Visvesvaraya Technological University,
Belgaum, Karnataka

Independent study Report
on

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY AND APPLICATIONS

Submitted in partial fulfillment of the requirement for the award of the degree of

Bachelor of Engineering in
in
Computer Science and Engineering

Submittted by

2SD16CS087 shravya k

Under the Guidance of
Dr. Shrihari M Joshi

Department of Computer Science and Engineering
S.D.M. College of Engineering and Technology
Dharwad, Karnataka, India

Academic Year 2019–2020

S.D.M. College of Engineering and Technology,
Dharwad–580002

CERTIFICATE

This is to certify that the project titled **INTODUCTION TO BLOCKCHAIN TECHNOLOGY AND APPLICATIONS** is a bona fide work carried out by **Shravya K (2SD16CS087)** submitted in partial fulfillment of the requirements for the award of the degree of **Bachelor of Engineering** in **Computer Science and Engineering** of **S.D.M. College of Engineering and Technology, Dharwad, Karnataka** (An autonomous institution affiliated to Visvesvaraya Technological University, Belgaum, Karnataka), during the year 2019–2020. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the department library. The project has been approved, as it satisfies the academic requirements in respect of project report prescribed for the said degree.

Dr. Shrihari M Joshi	**Dr. U. P. Kulkarni**
Project Guide	**Head of Department**

External Viva

Name of Examiners	Signature with Date
1)	
2)	

DECLARATION

We hereby declare that the dissertation work titled **INTODUCTION TO BLOCKCHAIN TECHNOLOGY AND APPLICATIONS**, has been carried out under the guidance of **Dr. Shrihari M Joshi, Professor, Department of Computer Science and Engineering, S.D.M. College of Engineering and Technology, Dharwad**, in partial fulfillment of the degree of **Bachelor of Engineering in Computer Science and Engineering** from **Visvesvaraya Technological University, Belgaum, Karnataka**, during the academic year 2019–2020.

I also declare that I have not submitted this dissertation to any other university for the award of any other degree.

Place: Dharwad

Date:

Name of Student	Signature with Date
Shravya K (2SD16CS087)	

ACKNOWLEDGEMENT

I consider it a privilege to express my sincere gratitude and respect to all those who guided and inspired us throughout this study.

I express my heartfelt thanks to our guide **Dr. Shrihari M Joshi**, for his valuable suggestions and guidance during the course of this study. The successful completion of this study owes to his coordination and streamlining of the study progress.

Abstract

Blockchain is an emerging technology platform for developing decentralized applications and data storage, over and beyond its role as the technology underlying the cryptocurrencies. The basic tenet of this platform is that it allows one to create a distributed and replicated ledger of events, transactions, and data generated through various IT processes with strong cryptographic guarantees of tamper resistance, immutability, and verifiability. Public blockchain platforms allow us to guarantee these properties with overwhelming probabilities even when untrusted users are participants of distributed applications with ability to transact on the platform. Even though, blockchain technology has become popularly known because of its use in the implementation of Cryptocurrencies such as BitCoin, Ethereum, etc., the technology itself holds much more promise in various areas such as time stamping, logging of critical events in a system, recording of transactions, trustworthy e-governance etc. Many researchers are working on many such use cases such as decentralized public key infrastructure, self-sovereign identity management, registry maintenance, health record management, decentralized authentication, decentralized DNS, etc. Also, corporations such as IBM and Microsoft are developing their own applications in diverse fields such as the Internet of Things (IoT), etc., even enabling blockchain platforms on the cloud

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 Blockchain Technology

At its most basic level, blockchain is literally just a chain of blocks. When we say the words "block" and "chain" in this context, we are actually talking about digital information (the "block") stored in a public database (the "chain") as shown in figure1. A blockchain is a growing list of records, called blocks, that are linked using cryptography. Blockchain is a distributed, decentralized, public ledger. Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activities and therefore cybersecurity concerns as a whole. Attractive properties of Blockchain are log of data with digital signature, Immutable (once written – cryptographically hard to remove from the log), Cryptographically secure – privacy preserving, Cryptographically secure – privacy preserving. "Blocks" are made up of digital pieces of information.

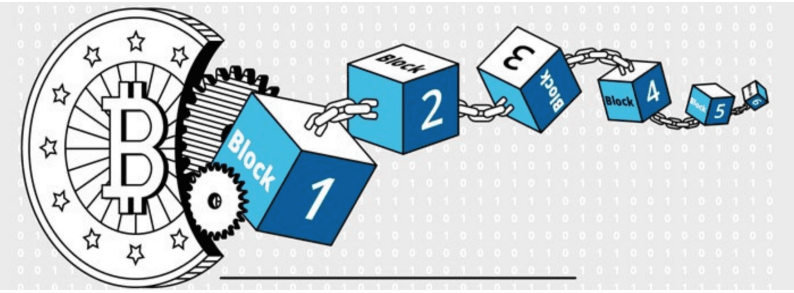


Figure 1: Blockchain

These informations contains 3 things:

1. Blocks store information about transactions like the date, time, and amount of your most recent purchases

2. Blocks store information about who is participating in transactions. Instead of using your actual name, your purchase is recorded without any identifying information using a unique “digital signature,” sort of like a username.

3. Blocks store information that distinguishes them from other blocks.Each block stores a unique code called a “hash” that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms.Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network as nodes. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added. Each computer in the blockchain network has its own copy of the blockchain, which means that there are millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network. This is what is meant by blockchain being a "distributed" ledger.

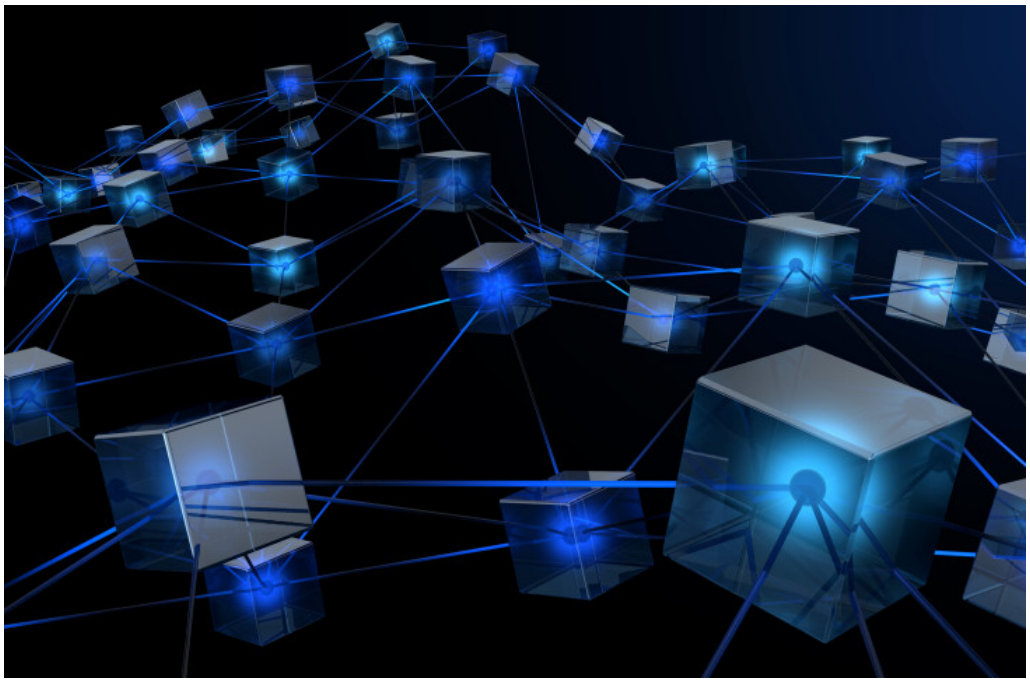


Figure 2: blockchain with million blocks

1.2 Applications

Blockchain technology can be integrated into multiple areas. The primary use of blockchains today is as a distributed ledger for cryptocurrencies, most notably bitcoin.Businesses have been thus far reluctant to place blockchain at the core of the business structure. 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.

1.2.1 Banking

Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you likely will have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of the time or day of the week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if banks are trading internationally), meaning that the money and shares are frozen for that time.

1.2.2 Cryptocurrency

Blockchain forms the bedrock for cryptocurrencies like Bitcoin.Under the central authority system, a user's data and currency are technically at the whim of their bank or government. If a user's bank collapses or they live in a country with an unstable government, the value of their currency may be at risk.By spreading its operations across a network of computers, blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also eliminates many of the processing and transaction fees. It also gives those in countries with unstable currencies a more stable currency with more applications and a wider network of individuals and institutions they can do business with, both domestically and internationally (at least, this is the goal.)

1.2.3 Healthcare

Health care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy

1.2.4 Smart Contracts

A smart contract is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a contract agreement. Smart contracts operate under a set of conditions that users agree to. When those conditions are met, the terms of the agreement are automatically carried out.

1.2.5 Supply Chain

Suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of their products, along with health and ethics labels like "Organic," "Local," and "Fair Trade."

1.2.6 Voting

Each vote would be stored as a block on the blockchain, making them nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and provide officials with instant results.

Chapter 2

Existing technology And Blockchain

2.1 Real Life Problems with Current Systems

There are many flaws in the current systems and technology for handling the transactions. Cyber crime is rising issue nowadays. Mostly people trust a third party organizations to do their transactions and may get cheated knowingly or unknowingly. Its very important to secure your data and keep track of your cyber activities to avoid theft.

2.1.1 Bank Frauds

Scenario 1: You find a check was used to pay someone but you never wrote the check either someone forged your check and/or signature or You did sign a check for x amount, but the amount field was modified. Now, how do you prove to the bank that an extra 0 was not there in your signing time?

Scenario 2: The monthly statement says that you did a transaction but you did not recall, or the amount of a transaction is different from what you had done. Either someone got your password, and possibly redirected OTP to another SIM (SIM Fraud) or Bank employees themselves might have done something. How do you argue to the bank? (Non-repudiation). How do you argue that the amount was modified? (Integrity).

2.1.2 Land Records

You buy a piece of land. Someone else claims to own the land but the one who sold you the land showed you paper work. Land registry office earlier said that the owner was rightful.

Now they say that they made a mistake – it was owned by the other person. You already paid for the land – to the first person. First person goes missing. How does any one prove who changed the land record?

2.1.3 Supply chain

Your buy ice cream for your restaurant from supplier B. Supplier B actually transports ice cream made in Company C's factory. Upon delivery, you have been finding that your ice cream is already melted. Who is responsible?
case 1: Supplier C says it's supplier B's fault as when picked up – ice cream was frozen.
case 2: Supplier B says that when received, the temperature was too high, so C must have stored it or made it wrong
To find the truth you put temperature sensors in B's truck and storage, C's factory and storage, and sensor data is digitally signed by the entity where the sensor is placed and put in a log. You check the log – but B and C both have hacked the log and deleted some entries. What to do?

2.2 Trust Model

Cyber Security is all about who you trust. Where is your trust anchor? Hardware, to not leak your cryptographic keys. Operating system, to not peek into your computation memory. Application, to not be control hijacked or attack other applications. Manufacturer, to not mess up your process memory.

2.3 Blockchain Security

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Let's say a hacker attempts to edit your transaction from a website so that you actually

have to pay for your purchase twice. As soon as they edit the amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on. In order to change a single block, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network.

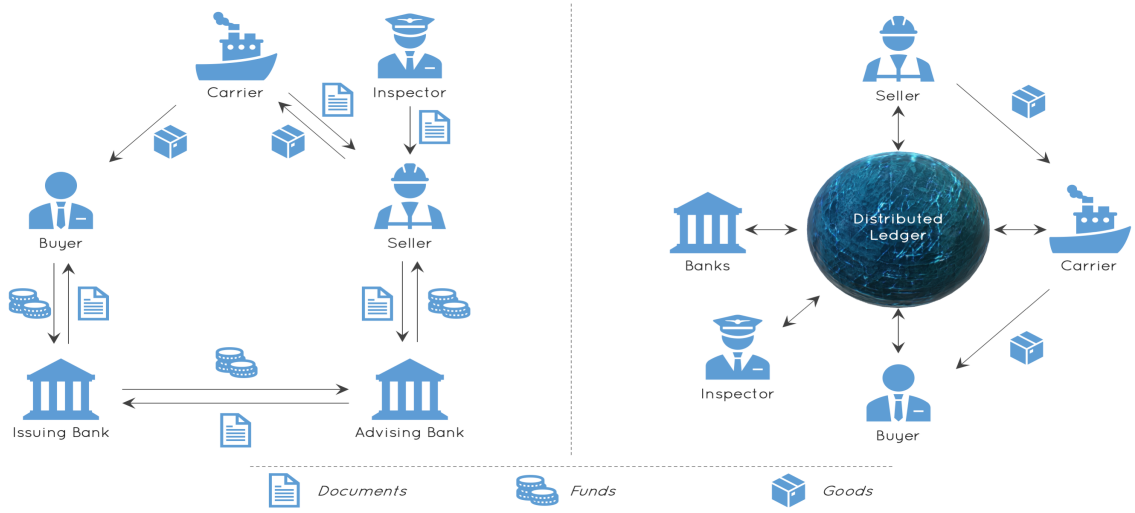


Figure 3: current vs. blockchain

Chapter 3

Algorithms and Implementations

3.1 Basics of Cryptography

Some basic terminologies of cryptography are, **PlainText:** The message, **Encryption:** Encoding of message, **Ciphertext:** Encrypted message, **Decryption:** decoding of ciphertext, **Cipher:** A method of encryption and decryption **Key:** Used to control encryption and decryption.

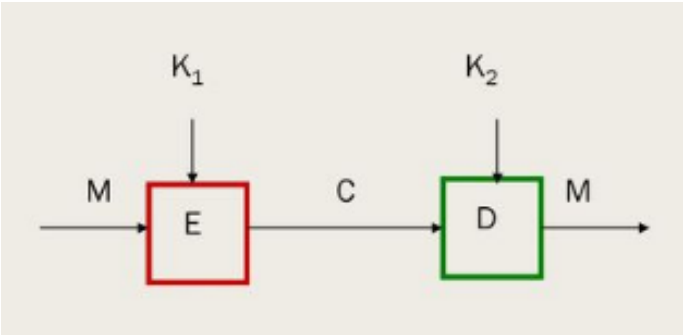


Figure 4: Key based encryption/decryption

Symmetric case: both keys are the same or derivable from each other. K1 = K2.
Asymmetric case: keys are different and not derivable from each other. K1 != K2.

3.1.1 Hashing

Hash function takes an arbitrary length string as input produces a fixed-size output (e.g 256 bits). Attractive properties are easy to compute and impossible to reverse. Some of the important security properties hash functions tries to achieve are:

- collision-resistant
- Hides the original String

- Almost impossible to get the original string from the output
- puzzle-friendly

3.1.2 Merkle Tree

Merkle tree or hash tree is a tree in which every leaf node is labelled with the cryptographic hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

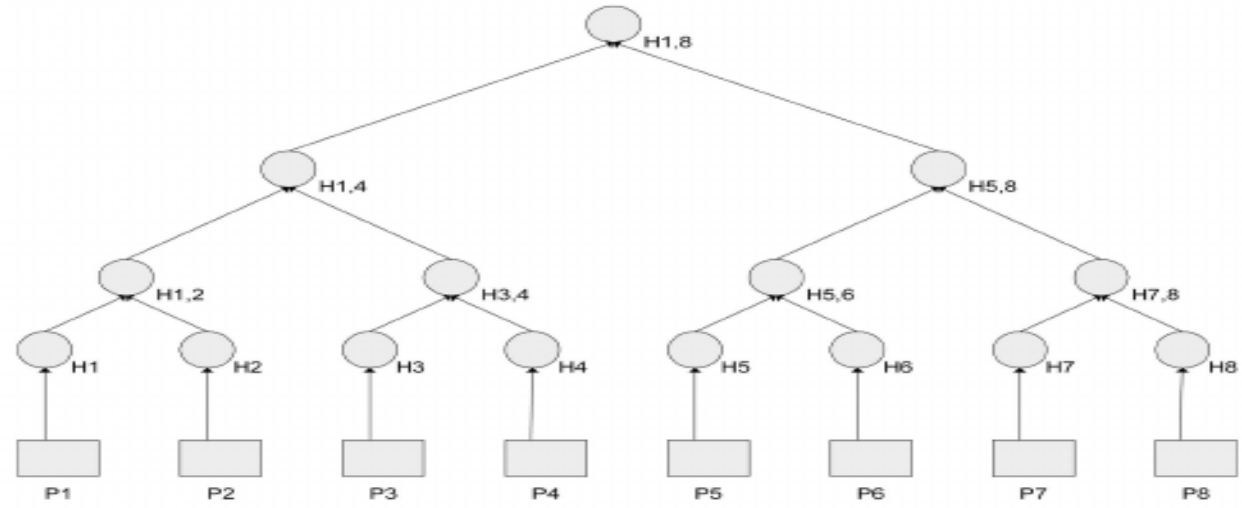


Figure 5: Mercle Tree

3.2 Ledger

A ledger is the principal book or computer file for recording and totaling economic transactions measured in terms of a monetary unit of account by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.A transaction is valid if sender's balance is greater or equal to amount being sent to receiver and a ledger is valid if all transactions in it are valid that is, every sender has the appropriate balance to conduct every transaction. blockchain is a ledger of transactions that is verifiable and permanent.

3.2.1 Centralization vs. decentralization ledger

Centralized Ledger: collection of transactions that are managed by a solitary player.The bank controls the contents, that is, which transactions get posted and the credits and debits to the ledger. [This means that the centralized ledger holder controls the contents of the ledger.]With a centralized ledger, you can't control when the ledger holder, the bank, decides to modify the ledger. The ledger holder can take money because you have an implicit or explicit understanding. Your agreement with your bank allows them to levy charges like fees and interest. What if the ledger holder isn't acting honorably? The consent is out of your hands because you signed a client agreement with the bank when you opened the account and this presents a serious risk if the ledger holder has malicious intent. For example, if the ledger holder goes out of business, you have little or no recourse.

decentralized Ledger: decentralized ledgers no single party has control, but roles can be assigned. There's no central location for the ledger and that's the peer to peer methodology behind Blockchain.There are several compelling benefits to a decentralized ledger. It's open and transparent. Every copy contains every transaction ever recorded. It maintains secure data with practically zero risk of tampering. The data remains intact and free of corruption because there are multiple copies held in multiple nodes. The decentralized ledger can be distributed just to trusted parties. On the other hand, there are a few drawbacks to the decentralized ledger. The time it takes to update the ledger can be problematic. For transactions that require real-time updating, the decentralized ledger may not be the solution. Because there are environments where real-time transactions drive prices, like in stock markets. Bitcoin updates approximately every 10 minutes. If the decentralized ledger is open to the public, the trust relationship has to be implied.

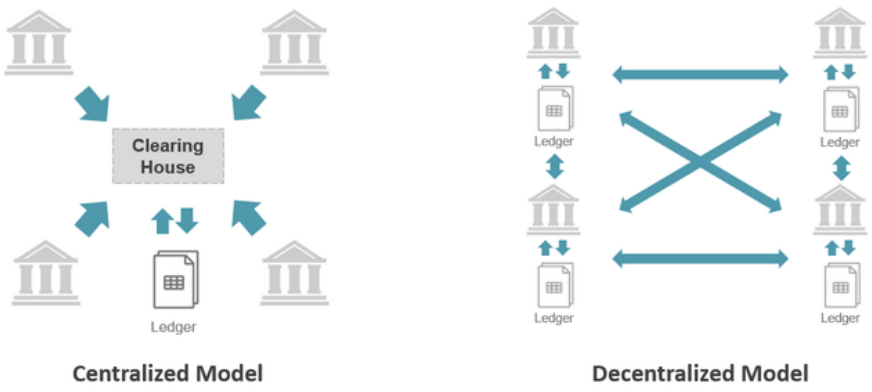


Figure 6: Centralized vs. Decentralized

3.3 Evolution of Blockchain

1st generation: Store and transfer of value (e.g. Bitcoin, Ripple,Dash).

2nd generation: Programmable via smart contracts (E.g. Ethereum).

3rd generation: Enterprise blockchains (E.g. Hyperledger, R3 Corda Ethereum Quorum).

Next generation: Highly scalable with high concurrency.

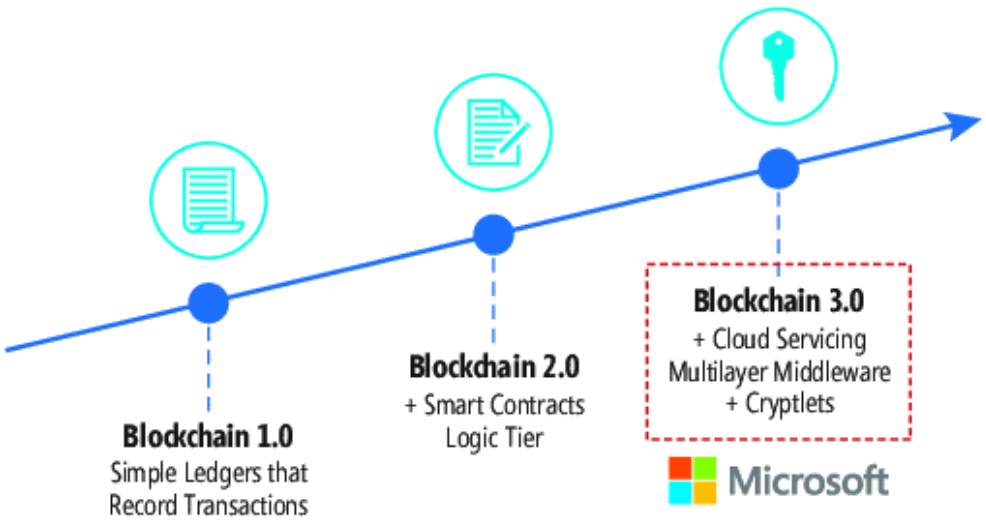


Figure 7: Evolution of blockchain

3.4 Consensus Algorithm

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain. The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.Various consensus algorithms:

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. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block.

Figure 8: Proof of Work

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

   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. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly. In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

Figure 9: Proof of Stake

3. **Proof of Burn (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.Depending on how the PoB is implemented, miners may burn the native currency of the Blockchain application or the currency of an alternative chain, such as bitcoin. The more coins they burn, the better are their chances of being selected to mine the next block.

Figure 10: Proof of Burn

4. **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 permissionned Blockchain networks. In this algorithm, every validator on the network gets a fair chance to create their own block. All the nodes do so by waiting for random amount of time, adding a proof of their wait in the block. The created blocks are broadcasted to the network for others consideration. The winner is the validator which has least timer value in the proof part. The block from the winning validator node gets appended to the Blockchain. There are additional checks in the algorithm to stop nodes from always winning the election, stop nodes from generating a lowest timer value.

Figure 11: Proof of Elapsed Time

3.5 Mechanics of Bitcoin

Bitcoin is a decentralized peer-to-peer virtual, or crypto, currency system. There is no central institution like a bank to control the system. But it has very strict rules that are controlled by cryptographic functions.

We use Asymmetric algorithms, to generate a pair of keys — public and private. Once a message is encrypted using a public key, it can only be decrypted using the corresponding private key and vice versa.

We achieve many things such as Non-repudiation and onfidentiality.Bitcoin also incorporates hashing. Hashing is used to check the integrity of information. When hashing a value, you obtain a unique string. If even a minor change is made to the original value, the hash will change completely. A Bitcoin address is a hashed format of a public key. You can safely publish your public key to the world and keep the private key secret.

Figure 12: Bitcoin

3.6 Ethereum

Ethereum is a blockchain that allows you to run programs in its trusted environment. Contrasts with the Bitcoin blockchain, which only allows you to manage cryptocurrency. Ethereum has a virtual machine – Ethereum Virtual Machine (EVM). The EVM allows code to be verified and executed on the blockchain, providing guarantees it will be run the same way on everyone's machine. This code is contained in "smart contracts". Ethereum maintains the state of the EVM on the blockchain. All nodes process smart contracts to verify the integrity of the contracts and their outputs.

Smart Contract: A smart contract is code that runs on the EVM. Smart contracts can accept and store ether, data, or a combination of both. Using the logic programmed into the contract, it can distribute that ether to other accounts or even other smart contracts.

Figure 13: Ethereum

3.6.1 Ethereum Design Principles

1. **Sandwich Complexity Model:** Complexity is handled by high-level-language compilers, argument serialization and deserialization scripts, storage data structure models, the leveldb storage interface and the wire protocol.

2. **Freedom (inspired by net neutrality):** users should not be restricted in what they use the Ethereum protocol for, and we should not attempt to preferentially favor or disfavor certain kinds of Ethereum contracts or transactions based on the nature of their purpose.

3. **Generalization:** protocol features and opcodes in Ethereum should embody maximally low-level concepts, so that they can be combined in arbitrary ways including ways that may not seem useful today but which may become useful later.

4. **Low in high level features:** a corollary to generalization, we often refuse to build in even very common high-level use cases as intrinsic parts of the protocol, with the understanding that if people really want to do it they can always create a subprotocol (eg. ether-backed subcurrency, bitcoin/litecoin/dogecoin sidechain, etc) inside of a contract.

3.7 Corda

Corda has no unnecessary global sharing of data: only those parties with a legitimate need to know can see the data within an agreement. Corda choreographs workflow between firms without a central controller. Corda achieves consensus between firms at the

level of individual deals, not the level of the system. Corda's design directly enables regulatory and supervisory observer nodes. Corda transactions are validated by parties to the transaction rather than a broader pool of unrelated validators. Corda supports a variety of consensus mechanisms. Corda records an explicit link between human-language legal prose documents and smart contract code. Corda is built on industry-standard tools . Corda has no native cryptocurrency

Figure 14: Corda

3.7.1 Principal Features of Corda

- Recording and managing the evolution of financial agreements and other shared data between two or more identifiable parties in a way that is grounded in existing legal constructs and compatible with existing and emerging regulation.
- Choreographing workflow between firms without a central controller.
- Supporting consensus between firms at the level of individual deals,not a global system.
- Supporting the inclusion of regulatory and supervisory observer nodes.
- Validating transactions solely between parties to the transaction.
- Supporting a variety of consensus mechanisms.
- Recording explicit links between human-language legal prose documents and smart contract code.
- Using industry-standard tools.
- Restricting access to the data within an agreement to only those explicitly entitled or logically privileged to it.

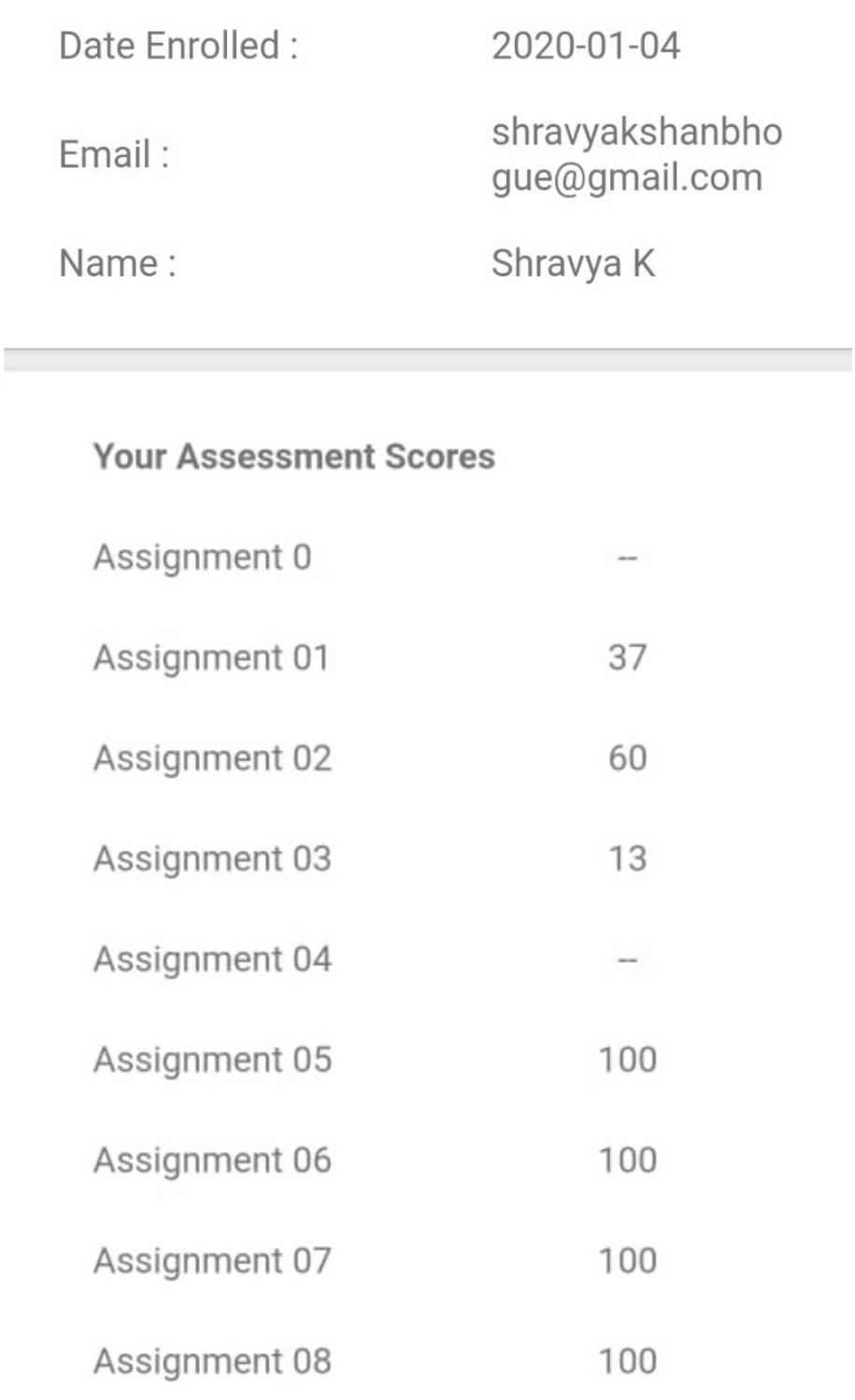
Chapter 4

Result And Conclusion

4.1 Conclusion

Blockchain technology could be quite complementary in a possibility space for the future world that includes both centralized and decentralized models. Like any new technology, the blockchain is an idea that initially disrupts, and over time it could promote the development of a larger ecosystem that includes both the old way and the new innovation.
While there are significant upsides to the blockchain, there are also significant challenges to its adoption. The roadblocks to the application of blockchain technology today are not just technical. The real challenges are political and regulatory, for the most part, to say nothing of the thousands of hours of custom software design and back-end programming required to integrate blockchain to current business networks.Some of the challenges standing in the way of widespread blockchain adoption are technology cost, speed inefficiency, illegal activity, central bank concerns, hack susceptibility.
Blockchain has seen its fair share of public scrutiny over the last two decades, with businesses around the world speculating about what the technology is capable of and where it's headed in the years to come. With many practical applications for the technology already being implemented and explored, in no small part because of bitcoin and cryptocurrency. As a buzzword on the tongue of every investor in the nation, blockchain stands to make business and government operations more accurate, efficient, and secure.

4.2 NPTEL Progress Screenshot:



Date Enrolled :	2020-01-04
Email :	shravyakshanbhogue@gmail.com
Name :	Shravya K

Your Assessment Scores

Assignment 0	--
Assignment 01	37
Assignment 02	60
Assignment 03	13
Assignment 04	--
Assignment 05	100
Assignment 06	100
Assignment 07	100
Assignment 08	100

Figure 15: NPTEL report

REFERENCES

NPTEL course on "Blockchain Technology and Applications" by **Sandeep K. Shukla IIT Kanpur** has helped me learn and prepare this report.

Websites I referred

- https://en.wikipedia.org/wiki/Blockchain
- https://en.wikipedia.org/wiki/Merkle_tree
- https://steemit.com/ledger/@crypt0k/centralized-and-decentralized-ledgers-
- https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/
- https://www.oreilly.com/library/view/blockchain/9781491920480/ch07.html
- https://thenewstack.io/the-mechanics-of-bitcoin/
- https://www.investopedia.com/terms/b/blockchain.asp