify occur to a person in an organisation.