Day 1 Assignment

Q. 1 What is your understanding of blockchain?

- blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".

-If you have been following banking, investing, or cryptocurrency over the last ten years, you may be familiar with “blockchain,” the record-keeping technology behind the Bitcoin network. And there’s a good chance that it only makes so much sense. In trying to learn more about blockchain, you've probably encountered a definition like this: “blockchain is a distributed, decentralized, public ledger."

Q. 2 What is core problem blockchain trying to solve?

-Distributed ledger technologies — collectively known as blockchain — have burst onto the business scene, accompanied by a significant amount of hype.1 They are widely expected to disrupt existing industries and lead to the creation of new types of companies.

-Some of the excitement may indeed be warranted, but only if organizations focus on how these technologies can be used to support their strategy. Without that lens, companies risk making large investments in initiatives that don’t create meaningful value

-.To begin, it’s critical to understand the basic uses and functionalities of blockchains, which tend to get lost in the buzz. So we will provide a quick primer on digital ledgers before discussing how companies should build powerful problem-solving applications that are uniquely configured to their own strategies.

1..The Power of a Ledger

2.About the Research

3.Problems That Blockchain Can Address

Q. 3 What are the few features that blockchain will give you?

#Basic Features of Blockchain Technology

1. Cannot be Corrupted

-There are some exciting blockchain features but among them “Immutability” is undoubtedly one of the key features of blockchain technology. But why is this technology uncorrupted? Let’s start with a connecting blockchain with immutability.

-Immutability means something that can’t be changed or altered.

2. Decentralized Technology

-The network is decentralized meaning it doesn’t have any governing authority or a single person looking after the framework. Rather a group of nodes maintains the network making it decentralized.

3. Enhanced Security

-As it gets rid of the need for central authority, no can just simply change any characteristics of the network for their benefit. Using encryption ensures another layer of security for the system.

4. Distributed Ledgers

-Usually, a public ledger will provide every information about a transaction and the participant. It’s all out in the open, nowhere to hide. Although the case for private or federated blockchain is a bit different. But still, in those cases many people can see what really goes on in the ledger.

5. Consensus

-Every blockchain thrives because of the consensus algorithms. 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.

6. Faster Settlement

-Traditional banking systems are quite slow. Sometimes it can take days to process a transaction after finalizing all settlements. It also can be corrupted quite easily. Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

Q. 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 (source). In Bitcoin Cash ( a hard fork from the Bitcoin blockchain ), the size of a block can go up to 8MB. This enables more transactions to be processed per second.

Anyway, a block is composed of a header and a long list of transactions.

1.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.

2.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. For example, this is a block. I will refer to this block as an example for this article.

The block header hash for this particular block is (right column): 000000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb

We also can see the previous block's hash (right column): 0000000000000000004b1ef0105dc1275b3adfd067aed63a43324929bed64fd7

Remember that we used the second hash to create the first. Every block uses the previous block's hash to construct its own hash. The block hash is a unique identifier. You won't find two blocks with the same hash.

The other way to identify a specific block is the block height. The is the position of the block in the blockchain. Our example's block is in the 500312 position. This means that there are 500311 blocks before this one. Since the creation of the Bitcoin blockchain in 2009, 500312 blocks have been created ( at the time of writing obviously ).

A block height is not unique. Several blocks can compete for the same position in the case of a fork, like Bitcoin Cash for example.

3.Merkle Trees

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

I feel that topics like that are easier to understand with actual examples. So we'll go coding for this. A merkle tree is constructed by recursively hashing pairs of nodes ( in this case, transactions ), until there is only one hash, called the root or merkle root. If we stay in the Bitcoin world, the cryptographic hash algorithm used is SHA256. This is applied twice each time.

An example: We have a block with 4 transactions. For the sake of simplicity, each transaction is a string:

const tA = 'Hello'

const tB = 'How are you?'

const tC = 'This is Thursday'

const tD = 'Happy new Year'

Q. 5 How is the Verifiability of blockchain has been attained?

#verifiability in below applications:

1. Blockchain provides the possibility to design new types of applications and systems that allow their users to store data in a secure and transparent way. In this paper, we design a fully verifiable online electronic voting protocol using a blockchain. Our e-voting protocol, called VYV for Verify-Your-Vote, involves cryptographic primitives based on Elliptic-Curve Cryptography (ECC), pairings and Identity Based Encryption (IBE). It ensures the following privacy and security properties: only eligible voter can vote, authentication of the voter, vote privacy, receipt-freeness, fairness, individual and universal verifiability.

2. Blockchain, the underlying technology that powers cryptocurrencies such as Bitcoin and Ethereum, is gaining so much attention from different industry stakeholders, governments and research communities. Its application is extending beyond cryptocurrencies and has been exploited in different domains such as finance, E-commerce, Internet of Things (IoT), healthcare, and governance. Some key attributes of the technology are decentralization, immutability, security and transparency. This paper aims to describe how permissioned Blockchain can be applied to a specific educational use case — decentralized verification of academic credentials. The proposed Blockchain-based solution, named ‘CredenceLedger’, is a system that stores compact data proofs of digital academic credentials in Blockchain ledger that are easily verifiable for education stakeholders and interested third party organizations.