Assignment-1

Course Code: CSE 319

Course Title: Computer Networks

Submitted to:

Name: Shamim Ahmed

Assistant Professor

Department of CSE

at Bangladesh University of Business and Technology

Submitted by:

Name: Syeda Nowshin Ibnat

ID: 17183103020

Intake: 39, Section: 1

Program: B.Sc. in CSE

Semester: Spring 2021

Date of Submission: 25.05.2021

Problem- 1

a) Blockchain Technology.

Solution: Over the past few years, we have consistently heard the term 'Blockchain technology. Blockchain technology came into inception when Satoshi Nakamoto (an unidentified individual or a group) submitted a paper based on his research to introduce bitcoin as a digital currency. During its early days, blockchain was considered to only be a part of the bitcoin currency. With time, blockchain found its applications apart from bitcoin and entered industries where this technology could make a difference. For us it is imperative to understand what is Blockchain, the technology used, how it works, and how it's becoming vital in the digital world.

What is Blockchain Technology?

To know about blockchain technology at first we need to know about blockchain. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. Sometimes, blockchain referred to as Distributed Ledger Technology(DLT)*, makes the history of any digital asset unalterable and transparent through the use of decentralization and cryptographic hashing.

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger.' Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

*A distributed ledger technology or DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.

A simple analogy for understanding blockchain technology is a Google Doc. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the doc are being recorded in real-time, making changes completely transparent.

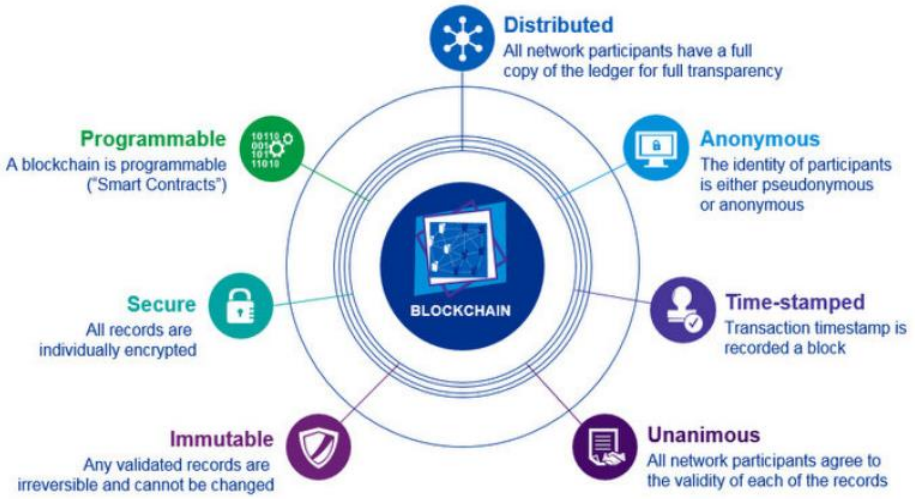


Figure 1: Properties of Distributed Ledger Technology(DLT)

Terms related to Blockchain Technology.

Let's explore the three basic concepts of blockchain technology.

- **Blocks -** Blocks are the components of the chain which store data in blockchain technology. As a block is created, nonce (a 32-bit whole number) generates a cryptographic hash (a 256-bit number). Unless mined, blocks are tied to this nonce and hash.
- **Nodes -** In this decentralized technology, nodes are electronic devices that keep copies of the blockchain.
- **Miners -** Miners create new blocks on the blockchain through a process called mining. To add a block to the chain, miners find a nonce that generates an accepted hash using various software. As each block has its own nonce and hash, along with the previous block's hash, the block's alteration isn't easy. Block manipulation is a complex process as it requires re-mining of all the blocks that follow and is, thus, a safety feature. After successfully mining the block, the change is accepted by all the nodes of the network.

- **Timestamp -** The timestamp is the details of the exact time when the block is created in the blockchain.
- **Transactions -** The transactions refer to the transactional data that has been collected and stored inside the block.
- **Hash -** Hash is the cryptographic hash of the block generated by applying an appropriate hash function, chosen for the blockchain, on the data stored in the block.
- **Previous Hash -** Previous hash is the hash of the last block, which is used to link the block from the last block present on the blockchain.

How does Blockchain Technology work?

In recent years, we may have noticed many businesses around the world integrating Blockchain technology. But how exactly does Blockchain technology work? The advancements of Blockchain are still young and have the potential to be revolutionary in the future; so, let's begin demystifying this technology.

Blockchain is a combination of three leading technologies:

1. Cryptographic keys
2. A peer-to-peer network containing a shared ledger
3. A means of computing, to store the transactions and records of the network

Blockchain can be defined as a shared ledger, allowing thousands of connected computers or servers to maintain a single, secured, and immutable ledger. Blockchain can perform user transactions without involving any third-party intermediaries. In order to perform transactions, all one needs are to have its wallet. A Blockchain wallet is nothing but a program that allows one to spend cryptocurrencies like BTC, ETH, etc. Such wallets are secured by cryptographic methods (public and private keys) so that one can manage and have full control over his transactions.

Now, this is how Blockchain works. Initially, when a user creates a transaction over a Blockchain network, a block will be created, representing that transaction is created. Once a block is create

d, the requested transaction is broadcasted over the peer-to-peer network, consisting of computers, known as nodes, which then validate the transaction.

A verified transaction can involve cryptocurrency, contracts, records, or any other valuable information. Once a transaction is verified, it is combined with other blocks to create a new block of data for the ledger. Here it is important to note that with each new transaction, a secured block is created, which are secured and bound to each other using cryptographic principles. Whenever a new block is created, it is added to the existing Blockchain network confirming that it is secured and immutable.

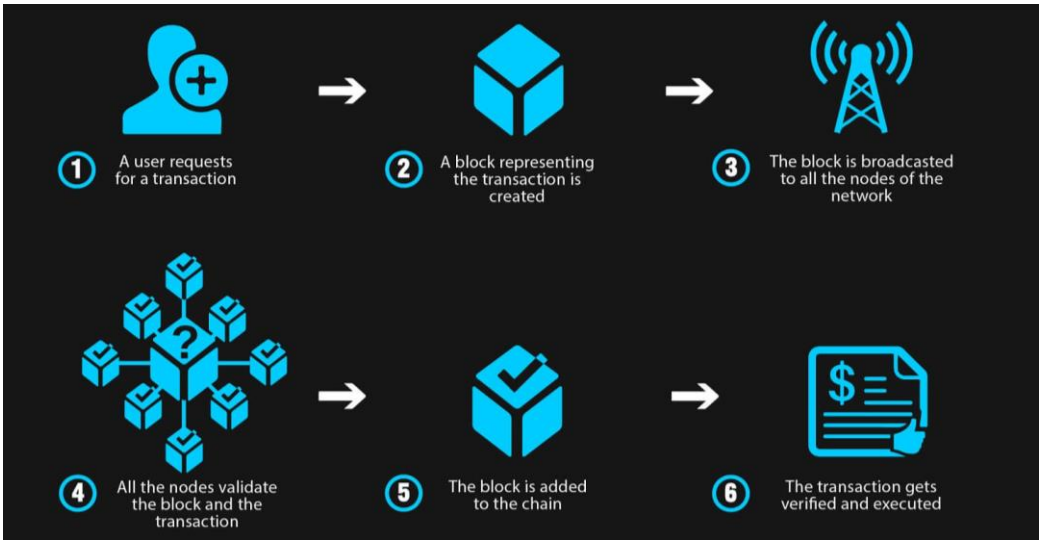


Figure: How does a blockchain work: A Step-by-Step view

Blockchain Architecture.

Let's see the Blockchain architecture by understanding its various components:

What is a Block?

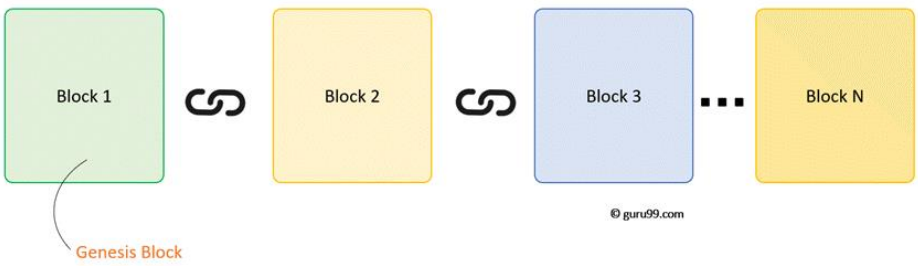


Figure: Blockchain is chain of Blocks that contains Data

A Blockchain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain.

For Example, A Bitcoin Block contains information about the Sender, Receiver, number of bitcoins to be transferred.

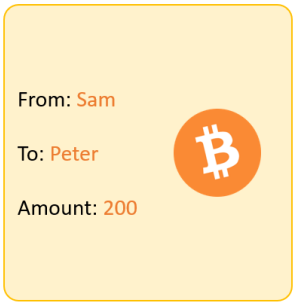


Figure: Bitcoin Block Example.

The first block in the chain is called the **Genesis block**. Each new block in the chain is linked to the previous block.

Understanding SHA256 - Hash

A block also has a hash. A hash can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

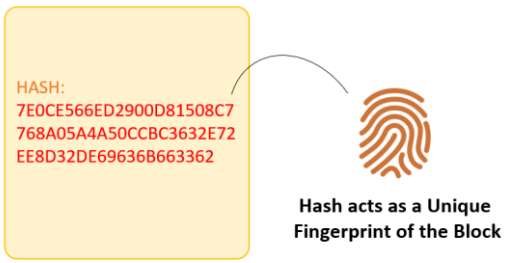


Figure: SHA256 - Hash

Therefore, the hash is very useful when we want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block. Each Block has: Data, Hash, Hash of the previous block.

Considering the following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block.

Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.

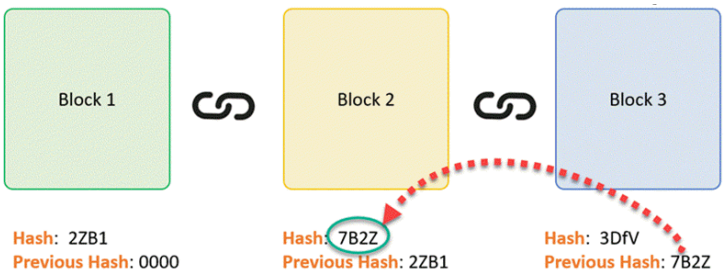
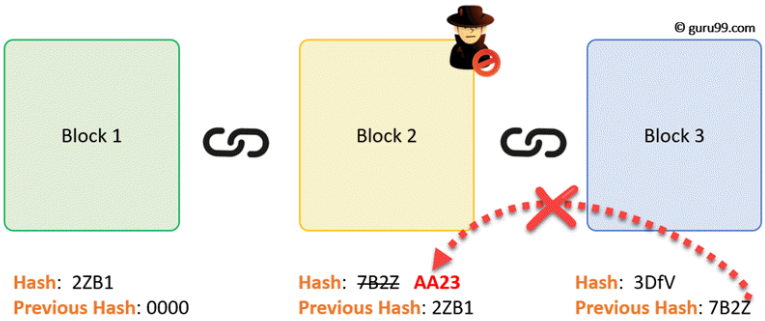


Figure: Hash and block

Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure.

Let's see how it works – Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.



Therefore, changing a single block can quickly make all following blocks invalid.

Consensus Algorithms in Blockchain Technology.

Consensus algorithms in blockchain are what that makes all the blockchain consensus sequences different from one another. Now, we will discuss various consensus algorithms and how they work.

1. **Proof of Work (PoW):**

This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm.

2. **Practical Byzantine Fault Tolerance (PBFT):**

PBFT tries to provide a practical Byzantine state machine replication that can work even when malicious nodes are operating in the system.

3. **Proof of Stake (PoS):**

This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake.

4. **Proof of Burn (PoB):**

With PoB, instead of investing into expensive hardware equipment, validators 'burn' coins by sending them to an address from where they are irretrievable. By committing the coins to an unreachable address, validators earn a privilege to mine on the system based on a random selection process. Thus, burning coins here means that validators have a long-term commitment in exchange for their short-term loss.

5. **Proof of Capacity:**

In the Proof of Capacity consensus, validators are supposed to invest their hard drive space instead of investing in expensive hardware or burning coins.

6. Proof of Elapsed Time:

PoET is one of the fairest consensus algorithms which chooses the next block using fair means only. It is widely used in permissioned Blockchain networks. In this algorithm, every validator on the network gets a fair chance to create their own block.

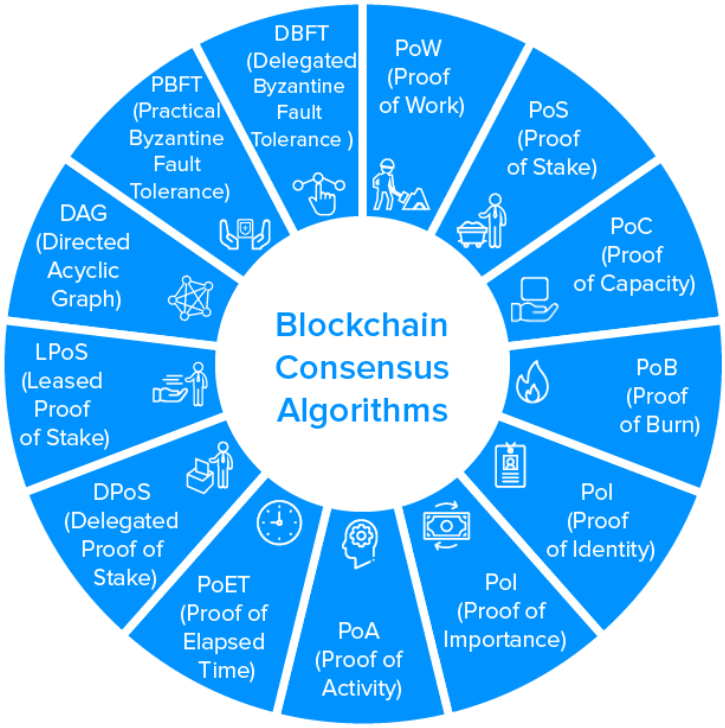


Figure: Different Types of Consensus Algorithms

Some facts on Blockchain Technology.

- Blockchain as we know it today was invented by an individual or a group of people using the pseudonym Satoshi Nakamoto. The first blockchain was conceptualized in 2008.

- The first mention of the world blockchain occurred at BitcoinTalk, the world's largest forum dedicated to Bitcoin.
- There are 5 countries (Switzerland, Gibraltar, Malta, Bermuda, Slovenia) that are perfect for blockchain and crypto startups.
- There are social networks that run on blockchains. One of the best known is Steemit, a blogging network that rewards users for posting or curating content.

- Chinese manufacturer Lenovo introduced a mobile device that features “Z-space”, a blockchain-based payment system. HTC has also launched its own blockchain-focused phone.
- IBM has about 1,500 employees working on more than 500 blockchain projects.
- IBM and the start-up Hu-manity.co launched a blockchain-based app that let patients sell anonymized data to pharmaceutical companies in September 2018.
- Blockchain technology has managed and distributed more than $270B in transactions.

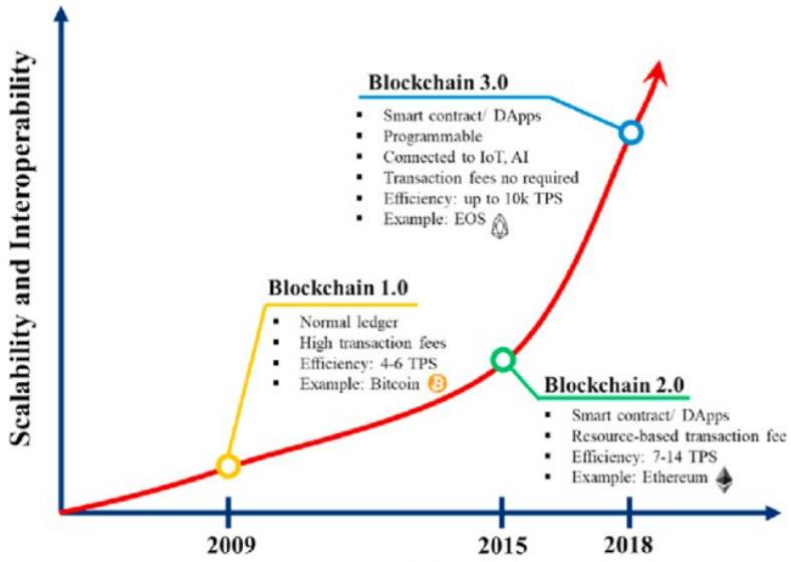


Figure: Timeline of Blockchain Technology

Some statistics on Blockchain Technology.

- By 2022, worldwide spending on blockchain solutions will reach **$11.7 billion**.
- The global blockchain technology market is estimated to accumulate **$20 billion in revenue by 2024**.
- Financial companies can **save up to $12 billion a year** from using blockchain.
- Total spending on integrating blockchain into **healthcare will rise to $5.61 billion by 2025**.
- More than **90% of people engaging in Bitcoin** are men.
- The **FBI owns 1.5%** of the world’s total bitcoins.
- **55% of healthcare applications** will have adopted blockchain for commercial deployment by 2025.

- **60% of CIOs were on the verge** of integrating blockchain into their infrastructure by the end of 2020.
- **More than 20 countries** have adopted or at least researched the concept of a national cryptocurrency.
- **74% of tech-savvy executive teams** say they believe there's a huge business potential in blockchain technology.
- The highest-ever price for a single Bitcoin **by January 2021: $41,940**.

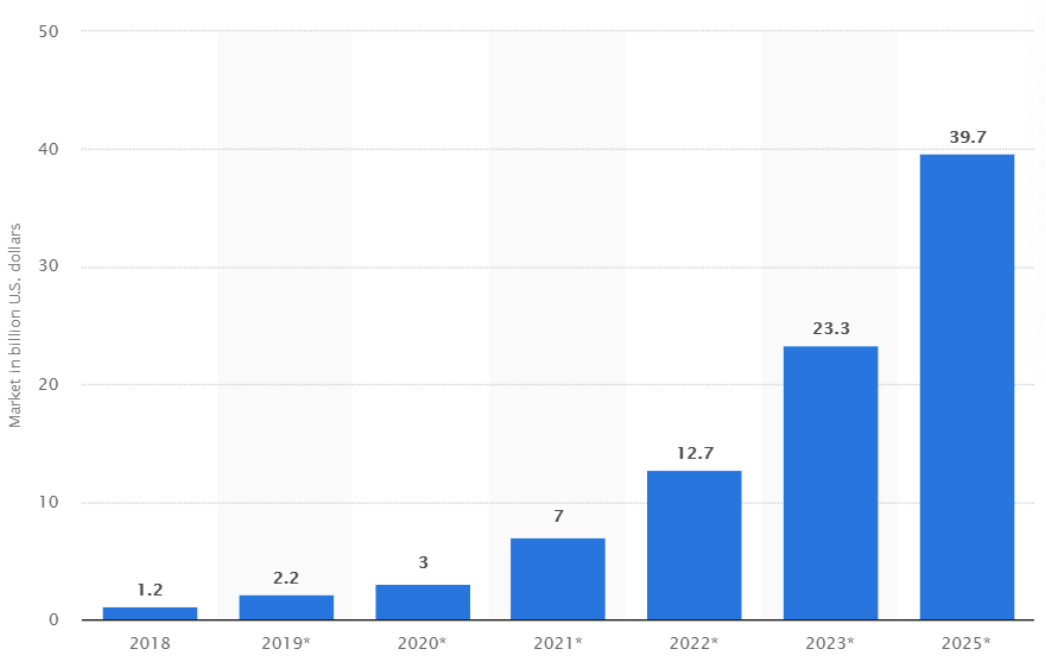


Figure: Size of the blockchain technology market worldwide from 2018 to 2025 (© Statista 2021)

Blockchain Security Issues.

Here are five of the most pressing security issues related to blockchain technology.

1. Vulnerabilities at Blockchain Endpoints

While blockchain has been touted as virtually "unhackable," it's important to remember that most blockchain transactions have endpoints that are far less secure. For example, the result of bitcoin trading or investment may be a large sum of bitcoin being deposited into a "hot wallet," or virtual savings account. These wallet accounts may not be as hacker-proof as the actual blocks within the blockchain. To facilitate blockchain transactions, several third-party vendors may be enlisted.

2. Scalability Issues

Today's blockchains are the largest ever built, and as the technology continues to gain in popularity, blockchains are only going to get bigger. This has caused some experts to be wary, simply because these large-scale blockchains are untested. Common concerns center around the issue that as the blockchain ecosystem grows, additional vulnerabilities may be discovered and exploited, or that the tech infrastructure that supports blockchain will become more prone to simple mistakes.

3. Regulation Issues

Still another blockchain security issue is the absence of clear regulatory standards. Since there's little standardization in the blockchain world, developers have a challenging time benefitting from the mistakes of others.

4. Insufficient Testing

A final issue to address: While blockchain has historically been used for cryptocurrency trades, it's increasingly being used in other fields. The problem is the coding used in non-cryptocurrency applications tends to be untested and highly experimental, meaning that hackers may be able to find and exploit vulnerabilities.

Misconceptions on Blockchain Technology.

- Blockchain and Bitcoin are the same.

  No, Blockchain is a technology, or rather a platform on which bitcoin functions. Bitcoin is just a use case of blockchain, and there are many other blockchain applications in the industry. We can't have Bitcoin without blockchain, but we can have blockchain without Bitcoin.
- Blockchain is a Product.

  Blockchain is not a product but a system with its utility in all the major sectors. Products can be built on the blockchain technology with all the requirements for the particular use case.

- There is Only one Blockchain.

  There are many blockchains; private business blockchains, like Hyperledger Fabric and open-sourced or public ones, like Ethereum, or Bitcoin.

- All Blockchains are Public.

  Private blockchains do exist. These blockchains spark the debate of whether it should be considered a blockchain since the authority is centralized; the various rights are exercised and vested in a central trusted party but is still cryptographically secured.

Figure: Bitcoin and Blockchain are not same

Pros and Cons of Blockchain Technology.

Figure: Pros and Cons of Blockchain Technology.

References:

i. *https://www.allerin.com/blog/blockchain-special*
ii. *https://www.simplilearn.com/tutorials/blockchain-tutorial*
iii. *https://www.ibm.com/topics/what-is-blockchain*
iv. *https://builtin.com/blockchain*
v. *https://diamanteblockchain.com/media/article/how-decentralization-is-the-latest-security-solution-in-the-it-ecosystem/*
vi. *https://www.slideteam.net/blog/top-10-blockchain-technology-powerpoint-templates*
vii. *https://www.upgrad.com/blog/basics-of-blockchain/*
viii. *https://medium.com/stk-token/10-misconceptions-of-blockchain-technology-38890bdaf6ab*
ix. *https://fortunly.com/statistics/blockchain-statistics/*
x. *https://techjury.net/blog/blockchain-statistics/*
xi. *https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/*
xii. *https://www.researchgate.net/publication/343803671_Recent_advances_on_industrial_datadriven_energy_savings_Digital_twins_and_infrastructures/figures*
xiii. *https://101blockchains.com/pros-and-cons-of-blockchain/*
xiv. *https://onlinedegrees.und.edu/blog/5-blockchain-security-issues/*
xv. *https://www.guru99.com/blockchain-tutorial.html#3*

Problem- 2

b) One of Existing Blockchain Project/Research Ideas.

1) Title of the paper:

Securing Smart Cities Using Blockchain Technology.

2) About:

This paper proposes a security framework that integrates the blockchain technology with smart devices to provide a secure communication platform in a smart city.

3) Framework:

1) Physical Layer: Smart city devices are equipped with sensors and actuators which collect and forward data to the upper layer protocols. Some of these devices such as Nest thermostat and Acer Fitbit are vulnerable to security attacks due to lax encryption and access control mechanisms. Further, there is no single standard for smart devices so that the data generated by them can be shared and integrated to provide cross-functionality.

2) Communication Layer: In this layer, smart city networks use different communication mechanisms such as Bluetooth, 6LoWPAN, WiFi, Ethernet, 3G, and 4G to exchange information among different systems. The blockchain protocols need to be integrated with this layer to provide security and privacy of transmitted data. For example, the transaction records can be converted into blocks using telehash which can be broadcast in the network. Protocols like BitTorrent can be used and Ethereum can provide smart contract functionalities.

3) Database Layer: In blockchain, distributed ledger is a type of decentralized database that stores records one after another. Each record in the ledger includes a time stamp and a unique cryptographic signature. The complete transaction history of the ledger is verifiable and auditable by any legitimate user. The key benefits of permission less ledger are that it is censorship resistant and transparent. However, the public ledger has to maintain complex shared records and it consumes more time to reach the consensus compared to the private ledger.

4) Interface Layer: This layer contains numerous smart applications which collaborate with each other to make effective decisions. For example, a smart phone application can provide location information to the smart home system so that it turns on the air conditioner 5 minutes

prior to reach at home. However, the applications should be integrated carefully since vulnerabilities in one application may give intruders access to other dependent processes.

4) Figure:

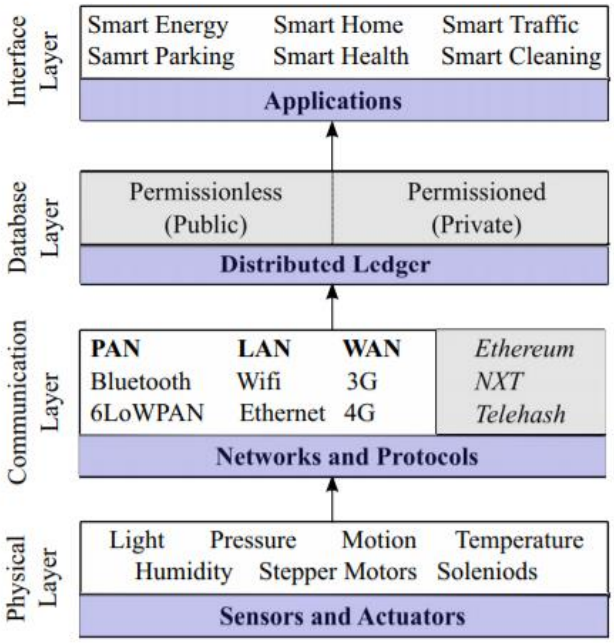


Figure 1: Smart city security framework

5) Outcome:

The main advantage of using blockchain is that it is resilient against many threats. Further, it provides a number of unique features such as improved reliability, better fault tolerance capability, faster and efficient operation, and scalability.

6) **Further scopes for the existing system:**

The future works is aim to design a system level model in order to investigate the interoperability and scalability of different platforms used in a smart city.

References

[1] K. &. M. V. Biswas, "Securing Smart Cities Using Blockchain Technology," *IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International,* pp. 1392-1393, 2016.