**BLOCKCHAIN**

**REPORT**

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR Four Weeks Training

at

**KERALA BLOCKCHAIN ACADEMY**

**(from 1 AUG to 30 AUG)**

SUBMITTED BY

Shashi Gupta

D4ITB1

1821072

1805555



**Information Technology Department**

**GURU NANAK DEV ENGINEERING COLLEGE**

LUDHIANA, INDIA

I

**BLOCKCHAIN**

**REPORT**

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR Four Weeks Training

at

**KERALA BLOCKCHAIN ACADEMY**

**(from 1 AUG to 30 AUG)**

SUBMITTED BY

Shashi Gupta

D4ITB1

1821072

1805555

**Information Technology Department**

**GURU NANAK DEV ENGINEERING COLLEGE**

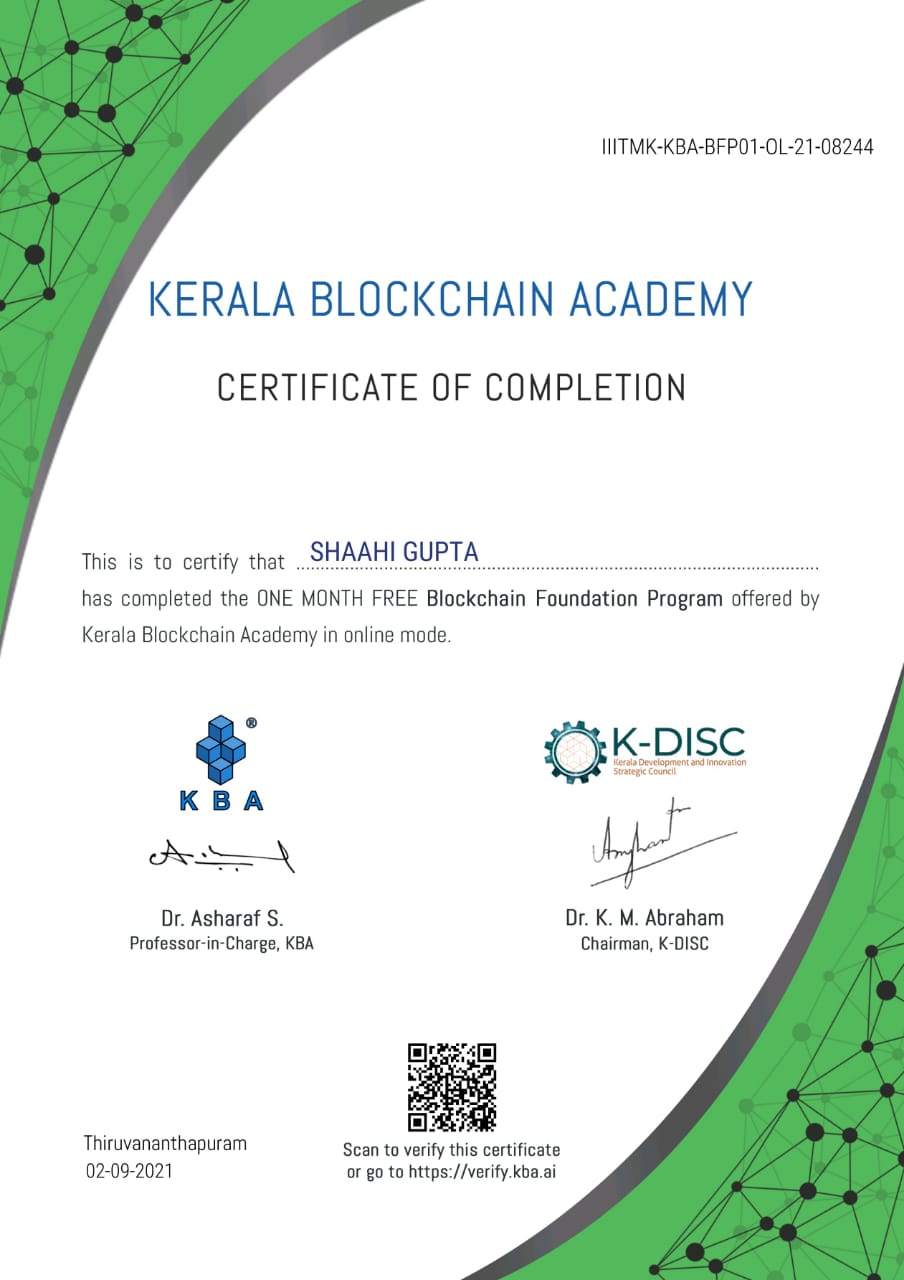
LUDHIANA, INDIA

II

**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. Considering the need to disseminate the emerging concepts for students, we decided to prepare a new course on blockchain technology platforms and applications.

III



IV

**ACKNOWLEDGEMENT**

I/WE are highly grateful to the Dr. Sehijpal Singh , Principal, Guru Nanak Dev Engineering College (GNDEC), Ludhiana, for providing this opportunity to carry out the six month industrial training at **KERALA BLOCKCHAIN ACADEMY.**

The constant guidance and encouragement received from Dr. K. S. Mann Dean T&P, GNDEC Ludhiana has been of great help in carrying out the project work and is acknowledged with reverential thanks.

I/WE would like to express a deep sense of gratitude and thanks profusely to **Dr. K. M. Abraham** Chairman of Company , . Without the wise counsel and able guidance, it would have been impossible to complete the report in this manner.

The help rendered by Mr **Dr. Asharaf S.** , Designation **Professor-In-Chargefor** experimentation is greatly acknowledged.

I/WE express gratitude to other faculty members of Information Technology department of GNDEC for their intellectual support throughout the course of this work.

Finally, I/WE are indebted to all whosoever have contributed in this report work and friendly stay at **KERALA BLOCKCHAIN ACADEMY**

**Shashi Gupta**

V

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Fig. No.** | **Figure Description** | **Page No.** |
| **Fig:1.2** | **Sturat-haber**  **w-scott-stornetta** | **3** |
| **Fig:1.2.1** | **Merkle-trees** | **4** |
| **Fig:1.2.2** | **Hal-finney** | **5** |
| **Fig:1.2.3** | **Satoshi-nakamoto** | **6** |
| **Fig:2** | **Transaction Flow** | **8** |
| **Fig:2.1** | **Bitcoin** | **9** |
| **Fig:2.1.1** | **Sender receiver** | **10** |
| **Fig:3** | **Ethereum** | **12** |
| **Fig:3.2** | **Decentralized** | **16** |
| **Fig:3.3** | **Hyperledger** | **17** |
| **Fig:3.4** | **Hyperledger Fabric** | **19** |

VI

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| **Contents**  **Abstract**  **Certificate**  **Acknowledgement**  **List of Figures**  **Table of Contents** | **Page No.**  **III**  **IV**  **V**  **VI**  **VII** |
| **Chapter 1: Introduction**   * 1. **Why do I Need To Know Blockchain**   2. **History Of Blockchain** | **1**  **2**  **3-6** |
| **Chapter 2: Transaction Flow**  **2.1 Bitcoin**  **2.1.1 How Bitcoins Works**  **2.1.2 How do people get Bitcoins?**  **2.2 Proof Of Work** | **7-8**  **9**  **10**  **11**  **12** |
| **Chapter 3: Introduction To Ethereum**  **3.1 How Does Ethereum Work?**  **3.1.1 Smart contracts defined**  **3.1.2 How smart contracts work**  **3.1.3 What is Solidity?**  **3.2 Decentralized Applications**  **3.3 Introduction To Hyperledger**  **3.4 Hyperledger Fabric** | **13**  **14**  **15**  **16**  **17**  **18**  **18**  **19** |
| **Chapter 4: Conclusion and Future Scope with Blockchain**  **4.1 FUTURE SCOPE**  **4.2 Conclusion** | **20**  **20**  **20** |
| **References** | **21** |

VII

**CHAPTER 1**

**INTRODUCTION**

[1]The original **Blockchain**is open-source technology which offers an alternative to the traditional intermediary for transfers of the crypto-currency **Bitcoin**. The intermediary is replaced by the **collective verification of the ecosystem** offering a huge degree of traceability, security and speed.

In the example above (a "**public Blockchain**"), there are multiple versions of you as “nodes” on a network acting as executors of transactions and miners simultaneously. Transactions are collected into blocks before being added to the Blockchain. Miners receive a Bitcoin reward based upon the computational time it takes to work out a) whether the transaction is valid and b) what is the correct mathematical key to link to the block of transactions into the correct place in the open ledger. As more transactions are executed, more Bitcoins flow into the virtual money supply. The "reward" miners get will reduces every 4 years until Bitcoin production will eventually cease (although estimates say this won't be until 2140!). Of course, although the original Blockchain was intended to manage Bitcoin, other virtual currencies, such as Ether, can be used.

1

**1.1 Why do I need to know about Blockchain?**

There are three reasons why you need to know about Blockchain:

1. Blockchain technology **doesn't have to exist publicly**. It can also exist privately - where **nodes**are simply points in a private network and the Blockchain acts similarly to a distributed ledger. Financial institutions specifically are under tremendous pressure to demonstrate regulatory compliance and many are now moving ahead with Blockchain implementations. Secure solutions like Blockchain can be a crucial building block to reduce compliance costs.
2. Block-chain technology is **broader than finance**. It can be applied to any multi-step transaction where traceability and visibility is required. **Supply chain** is a notable use case where Blockchain can be leveraged to manage and sign contracts and audit product provenance. It could also be leveraged for **votation**platforms, titles and deed management - amongst myriad other uses. As the digital and physical worlds converge, the practical applications of Blockchain will only grow.
3. exponential and disruptive growth of Blockchain will come from the **convergence**of public and private Blockchains to an ecosystem where firms, customers and suppliers can collaborate in a secure, auditable and virtual way.

2

**1.2 HISTORY OF BLOCKCHAIN**

[2] The blockchain technology was described in **1991** by the research scientist **Stuart Haber** and **W. Scott Stornetta**. They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of **cryptographically** secured chain of blocks to store the time-stamped documents.

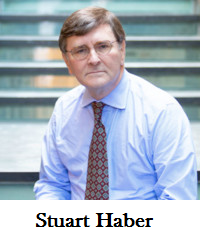


Fig: 1.2

In **1992**, Merkle Trees were incorporated into the design, which makes [blockchain](https://www.javatpoint.com/blockchain-tutorial) more efficient by allowing several documents to be collected into one block. **Merkle Trees** are used to create a 'secured chain of blocks.' It stored a series of data records, and each data records connected to the one before it. The newest record in this chain contains the history of the entire chain. However, this technology went unused, and the patent lapsed in 2004.

3

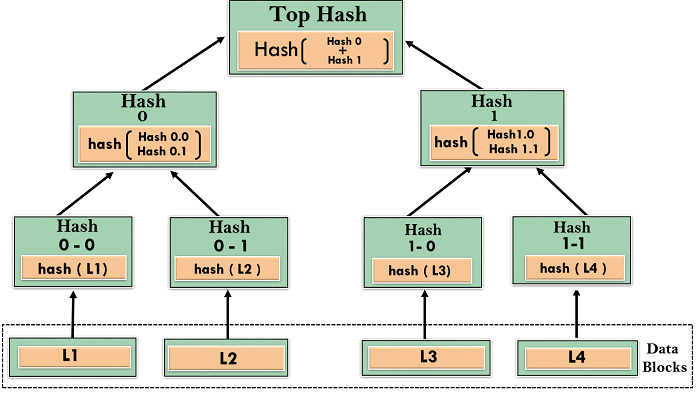


Fig:1.2.1

In **2004**, computer scientist and cryptographic activist **Hal Finney** introduced a system called **Reusable Proof Of Work(RPoW)** as a prototype for digital cash. It was a significant early step in the history of cryptocurrencies. The RPoW system worked by receiving a non-exchangeable or a non-fungible Hashcash based proof of work token in return, created an **RSA-signed** token that further could be transferred from person to person.

RPoW solved the double-spending problem by keeping the ownership of tokens registered on a trusted server. This server was designed to allow users throughout the world to verify its correctness and integrity in real-time.

4



Fig:1.2.2

Further, in **2008**, **Satoshi Nakamoto** conceptualized the theory of **distributed blockchains**. He improves the design in a unique way to add blocks to the initial chain without requiring them to be signed by trusted parties. The modified trees would contain a secure history of data exchanges. It utilizes a peer-to-peer network for timestamping and verifying each exchange. It could be managed autonomously without requiring a central authority. These improvements were so beneficial that makes blockchains as the backbone of cryptocurrencies. Today, the design serves as the public ledger for all transactions in the [cryptocurrency](https://www.javatpoint.com/blockchain-cryptocurrency) space.

The evolution of blockchains has been steady and promising. The words block and chain were used separately in Satoshi Nakamoto's original paper but were eventually popularized as a single word, the Blockchain, by **2016**. In recent time, the file size of cryptocurrency blockchain containing records of all transactions occurred on the network has grown from **20 GB** to **100 GB**.

5



Fig:1.2.3

6

**CHAPTER 2**

**TRANSACTION FLOW**

[3] Blockchain Technology is mostly about the transactions that we make digitally for ourselves. Eventually, these transactions make their way to the various blocks that become part of the Blockchain later on. So, it is important to understand the transaction life cycle in Blockchain technology.

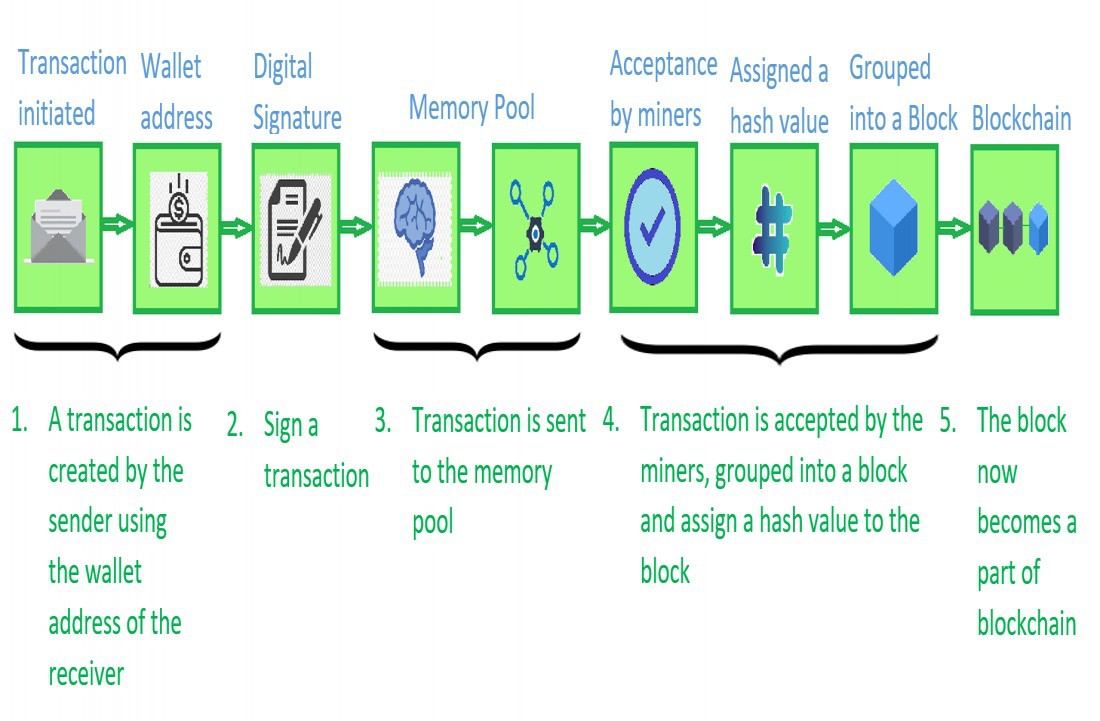
This lifecycle follows the journey of a single transaction as it makes its way through each stage in the process of joining the blockchain. Transaction in simple words is the process of sending money by the sender and the receiver receiving it. The Blockchain transaction is also quite similar, but it is made digitally.

Sourav and Suraj are two Bitcoin users. Sourav wants to send 1 bitcoin to Suraj.

1. First, Sourav gets Suraj’s wallet address (a wallet in the blockchain is a digital wallet that allows users to manage their transactions). Using this information, he creates a new transaction for 1 bitcoins from his wallet and includes a transaction fee of 0.003 bitcoin.
2. Next, he verifies the information and sends the transaction. Each transaction that is initiated is signed by a digital signature of the sender that is basically the private key of the sender. This is done in order to make the transaction more secure and to prevent any fraud.
3. Sourav’s wallet then starts the transaction signing algorithm which signs his transaction using his private key.
4. The transaction is now broadcasted to the memory pool within the network.
5. This transaction is eventually accepted by the miners. These miners, group this transaction into a block, find the Proof of Work, and assign this block a hash value to be mapped into the blockchain.
6. This block is now placed on the Blockchain.
7. As this block gains confirmation, it is accepted as a valid transaction in the network.
8. Once this transaction is accepted, Suraj finally gets his bitcoin.

The below diagram is a pictorial representation of the various stages in a transaction life cycle as discussed above.

7



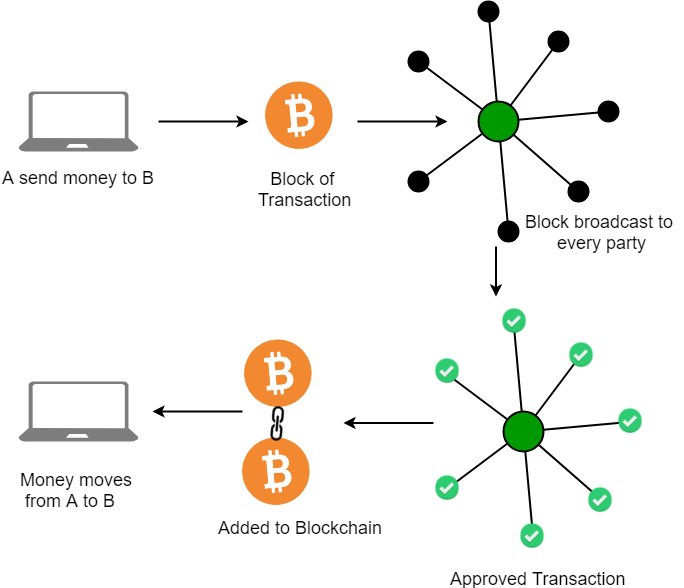


Fig:2

8

**2.1 BITCOIN**

Satoshi Nakamoto introduced the bitcoin in the year 2008. Bitcoin is a cryptocurrency(virtual currency), or a digital currency that uses rules of cryptography for regulation and generation of units of currency. A Bitcoin fell under the scope of [cryptocurrency](https://www.javatpoint.com/blockchain-cryptocurrency) and became the first and most valuable among them. It is commonly called decentralized digital currency.

A bitcoin is different from other traditional currencies such as Dollar, Pound, and Euro, which can also be used to buy things and exchange values electronically. There are no physical coins for bitcoins or paper bills. When you send bitcoin to someone or used bitcoin to buy anything, you don?t need to use a bank, a credit card, or any other third-party. Instead, you can simply send bitcoin directly to another party over the internet with securely and almost instantly.

Bitcoin, often described as a cryptocurrency, a virtual currency or a digital currency - is a type of money that is completely virtual. It's like an online version of cash. You can use it to buy products and services, but not many shops accept Bitcoin yet and some countries have banned it altogether.

The physical Bitcoins you see in photos are a novelty. They would be worthless without the private codes printed inside them



Fig:2.1

9

## **2.1.1 How Bitcoin Works?**

When you send an email to another person, you just type an email address and can communicate directly to that person. It is the same thing when you send an instant message. This type of communication between two parties is commonly known as Peer-to-Peer communication.

Whenever you want to transfer money to someone over the internet, you need to use a service of third-party such as banks, a credit card, a PayPal, or some other type of money transfer services. The reason for using third-party is to ensure that you are transferring that money. In other words, you need to be able to verify that both parties have done what they need to do in real exchange.

**For example**, Suppose you click on a photo that you want to send it to another person, so you can simply attach that photo to an email, type the receiver email address and send it. The other person will receive the photo, and you think it would end, but it is not. Now, we have two copies of photo, one is a simple email, and another is an original file which is still on my computer. Here, we send the copy of the file of the photo, not the original file. This issue is commonly known as the double-spend problem.



Fig:2.1.1

The double-spend problem provides a challenge to determine whether a transaction is real or not. How you can send a bitcoin to someone over the internet without needing a bank or some other institution to certify the transfer took place. The answer arises in a global network of thousands of computers called a Bitcoin Network and a special type of decentralized laser technology called **blockchain**.

10

**2.1.2 How do people get Bitcoins?**

There are three main ways people get Bitcoins.

* You can **buy Bitcoins** using 'real' money.
* You can **sell things**and let people pay you with Bitcoins.
* Or they can be **created** using a computer.

**2.2 PROOF OF WORK**

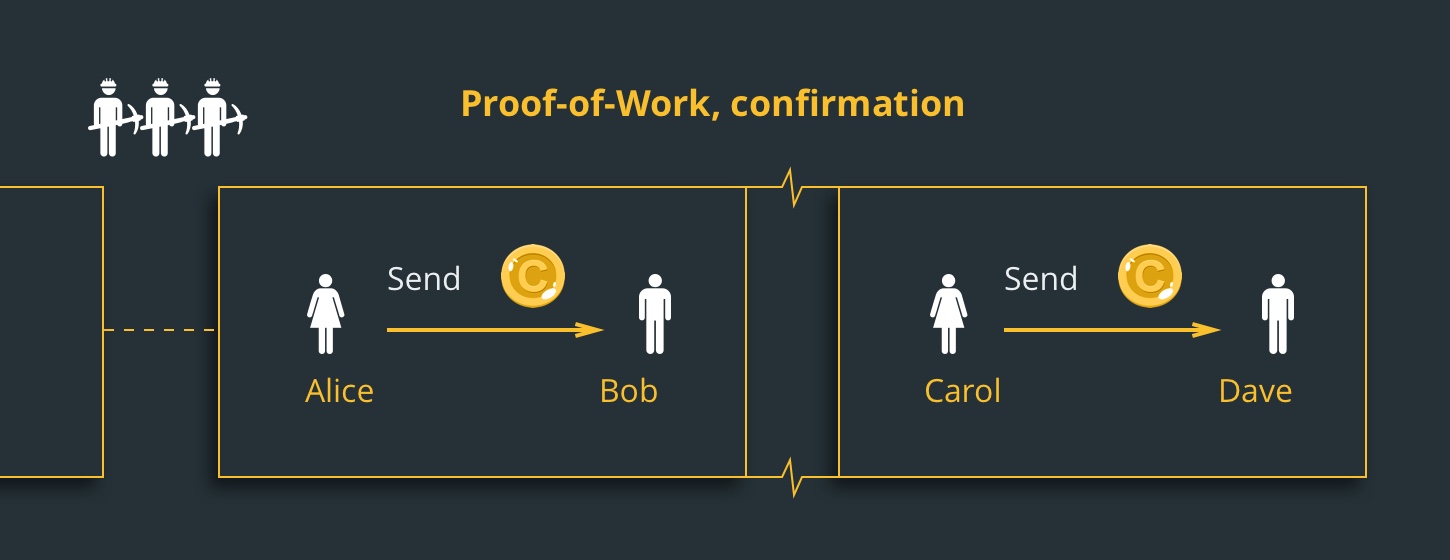
Proof of Work(PoW) is the original consensus algorithm in a blockchain network. The algorithm is used to confirm the transaction and creates a new block to the chain. In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network. The process of competing against each other is called mining. As soon as miners successfully created a valid block, he gets rewarded. The most famous application of Proof of Work(PoW) is Bitcoin.

Producing proof of work can be a random process with low probability. In this, a lot of trial and error is required before a valid proof of work is generated. The main working principle of proof of work is a mathematical puzzle which can easily prove the solution. Proof of work can be implemented in a blockchain by the Hashcash proof of work system.

11



In the puzzle game, [bitcoin](https://www.javatpoint.com/bitcoin) software creates a challenge, and there is a game begins. This game involves all miners competing against each other to solve the challenges, and this challenge will take approximately 10 minutes to be completed. Every single miner starts trying to find the solution to that one Nonce that will satisfy the hash for the block. At some specific point, one of those miners in the global community with higher speed and great hardware specs will solve the cryptography challenge and be the winner of the game. Now, the rest of the community will start verifying that block which is mined by the winner. If the nonce is correct, it will end up with the new block that will be added to the blockchain. The concept of generating a block provides a clear explanation of proof of work(PoW).



12

**CHAPTER 3**

**INTRODUCTION TO ETHEREUM**

[4] Ethereum is often referred to as the second most popular cryptocurrency, after Bitcoin. But unlike Bitcoin—and most other virtual currencies—Ethereum is intended to be much more than simply a medium of exchange or a store of value. Instead, Ethereum calls itself a decentralized computing network built on blockchain technology. Let’s unpack what that means**.**



Fig:3

**3.1 How Does Ethereum Work?**

Like all cryptocurrencies, Ethereum works on the basis of a blockchain network. A blockchain is a decentralized, distributed public ledger where all transactions are verified and recorded.

It’s distributed in the sense that everyone participating in the Ethereum network holds an identical copy of this ledger, letting them see all past transactions. It’s decentralized in that the network isn’t operated or managed by any centralized entity—instead, it’s managed by all of the distributed ledger holders.

13

Blockchain transactions use cryptography to keep the network secure and verify transactions. People use computers to “mine,” or solve complex mathematical equations that confirm each transaction on the network and add new blocks to the blockchain that is at the heart of the system. Participants are rewarded with cryptocurrency tokens. For the Ethereum system, these tokens are called Ether (ETH).

Ether can be used to buy and sell goods and services, like Bitcoin. It’s also seen rapid gains in price over recent years, making it a de-facto speculative investment. But what’s unique about Ethereum is that users can build applications that “run” on the blockchain like software “runs” on a computer. These applications can store and transfer personal data or handle complex financial transactions.

“Ethereum is different from Bitcoin in that the network can perform computations as part of the mining process,” says Ken Fromm, director of education and development at the Enterprise Ethereum Alliance. “This basic computational capability turns a store of value and medium of exchange into a decentralized global computing engine and openly verifiable data store.”

## **3.1.1 Smart contracts defined**

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

## **3.1.2 How smart contracts work**

Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions  when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

14

that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

Then the smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts

#### **3.1.3 What is Solidity?**

Solidity is known as a contract-based, high-level programming language. This platform has similar syntax to the scripting language of JavaScript. Solidity as a programming language is made to enhance the Ethereum Virtual Machine. Solidity is statically typed scripting language which does the process of verifying and enforcing the constraints at compile-time as opposed to run-time

1. Solidity is known as a contract-based, high-level programming language.
2. This platform has similar syntax to the scripting language of JavaScript.
3. Solidity as a programming language is made to enhance the Ethereum Virtual Machine.
4. Solidity is statically typed scripting language which does the process of verifying and enforcing the constraints at compile-time as opposed to run-time.
5. This typed programming languages will help and do the checking at run-time as opposed to Compile-time.
6. This platform also supports inheritance in object-oriented programming, inheritance enables new objects to take on the properties of existing objects.

**3.2 DECENTERLIZED APPLICATION**

[5] Decentralized applications (dApps) are digital applications or programs that exist and run on a blockchain or peer-to-peer (P2P) network of computers instead of a single computer. DApps (also called "dapps") are outside the purview and control of a single authority. DApps—which are often built on the Ethereum platform—can be developed for a variety of purposes including gaming, finance, and social media.

15

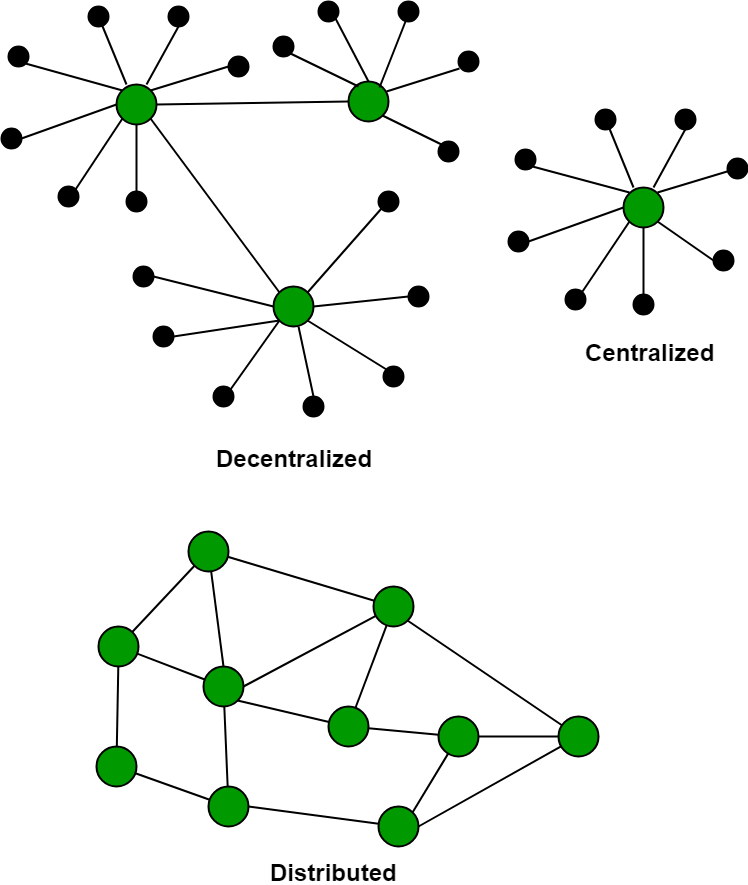


Fig:3.2

**3.3 Introduction To Hyperledger**

Hyperledger is an open source project under linux foundation where people can come and work on the platform to develop the blockchain related use-cases. According to Brian behlendorf, executive director of Hyperledger, Hyperledger provides the platform to create personalized blockchain service according to the need of business work. Unlike other platform for developing blockchain based software, Hyperledger has an advantage of creating secured and personalized blockchain network. The public blockchain requires every peers in the network for completing the process and run consensus at the same time. when the business requires confidentiality in the work, the public network fails to keep this as it does not support private and consortium network.

16

Example:

Consider a situation when person X wants to buy medicine from person Y, who was a doctor living in another country. As medicine requirement is of the one person’s private need, they need to maintain the data confidentially. But Dr. Y is selling medicine in the network to so many people, in case of public blockchain, every transaction will get updated in the network to all the peers. That’s where hyperledger find its significance. In the hyperledger, the parties are directly connected and the concerned people’s ledger will be updated. Hence providing the privacy and confidentiality.

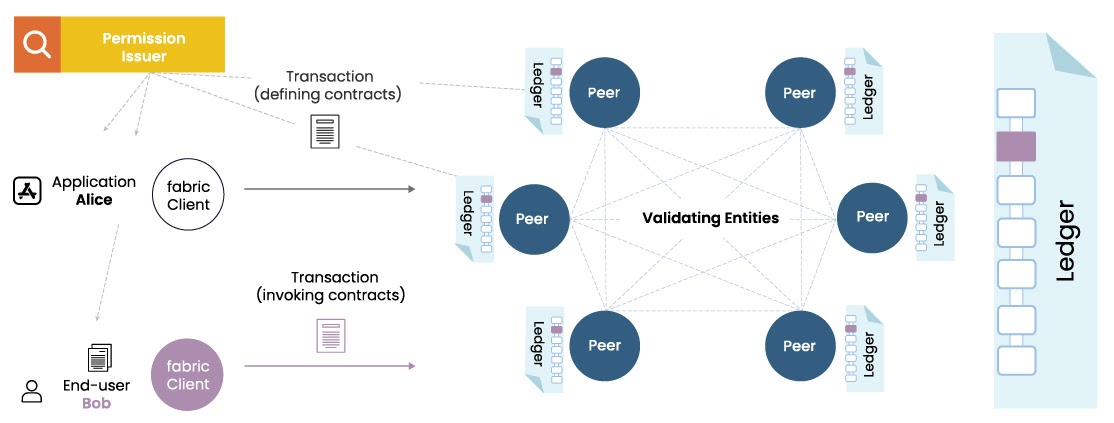


Fig:3.3

**3.4 HYPERLEDGER FABRIC**

Hyperledger Fabric is an open-source platform for building distributed ledger solutions, with a modular architecture that delivers high degrees of confidentiality, flexibility, resiliency, and scalability. This enables solutions developed with fabric to be adapted for any industry. This is a private and confidential blockchain framework managed by the Linux F Workflow:

17

For each and every transaction in the fabric, the following steps are followed-

1. **Creation of the proposal:** Imagine a deal between a smartphone manufacturer company and a smartphone dealership. The transaction begins when a member organization proposes or invokes a transaction request with the help of the client application or portal. Then the client application sends the proposal to peers in each organization for endorsement.
2. **Endorsement of the transaction:** After the proposal reaches the endorser peers (peers in each organization for endorsement of a proposal) the peer checks the fabric certificate authority of the requesting member and other details that are needed no authenticate the transaction. Then it executes the chain code (a piece of code that is written in one of the supported languages such as Go or Java) and returns a response. This response indicates the approval or rejection of the following transaction. The response is carried out to the client.
3. **Submission to ordering service:** After receiving the endorsement output, the approved transactions are sent to the ordering service by the client-side application. The peer responsible for the ordering service includes the transaction into a specific block and sends it to the peer nodes of different members of the network.
4. **Updating the ledger**: After receiving this block the peer nodes of such organizations update their local ledger with this block. Hence the new transactions are now committed.

18

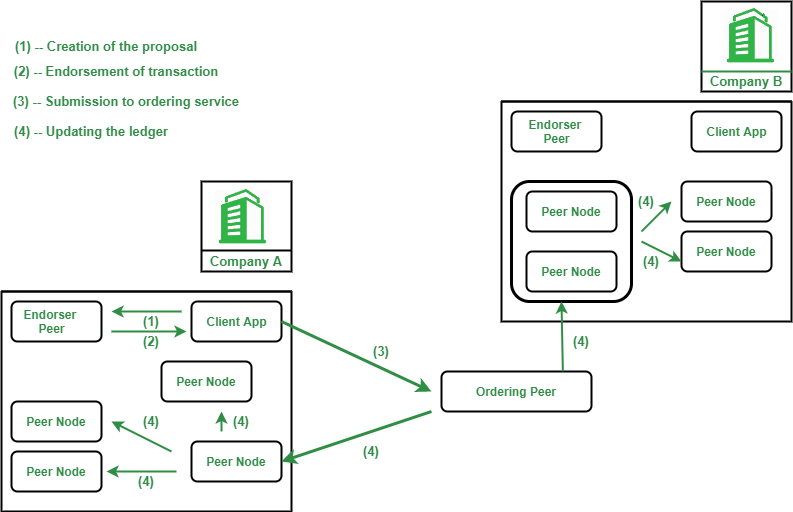


Fig:3.4

19

**CHAPTER 4**

**CURRENT IMPLETATION AND FUTURE SCOPE WITH BLOCKCHAIN**

**[6] Blockchain technology** is the growing invention which includes a chain of blocks. A **Blockchain** is a distributed or a **digital ledger**, which is primarily created to record the details of each financial and non-financial transaction. The absolute and permanent data is stored in a distributed database. The entire record is completely transparent which means that anyone who is linking to the network is able to view the transactions. Fundamentally, the **Blockchain technology** is the combination of three technologies, i.e. private key cryptography, P2P network, and the program. The **Blockchain technology** has shown its revolution in the field of information registration and distribution which removes the requirement for an intermediary expert to enable the digital relationships.

**Blockchain technology** has provided the most popular product, i.e. Bitcoin which is a type of cryptocurrency and functions as a public ledger for all transactions happening on the network. It has resolved the problem of double spending, unauthorized spending, and thus increasing security. It also helps to remove the need for an intermediary expert. Since there has been a substantial increase in the number of cyber attacks recently, the **Blockchain technology** help to attract the varied audience

**4.1 FUTURE SCOPE**

1. **Blockchain in Digital Advertising**
2. **Blockchain in Cyber Security**
3. **Blockchain will remove the requirement of the third party**
4. **Governments will provide their digital currencie**
5. **Managing World trade with the help of Blockchain Technology**
6. **Use of Blockchain in the Internet of Things and Networking**
7. **Blockchain in cloud storage**

**4.2 Conclusion:**

The **application of Blockchain technology** is not limited only to the finance industry. It has a fantastic future in different sectors such as supply chain management, digital advertising, forecasting, cyber security, Internet of things, networking, etc. **Blockchain technology** also has a huge prospective to provide the new openings for occupation in the industry. It also enhances the professional’s capability to upgrade themselves. With the help of **Blockchain technology**, it is possible to transform the whole world into a much smaller place. The transactional activities can be performed much faster and efficiently using Blockchain. Blockchain technology is going to be used in many more sectors in the future such as in government systems as these systems are  slow, dense, and likely to corruption. Implementing **Blockchain technology** in government system can make their operations much more secure and efficient.

20

REFRENCES:

[Ref number] Author’s initials. Author’s Surname, Book Title, edition (if not first). Place of publication: Publisher, Year

[1]  Government of **Kerala, KBA (**Digital Sciences), IIITM-K Building Thiruvananthapuram Kerala : Government of **Kerala, 2017.**

[2] Sandeep . Jain, GeeksforGeeks, Noida Utter Pradesh: Sandeep jain, 2006.

[3] Toshendra.Sharma, Blockchain Council, Walnut : Toshendra.Sharma: 2007.

[4] Aaron.Wood and Alex.Cohen, Cointelegraph (Digital Media) Sanfrancisco : Aaron Wood, 2013.

[5] Sonoo.Jaiswal, JavaTpoint, Noida : Sonoo.Jaiswal 2013.

[6] IITs, NPTEL, Roorkee, Delhi, Madras, Kharagpur: CRC Press, Willey, Springer, 2003.

21