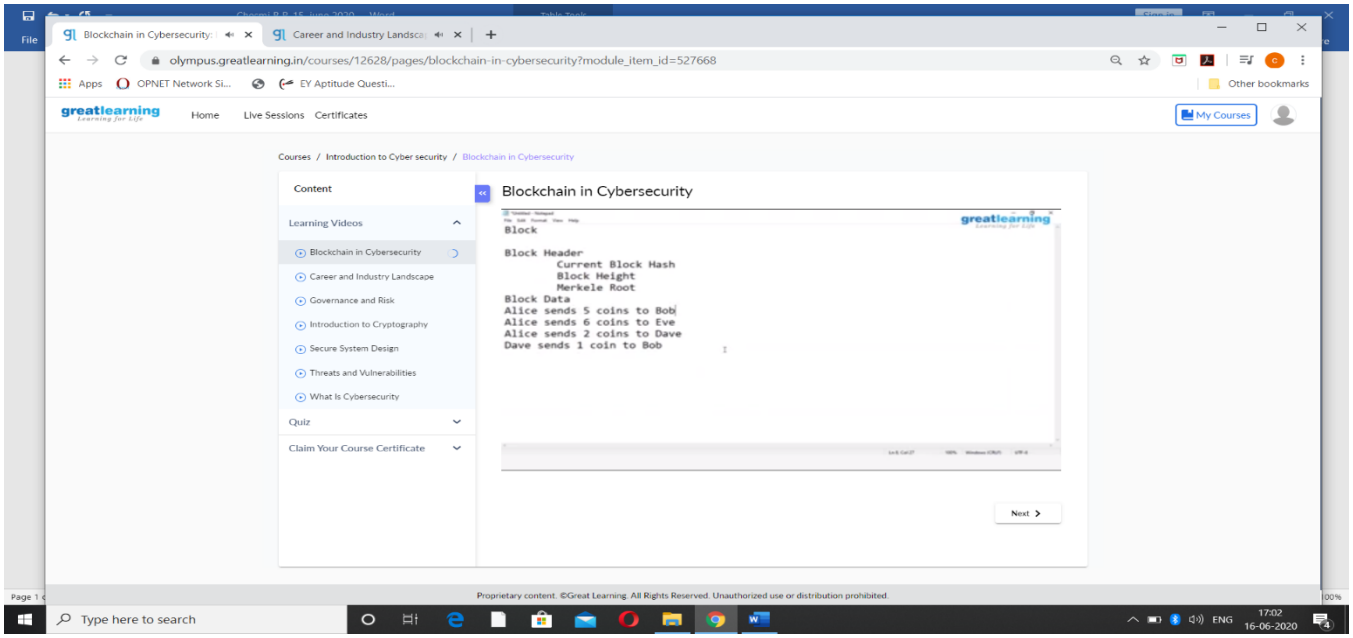
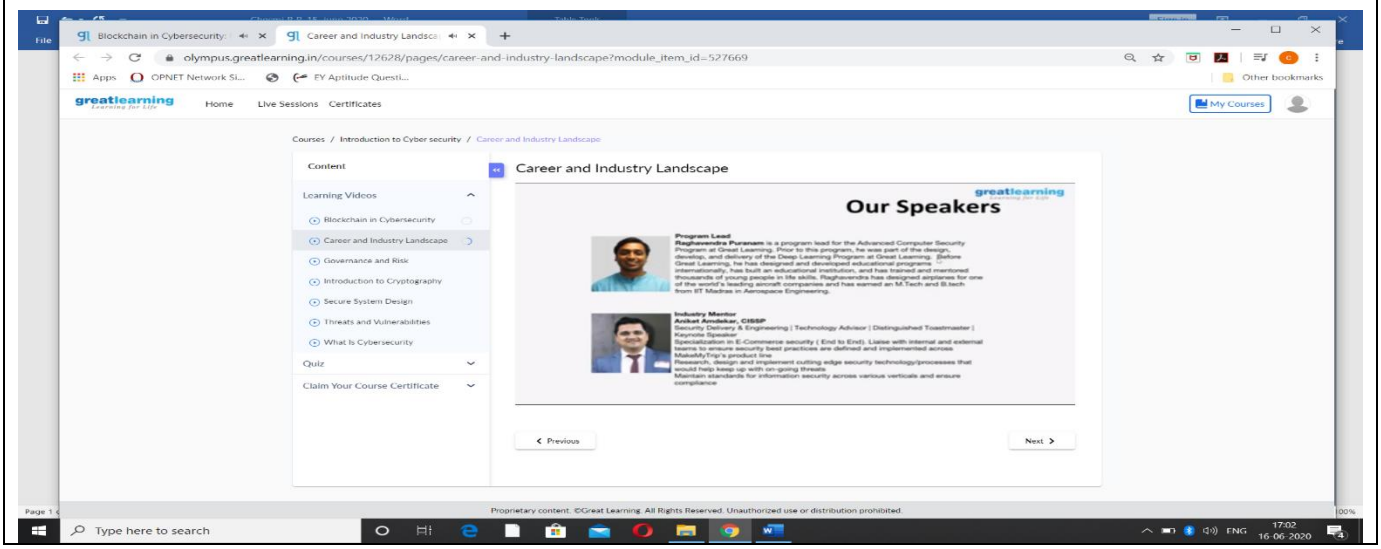
DAILY ASSESSMENT FORMAT

Date:	16/6/2020	Name:	Shilpa S
Course:	Cyber Security	USN:	4AL14EC078
Topic:	Blockchain in cyber security Career and industry landscape	Semester & Section:	8th sem A sec
Github Repository:	Shilpa_online		

FORENOON SESSION DETAILS





REPORT:

The high level of dependency on the internet and technology today has resulted in new revenue streams and business models for organizations, but with this arises new gaps and opportunities for hackers to exploit.

Cybercriminals have become increasingly complex and are attempting to steal valuable data like financial data, health records, personal identifiable information (PII) and intellectual property, and are resorting to highly profitable strategies like disrupting the overall operations of a business via DDoS attacks, or monetizing data access via the utilization of advanced ransomware techniques.

So, will blockchain technology be a cybersecurity help or hindrance? A blockchain is basically a decentralized, digitized, public ledger of all cryptocurrency transactions and uses what is known as the Distributed Ledger Technology. This could potentially help enhance cyber-defense as the platform can prevent fraudulent activities via consensus mechanisms, and detect data tampering depending on its underlying characteristics of operational resilience, data encryption, auditability, transparency and immutability

Blockchain resolves the 'lack of trust' problem between counterparties at a very basic level. Blockchain is a distributed database used in both private and public applications rather than a centralized structure where all the information is stored in few very large databases. The data pertaining to each batch of valid transactions is stored within its own block; every block is connected to the block which is situated in the position before it and grows continuously as new blocks of information are appended.

Owing to their distributed nature, blockchains provide no 'hackable' entrance or a central point of failure and, thereby, provide more security when compared with various present database-driven transactional structures.

Eliminating Human Factor from Authentication

Businesses are able to authenticate devices and users without the need for a password with the help of blockchain technology. This eliminates human intervention from the process of authentication, thereby avoiding it from becoming a potential attack vector.

The utilization of a centralized architecture and simple logins are the big weakness of conventional systems. No matter how much money an organization invests in security, all these efforts go in vain if the employees and customers use passwords that are easy to steal or crack. Blockchain offers strong authentication and resolving single point of attack at the same time.

With the help of blockchain, a security system used in an organization can leverage a distributed public key infrastructure for authenticating devices and users. This security system provides each device with a specific SSL certificate instead of a password. Management of certificate data is carried out on the blockchain and this makes it virtually impossible for attackers to utilize fake certificates.

Decentralized Storage

Blockchain users can maintain their data on their computer in their network. Because of this, they can make sure that the chain won't collapse. For instance, if someone who is not the owner of a component of data (such as an attacker) attempts to tamper with a block, the entire system examines each and every data block to locate the one that differs from the rest. If this type of block is located by the system, it simply excludes the block from the chain, recognizing it as false.

Blockchain is designed in a way that the storage location or central authority doesn't exist. On the network, every user has a role to play in storing some or all the blockchain.

Everyone in the blockchain network is responsible for verifying the data that is shared and/or maintained to ensure existing data can't be removed and false data can't be added.

Traceability

Every transaction added to a private or public blockchain is timestamped and signed digitally. This means that companies can trace back to a particular time period for every transaction and locate the corresponding party on the blockchain through their public address.

This feature relates to non-repudiation: the assurance that someone can't verify their signature's authenticity on a file, or the authorship a transaction that they originated. This blockchain's functionality increases the system's reliability as every transaction is associated cryptographically to a user.

Any new transaction that gets appended to a blockchain results in the transformation of ledger's global state. This implies that with the system's every new iteration, the previous state will be stored resulting in a history log that is completely traceable.

The audit capability of blockchain offers companies with a level of security and transparency over every iteration. From the perspective of cybersecurity, this offers entities with an additional level of reassurance that the data hasn't been tampered with and is authentic.

DDoS

Blockchain transactions can be denied easily if the participating units are impeded from sending transactions. For example, a DDoS attack on a set of entities or an entity can cripple the entire attendant infrastructure and the blockchain organization. These kind of attacks can introduce integrity risks to blockchain.

At present, the difficulty in impeding the attacks due to DDoS comes from the existing Domain Name System. The implementation of blockchain technology would completely decentralize the DNS, distributing the contents to more number of nodes thereby making it almost impossible for cyber-attackers to hack. A system can make sure that it is invulnerable to hackers by using blockchains to safeguard data unless every single node is wiped clean at the same time.

Blockchain technology is here to stay and it will help us protect as companies, individuals, and governments. The innovative blockchain utilization is already becoming a component of other fields beyond cryptocurrencies and is mainly useful to enhance cybersecurity.

Though few of the underlying capabilities of blockchains offer data availability, integrity, and confidentiality, like various other systems, cybersecurity standards and controls must be followed by companies within their technical infrastructure with the help of blockchains to protect them from outside attacks.