**Assignment-1**

Date: 06-11-22

1. **What is Mining and explain its significance with respect to bitcoin? How much computation power is required for it?**

**Bitcoin Mining**

* Bitcoin mining is the process of getting hold of the digital asset without actually buying it. From this, one can create new Bitcoins that enter into circulation and also add to the blockchain ledger.
* People compete to earn bitcoin rewards by applying computing power in a process known as 'Proof of Work' (PoW). The process is named such because only participants (miners) who have proven they've dedicated sufficient resources (work) will have a chance at winning the rewards.
* Approximately every 10 minutes, rewards are distributed to a single winning 'miner.'
* Rewards are twofold:

(1) the 'block reward,' which is newly minted bitcoin. The block reward is currently set at 6.25 bitcoins (but will be cut in half from early May 2024, then cut in half again four years later and so on).

(2) the fees associated with all transactions in the current block. End users wishing to make a transaction must attach a fee to the proposed transaction as incentive for miners to include it in the next block.

* Mining Bitcoin is a very technical process and requires huge processing power. Basically, the processing power of the computer will be directly proportional to the rate or mining speed, and thus, profit. So, if a person's computer is slow, it may not produce enough Bitcoins.

**Computation power required**

* To mine Bitcoins, one can use a normal computer that has a CPU, motherboard, RAM, and storage. The only difference and the most important requirement here is the graphics processing unit (GPU) or the video card. A high-performance GPU is an essential aspect if a person wants to mine Bitcoin.
* Bitcoin mining is done using specialised hardware called ASICs that stands for Application-Specific Integrated Circuits. This is to tackle the problems of the computer and upgrade the processing power.
* The requirement of GPU and ASICs could be collectively heavy on a person's pocket. One also needs to have a constant active internet connection for this work.
* The other important aspect is the requirement of electricity for mining machines. It is said that the largest Bitcoin miners were operated in China where the electricity was cheaper as compared to the developed nations.
* A person should be able to bear the cost of running a home-based system for mining Bitcoins. Also, a cooling device would be needed to prevent the system from overheating.
* Bitcoin mining could be a bright opportunity for digital coin makers but it clearly demands adequate infrastructure to work accordingly.

1. **Explain the properties of the blockchain and mention one property which you like the most.**

**Blockchain,** at its most basic level, is a way to store data. Data has been and can be stored in many ways, starting from as simple as writing it in a book to getting a little more modern and technical with storing data in file systems that then kind of went to storing data in databases. I mean, the databases came within multiple types like relational non-relational, etc and then blockchain is another way to store data, which has some very nice **properties**.

**Properties of the blockchain**

* Immutability

Once a block is confirmed, the data recorded to the blockchain cannot be removed or edited. Each block is stacked upon the previous block. The next block must have the preceding blocks has in order to be added to the chain. This assures that the blockchain stays in chronological order, effectively making it tamper-proof.

* Decentralized

The Blockchain ledger is shared among multiple participants. This ensures transparency between participants in the Blockchain network nodes without the need to have a central authority controlling it Decentralised trust: all Blockchains are trusted services, this trust does not only apply to transactions but extends to data, services, processes, identities, business logic, terms of an agreement or physical objects.

It applies to almost anything that can be digitised as a (smart) asset with an intrinsic or related value

Decentralised infrastructure: Blockchain can also be seen as a software design approach that binds together a number of computers that commonly obey the same ‘consensus’ process to release or record information they hold, and where all related interactions are verified by cryptography.

Decentralised database: Blockchain destroys the paradigm of current proprietary databases. A Blockchain is like a place where you store semi-public data in a space. Anyone can verify that you put that information there, because the container has your signature, but only you can securely unlock what is inside the container, because only you have the private keys to that data.

* Timestamped

Blockchains are timestamped by default. This means that, it helps in a decentralized manner. So, that helps again in trying to see, how the data has changed when some record was updated and who updated it. So, these properties are what make blockchain interesting.

Without these properties, blockchain is just like any other place, where you can store data. But these properties are what makes blockchain, a blockchain and the reason it is called blockchain is that, every data point is termed as a block. As you store more and more data, it gets stored as a chain of blocks. That’s why it’s called a blockchain. It came into mainstream with the advent of cryptocurrencies but given the **properties of blockchain** it is, it can definitely be used, apart from cryptocurrencies.

According to me, the most interesting property is the second property, decentralization. In this, no single entity has control. Blockchain needs a group of nodes to be able to serve that work as points where all the data is stored in a decentralized manner. And these nodes work together to make sure that the correct provenance of data is maintained, which means that the correct timeline of data is maintained.