Karnatak Law Society's

GOGTE INSTITUTE OF TECHNOLOGY

Udyambag Belagavi -590008

Karnataka, India.

A Course Project Report on

Blockchain

Submitted for the requirements of 5th semester B.E. in CSE

for **"Information and Network Security(18CS652)"**

Submitted by

NAME	USN
1)Nimisha G J	**2GI20CS074**
3)Pratik D	**2GI20CS093**

Under the guidance of

Prof. Amruta Deshpande

Assistant Professor, Dept. of CS

Academic Year 2022-2023 (Even semester)

Karnatak Law Society's
GOGTE INSTITUTE OF TECHNOLOGY
Udyambag Belagavi -590008
Karnataka, India.

Department of Computer Science and Engineering

Certificate

This is to certify that the Course Project work titled **"BlockChain"** carried out by **Nimisha G J, Pratik D** bearing **USNs:2GI20CS074, 2GI20CS093**for **Information and network security(18CS652)** course is submitted in partial fulfilment of the requirements for 5th semester B.E. in **COMPUTER SCIENCE AND ENGINEERING,** Visvesvaraya Technological University, Belagavi. It is certified that all corrections/ suggestions indicated have been incorporated in the report. The course project report has been approved as it satisfies the academic requirements prescribed for the said degree.

Date: Signature of Guide

Place: Belagavi Prof. Amruta Deshpande

Assistant., Prof., Dept. of CSE

KLS Gogte Institute of Technology, Belagavi

Karnatak Law Society's
GOGTE INSTITUTE OF TECHNOLOGY
Udyambag Belagavi -590008

Academic Year 2022-23 (Odd Semester)

Semester: V

Course: Information and Network Security(18CS652)

Rubrics for evaluation of Course Project

Marks allocation: (Page 2)

	Batch No. :					
1.	Seminar/Project Title:	Marks Range	USN/Roll No			
			2GI20CS074	2GI20CS093		
2.	Abstract (PO2)	0-2				
3.	Application of the topic to the course (PO2)	0-3				
4.	Literature survey and its findings (PO2)	0-4				
5.	Methodology, Results and Conclusion (PO1,PO3,PO4)	0-6				
6.	Report and Oral presentation skill (PO9,PO10)	0-5				
	Total	20				

*** 20 marks is converted to 10 marks for CGPA calculation**

1.Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.
2.Problem Analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and Engineering sciences.
3.Design/Development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4.Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5.Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6.The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7.Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8.Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9.Individual and team work: Function effectively as an individual and as a member or leader in diverse teams, and in multidisciplinary settings.
10.Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. Project management and finance: Demonstrate knowledge and understanding of the engineering management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. Life-long learning: Recognize the need for and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological channel

Blockchain:

A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes.Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). The timestamp proves that the transaction data existed when the block was created. Since each block contains information about the previous block, they effectively form a chain (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design

History of BlockChain:

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta.They wanted to implement a system wherein document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block. Under their company Surety, their document certificate hashes have been published in The New York Times every week since 1995.

The first decentralized blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize the rate at which blocks are added to the chain. The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network.

Structure and Design:

A blockchain is a decentralized, distributed, and often public, digital ledger consisting of records called blocks that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks.This allows the participants to verify and audit transactions independently and relatively

inexpensively.A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests.Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double-spending. A blockchain has been described as a value-exchange protocol.A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Logically, a blockchain can be seen as consisting of several layers:

- infrastructure (hardware)
- networking (node discovery, information propagation and verification)
- consensus (proof of work, proof of stake)
- data (blocks, transactions)
- application (smart contracts/decentralized applications, if applicable)

Blocks:

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree.Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the genesis block (Block 0). To assure the integrity of a block and the data contained in it, the block is usually digitally signed.

BlockTime:

The block time is the average time it takes for the network to generate one extra block in the blockchain. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is on average 10 minutes.

Hard fork:

A hard fork is a change to the blockchain protocol that is not backward-compatible and requires all users to upgrade their software in order to continue participating in the network. In a hard fork, the network splits into two separate versions: one that follows the new rules and one that follows the old rules.

Decentralization:

By storing data across its peer-to-peer network, the blockchain eliminates some risks that come with data being held centrally.The decentralized blockchain may use ad hoc message passing and distributed networking.

In a so-called "51% attack" a central entity gains control of more than half of a network and can then manipulate that specific blockchain record at will, allowing double-spending.

Blockchain security methods include the use of public-key cryptography.:5 A public key (a long, random-looking string of numbers) is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.

Finality:

Finality is the level of confidence that the well-formed block recently appended to the blockchain will not be revoked in the future (is "finalized") and thus can be trusted. Most distributed blockchain protocols, whether proof of work or proof of stake, cannot guarantee the finality of a freshly committed block, and instead rely on "probabilistic finality": as the block goes deeper into a blockchain, it is less likely to be altered or reverted by a newly found consensus.

Openness:

Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view. Because all early blockchains were permissionless, controversy has arisen over the blockchain definition.

Permissionless (public) blockchain:

An advantage to an open, permissionless, or public, blockchain network is that guarding against bad actors is not required and no access control is needed.This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer.

Types of Blockchain:

Currently, there are at least four types of blockchain networks — public blockchains, private blockchains, consortium blockchains and hybrid blockchains.

Public blockchains

A public blockchain has absolutely no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol).Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm.

Some of the largest, most known public blockchains are the bitcoin blockchain and the Ethereum blockchain.

Private blockchains

A private blockchain is permissioned.One cannot join it unless invited by the network administrators. Participant and validator access is restricted. To distinguish between open blockchains and other peer-to-peer decentralized database applications that are not open ad-hoc compute clusters, the terminology Distributed Ledger (DLT) is normally used for private blockchains.

Hybrid blockchains

A hybrid blockchain has a combination of centralized and decentralized features.The exact workings of the chain can vary based on which portions of centralization and decentralization are used.

Sidechains

A sidechain is a designation for a blockchain ledger that runs in parallel to a primary blockchain.Entries from the primary blockchain (where said entries typically represent digital assets) can be linked to and from the sidechain; this allows the sidechain to otherwise operate independently of the primary blockchain (e.g., by using an alternate means of record keeping, alternate consensus algorithm, etc.).

Uses of Blockchain:

Cryptocurrencies

Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain.

The criminal enterprise Silk Road, which operated on Tor, utilized cryptocurrency for payments, some of which the US federal government has seized through research on the blockchain and forfeiture.

Governments have mixed policies on the legality of their citizens or banks owning cryptocurrencies. China implements blockchain technology in several industries including a national digital currency which launched in 2020.To strengthen their respective currencies, Western governments including the European Union and the United States have initiated similar projects.

Games

Blockchain technology, such as cryptocurrencies and non-fungible tokens (NFTs), has been used in video games for monetization. Many live-service games offer in-game customization options, such as character skins or other in-game items, which the players can earn and trade with other players using in-game currency. Some games also allow for trading of virtual items using real-world currency, but this may be illegal in some countries where video games are seen as akin to gambling, and has led to gray market issues such as skin gambling, and thus publishers typically have shied away from allowing players to earn real-world funds from games.Blockchain games typically allow players to trade these in-game items for cryptocurrency, which can then be exchanged for money.

The first known game to use blockchain technologies was CryptoKitties, launched in November 2017, where the player would purchase NFTs with Ethereum cryptocurrency, each NFT consisting of a virtual pet that the player could breed with others to create offspring with combined traits as new NFTs. The game made headlines in December 2017 when one virtual pet sold for more than US$100,000. CryptoKitties also illustrated scalability problems for games on Ethereum when it created significant congestion on the Ethereum network in early 2018 with approximately 30% of all Ethereum transactions[clarification needed] being for the game.

Other uses

Blockchain technology can be used to create a permanent, public, transparent ledger system for compiling data on sales, tracking digital use and payments to content creators, such as

wireless users or musicians. The Gartner 2019 CIO Survey reported 2% of higher education respondents had launched blockchain projects and another 18% were planning academic projects in the next 24 months. In 2017, IBM partnered with ASCAP and PRS for Music to adopt blockchain technology in music distribution. Imogen Heap's Mycelia service has also been proposed as a blockchain-based alternative "that gives artists more control over how their songs and associated data circulate among fans and other musicians."

New distribution methods are available for the insurance industry such as peer-to-peer insurance, parametric insurance and microinsurance following the adoption of blockchain. The sharing economy and IoT are also set to benefit from blockchains because they involve many collaborating peers.The use of blockchain in libraries is being studied with a grant from the U.S. Institute of Museum and Library Services.

Energy consumption concerns:

Some cryptocurrencies use blockchain mining — the peer-to-peer computer computations by which transactions are validated and verified. This requires a large amount of energy. In June 2018, the Bank for International Settlements criticized the use of public proof-of-work blockchains for their high energy consumption.

Early concern over the high energy consumption was a factor in later blockchains such as Cardano (2017), Solana (2020) and Polkadot (2020) adopting the less energy-intensive proof-of-stake model. Researchers have estimated that Bitcoin consumes 100,000 times as much energy as proof-of-stake networks.

In 2021, a study by Cambridge University determined that Bitcoin (at 121 terawatt-hours per year) used more electricity than Argentina (at 121TWh) and the Netherlands (109TWh).According to Digiconomist, one bitcoin transaction required 708 kilowatt-hours of electrical energy, the amount an average U.S. household consumed in 24 days.

In February 2021, U.S. Treasury secretary Janet Yellen called Bitcoin "an extremely inefficient way to conduct transactions", saying "the amount of energy consumed in processing those transactions is staggering".[154] In March 2021, Bill Gates stated that "Bitcoin uses more electricity per transaction than any other method known to mankind", adding "It's not a great climate thing."

Nicholas Weaver, of the International Computer Science Institute at the University of California, Berkeley, examined blockchain's online security, and the energy efficiency of proof-of-work public blockchains, and in both cases found it grossly inadequate. The 31TWh-45TWh of electricity used for bitcoin in 2018 produced 17-23 million tonnes of CO2. By 2022,

the University of Cambridge and Digiconomist estimated that the two largest proof-of-work blockchains, Bitcoin and Ethereum, together used twice as much electricity in one year as the whole of Sweden, leading to the release of up to 120 million tonnes of CO2 each year.

Simple illustration of blocks in blockchain:

Code:

```
import hashlib

class Blockchain_Handson:

    def __init__(self, previous_block_hash, transaction_list):

        self.previous_block_hash = previous_block_hash
        self.transaction_list = transaction_list

        self.block_data = f"{' - '.join(transaction_list)} - {previous_block_hash}"
        self.block_hash = hashlib.sha256(self.block_data.encode()).hexdigest()

t1 = "Lenevo"
t2 = "Samsung"

block1 = Blockchain_Handson('firstblock', [t1, t2])

print(f"Block 1 data: {block1.block_data}")
print(f"Block 1 hash: {block1.block_hash}")
```

Output:

```
Block 1 data: Lenevo - Samsung - firstblock
Block 1 hash: d268d54002ad13825285394b07898bb0d897c9c3ec1dc79fd014b7d2070e7577
```

Conclusion:

From this experiment we can conclude that the blockchain technology is very secure and it is very hard to crack or change the information without anyone noticing it,but it consumes more energy and very hard to maintain and is not environmental friendly

Reference:

- https://en.wikipedia.org/wiki/Blockchain
- James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson, 2013.
- Andrew S Tanenbaum, Computer Networks, fifth edition, Pearson