**Block chain Day 1 Assignment**

**Question 1 : What is your understanding of block chain**

**Ans :**

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. 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. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).

Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a [hash](http://www.euromoney.com/learning/blockchain-explained/how-blockchain-data-is-stored-and-secured).

This means if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions of the chain.

Blockchains such as [Bitcoin](https://www.euromoney.com/learning/blockchain-explained/the-difference-between-blockchain-and-bitcoin)and Ethereum are constantly and continually growing as blocks are being added to the chain, which significantly adds to the security of the ledger.

You (a "**node**") have a file of transactions on your computer (a **"ledger"**). Two government accountants (let's call them **"miners"**) have the**same file** on theirs (so it’s **"distributed"**). As you make a transaction, your computer sends an e-mail to each accountant to inform them.

Each accountant rushes to be the first to check whether you can afford it (and be paid their salary **"Bitcoins"**). The first to check and validate hits “REPLY ALL”, attaching their logic for verifying the transaction (**"proof of work"**). If the other accountant agrees, everyone updates their file…

This concept is enabled by **"Blockchain"** technology.

**Question 2 : What is the core problem block chain trying to solve?**

**Ans :**

In creating a blockchain, organizations need to define the specific problem they are trying to solve. Then they must determine which transactions or interactions the blockchain should capture and who should have access to which portions. Verification is a key benefit.

The types of problems that blockchains can solve are far-ranging, spanning many industries and contexts. Here we will explore just a few common examples.

**Paying for contributions to intellectual property.** The video game industry offers a useful window into what’s possible when you define a problem that a particular set of stakeholders face — and then design a blockchain to solve the problem. In this case, the stakeholders were the people contributing their creativity and smarts to developing games. And the problem was the cumbersome, archaic way in which royalties and rights were managed across the industry.

Developing a video game typically involves production companies and game-publishing houses (such as Sony Interactive Entertainment, Tencent Games, Microsoft Studios, and Electronic Arts), development companies, video game console makers, computer manufacturers, and mobile phone makers, as well as contractors — writers, voice actors, composers, musicians, and so on.

**Establishing history of ownership.** In addition to addressing problems related to intellectual property and licensing, blockchain is being used to establish origins and ownership. Consider the diamond industry, which has long been subject to corrupt activity. In western and central Africa, for example, rebel groups have used “blood diamonds” to finance armed conflicts against governments. In response, the diamond industry has attempted to create provenance certification programs. The proper tracking of diamonds could bring much-needed transparency to the industry, ensuring that blood diamonds do not support insurgents’ efforts by preventing the gems from entering the supply chain in the first place. However, these efforts haven’t been easy, as paper-based certification systems are prone to fraud and corruption.

**Making supply chains more efficient and transparent.** The ability to track provenance can address another type of problem: reducing the amount of inefficiency and lack of clarity in supply chains. In early 2018, the Danish shipping giant Maersk and IBM announced a joint venture to create a real-time digital ledger for global shipping. The cargo, transport, and shipping industry has long suffered from a lack of transparency with regard to the sourcing and timing of shipments, which public ledgers might be able to solve.

Other companies are developing their own distributed ledgers to cover their entire supply chains. Walmart provides a good exampleHowever, a distributed ledger will extend this advantage by recording the origins of raw materials and products in the supply chain. This will also allow for more transparent consumer labeling and answer questions about sustainability in a more timely and detailed fashion.

**Question 3: What are the few features that block chain will give you?**

**Ans :**

**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. This is one of the blockchain features that help to ensure that the technology will remain as it is – a permanent, unalterable network. But how does it maintain that way?

[Blockchain technology](https://101blockchains.com/ultimate-blockchain-technology-guide/) works slightly different than the typical banking system. Instead of relying on centralized authorities, it ensures the blockchain features through a collection of nodes.

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

## 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.

This is one of the key features of blockchain technology that works perfectly. Let me make it simpler. Blockchain puts us users in a straightforward position. As the system doesn’t require any governing authority, we can directly access it from the web and store our assets there.

You can store anything starting from cryptocurrencies, important documents, contracts or other valuable digital assets. And with the help of blockchain, you’ll have direct control over them using your private key. So, you see the decentralized structure is giving the common people their power and rights back on their assets.

## 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. Well, it’s extremely secure because it offers a special disguise – Cryptography.

Added with decentralization, cryptography lays another layer of protection for users. Cryptography is a rather complex mathematical algorithm that acts as a firewall for attacks.

## 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.

That’s because the ledger on the network is maintained by all other users on the system. This distributed the computational power across the computers to ensure a better outcome.

This is the reason it’s considered one of the blockchain essential features. The result will always be a higher efficient ledger system that can take on the traditional ones.

## 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.

In simple terms, the consensus is a decision-making process for the group of nodes active on the network. Here, the nodes can come to an agreement quickly and relatively faster. When millions of nodes are validating a transaction, a consensus is absolutely necessary for a system to run smoothly. You could think of it as kind of a voting system, where the majority wins, and the minority has to support it.

## 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.

These blockchain important features make life easier for foreign workers. Many people travel to another country in search of a better life and job and leave families behind. However, sending money to their families overseas takes a lot of time and could become fatal in time of need.

**Question 4 : What all things does block chain contains?**

**Ans :**

Blockchain consists of three important concepts: blocks, nodes and miners.

### **1. Blocks**

Every chain consists of multiple blocks and each block has three basic elements:

* The **data** in the block.
* A 32-bit whole number called a **nonce.** The nonce is randomly generated when a block is created, which then generates a block header hash.
* The **hash** is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

### **2. Miners**

Miners create new blocks on the chain through a process called mining.

In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it is as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.

When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

View All Jobs

### **3. Nodes**

One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning.

Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a [unique alphanumeric identification number](https://hbr.org/2017/01/the-truth-about-blockchain) that shows their transactions.

Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scaleability of trust via technology.

**Question 5 : How is the verifiability of block chain has been attained?**

**Ans :**

Most security and privacy research studies on blockchain have been focused along two threads: (1) uncovering some attacks suﬀered by blockchain based systems to date, and (2) putting forward speciﬁc proposals of employing some state of the art countermeasures against a subset of such attacks.However,veryfeweﬀortshavebeenmadetoprovideanin-depthanalysisofthesecurityand privacy properties of blockchainand diﬀerent blockchainimplementation techniques. This survey presents a comprehensive review of the security and privacy of blockchains. We ﬁrst describe the notion of blockchains for online transactions, and discuss the basic and additional security and privacy attributes of blockchains. Then we discuss a set of corresponding security techniques, especially cryptographic solutions, for realizing both basic and additional security goals. We argue that, as blockchain technology continues to attract attentions and to be deployed in various applications, it is critical to gain an in-depth understanding of the security and privacy properties of blockchain and the degree of trust that blockchain may provide. Such understanding may shed light on the root causes of vulnerabilities in current blockchain deployment models and provide foresight and technological innovation on robust defense techniques and countermeasures.

In the context of Bitcoin systems, the blockchain is employed as its secure, private and trusted public archive for all transactions that trade bitcoins on the Bitcoin network. This ensures that all bitcoin transactions are recorded, organized and stored in cryptographically secured blocks, which are chained in a veriﬁable and persistent manner. Blockchain is the pivotal guard in securing bitcoin transactions from many known and hard security, privacy and trust problems, such as double spending, unauthorized disclosure of private transactions, reliance of a trusted central authority, and the untrustworthiness of decentralized computing. The bitcoin way of deploying blockchainhas been the inspiration for many other applications, such as healthcare, logistics, education certiﬁcation, crowd sourcing, secure storage. The blockchain ecosystem is growing rapidly with increasing investment and interests from industry, government and academia.

**Komal Lende** [**Komallende.211@gmail.com**](mailto:Komallende.211@gmail.com)