

Mobile Crowdsourcing using Blockchain

Project report submitted in partial fulfilment of the requirement for the degree of
Bachelor of Technology

in

Computer Science and Engineering/Information Technology

By

Varun Mishra (161356)

Vipul Kashyap (161361)

Under the supervision of

Dr. Hemraj Saini

Dr. Geetanjali



Department of Computer Science & Engineering and Information Technology
Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented in this report entitled “**Mobile Crowd Sourcing using Blockchain** ” in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** submitted in the Department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat is an authentic record of my own work carried out over a period from August 2019 to May 2020 under the supervision of **Dr. Geetanjali (Asst. Prof.) CSE & IT**.

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

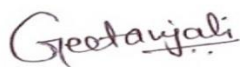


Varun Mishra
161356



Vipul Kashyap
161361

This is to certify that the above statement made by the candidate is true to the best of my knowledge.



Dr. Geetanjali
Asst. Prof. (SG)
CSE & IT

Dr. Hemraj Saini
Asso. Prof.
CSE & IT

Dated: 27 May 2020

ACKNOWLEDGEMENT

It is our privilege to express our deep gratitude and regards to our project supervisor Assistant Professor Dr. Geetanjali for her mentoring, valuable inputs, guidance and constructive criticism throughout the duration of this project. We also express our sincere thanks for encouraging and allowing us to present the project on the topic “**Mobile Crowdsourcing using Blockchain**” for the partial fulfillment of the requirements leading to the award of B.Tech. degree.

We would also like to thank Dr Satya Prakash Ghrera, Head of Department (CSE) for providing us a great opportunity to work on such an interesting project.

Last but not least we would like to express our sincere gratitude to our family members who stood by us and supported us in every phase of this project and gave us the much required moral support in carrying out this project successfully.

Varun Mishra

Vipul Kashyap

Contents

Chapter-1 Introduction.....	1
1.1 Introduction:.....	5
1.2 Problem Statement:	5
1.3 Objective:.....	6
1.4 Organization:	6
Chapter-2 Literature Survey.....	16
Paper 1: Crowd-sourcing Data from Mobile Smart-phones in Urban Spaces.....	16
Paper 2: Mobile Crowd-sourcing support system for disaster surveillance and response	17
Paper 3: Smart Notes: Application of Crowd-sourcing to the Detection of Web Threats	19
Paper 4: Block chain application for cyber security	20
Paper 5: Making sense of Bit coin, Block chain and Crypto Currency	23
Paper 6: A Survey of Crowd-sourcing Systems	26
Paper 7: Crowd-sourcing using Smart Phones	27
Chapter-3 System Development.....	29
Proposed Approach.....	30
Need:	31
Benefit:	32
Algorithm:	36
Chapter 4 Performance Analysis	39
ATTACKS:.....	41
Chapter-5 Conclusion and Future work.....	50
References :	523

Chapter-1

Introduction

1.1 Introduction:

Mobile crowd-sourcing is referred as crowd-sourcing using cell-phones. The main difficulty is that it can be tackled including the usage of distributed tasks between the users, and the mobile senses used in the collection of wisdom of the crowd. The mobile crowd-sourcing is used for gathering of information and data that comes from the end workers and is then used to complete a task for the users.

However the use of the mobile applications for crowd sourcing has found to be a great challenge to the end user and workers because of various attacks and security attacks. Sometimes the data that is collected by the various workers can be changed by the malicious users.

In order to protect the data from the attacks and security threats blockchain technology can be used. A blockchain is basically a group of records that are attached to each other and block contain a hash function for the previous data-node, and the transaction data.

So in this project we have showed how the data which is collected using the mobile crowd-sourcing technique can be protected from the security threats using blockchain technology.

1.2 Problem Statement:

As above discussed in the introduction the mobile crowd-sourcing enables large group of buyers and sellers to share the data on a common platform and due to which there are possibilities of security threats. The data can be very vulnerable to the threats due to high level of usage as the data can be altered by some malicious users. In this project, the concept of block chain has been shown in mobile crowd-sourcing.

1.3 Objective:

To provide a system which can protect the data and information of the users in crowdsourcing from security threats and malicious users using block chain technology.

1.4 Organization:

In **Chapter 1**, This report have gave a brief introduction about mobile crowd-sourcing, types of mobile crowd-sourcing techniques, its architecture, security and its need in mobile crowd-sourcing, different types of attacks, Block chain technology , why Block chain is essential in the field of mobile crowd sourcing and its architecture. In this report we have also mentioned objective of the project in this chapter.

In **Chapter 2**, This report have provided the Literature Survey to show what theoretical and methodological contributions has been done by various researchers in mobile crowd-sourcing.

In **Chapter 3**, This report have mentioned the proposed approach, its need and benefits. It have also described how the particular technology has been used to complete the project. It includes Algorithm, flowchart etc. It describes the mechanism of using various nodes and data and how data is kept by the various users.

In **Chapter 4**, This chapter have given the performance analysis that describes how mobile crowd-sourcing technique works with and without using blockchain. There are different types of attacks which can occur including Denial of Service, message alteration, false report etc. It is basically the implementation part of the project.

In **Chapter 5**, In the following chapter have just gave the conclusion and future work that can be done on the project later. It includes various references that are used in completing the project. The references are given in IEEE style.

Mobile Crowd-sourcing

Crowd-sourcing has emerged as a major technique that facilitates like processing the data and then problem solving abilities. It mainly refers to the people who collects the data while using the devices such as cell-phones or tablets and share this data. This data can be used by third parties for surveys or any related work.

The crowd-sourcing system include a platform installed on the devices as well as cloud. Mobile crowd-sourcing generally involves demographically distributed task and the sensing using the collection of wisdom of crowd.

The human being intelligence based crowd-sourcing contains three different groups of roles that are: the people makes requests, the workers and a central hub of crowd-sourcing system. The requesters submit the task which are most of the time challenging for the computers too but easy for human beings to complete with the help of the crowd-sourcing system.

A group of workers, which are interested in the task are in competition and submit the appropriate solutions to the crowd-sourcing system, while the person who will request will be in the position of selecting a proper solution and gives the workers the reward for the same. Considering the current world's biggest freelancing market place, up work, for instance, it will require the clients who will be known as the requesters to deposit a milestone payments for the same into account before all the work begins.

Then the client can interview the freelancers for the better results also known as the worker to design the software or write the details. Freelancers, who focuses on the areas of the expertise and will compete for the job and the deserving will be rewarded accordingly.

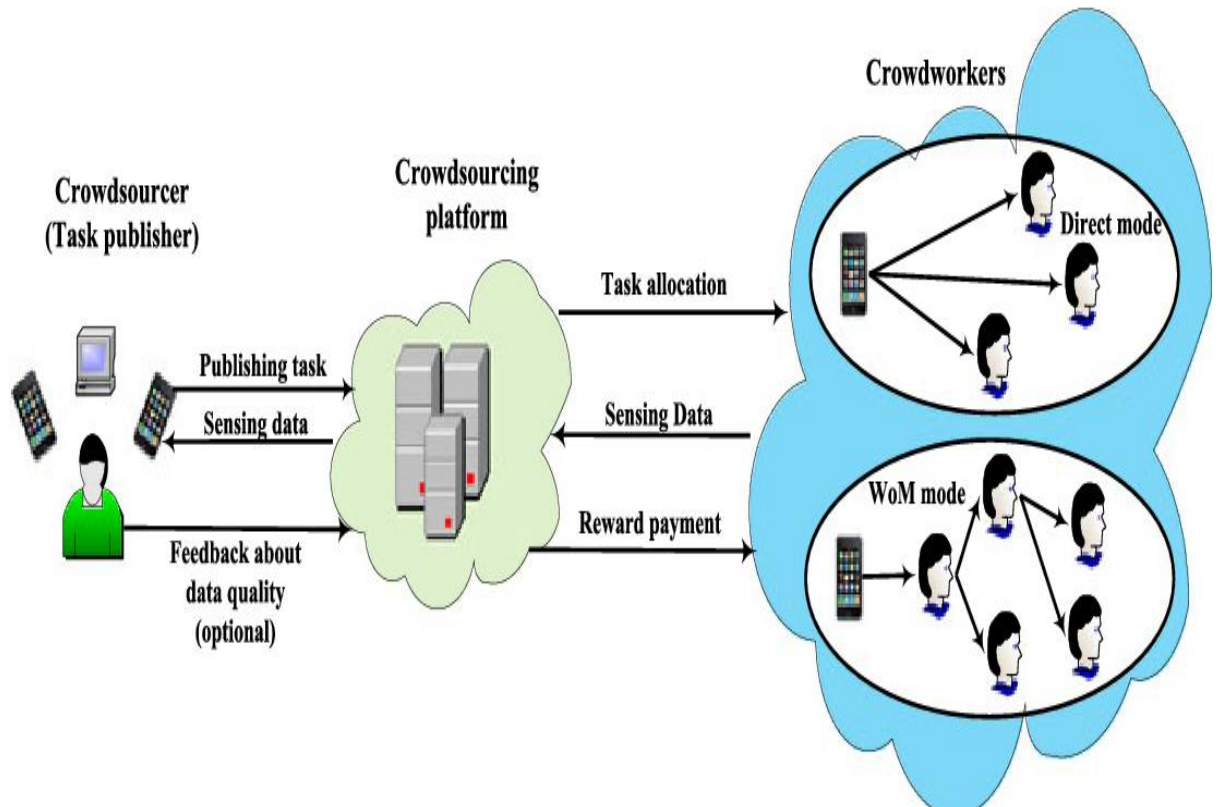


Fig. 1.1: Crowd sourcing

Despite being efficient it's a difficult process as human element is involved in the process. The program structure with the help of human computation is bit separate from the of the systems based on computer. Moreover, it relies on humans and thus the method that will take longer than the needed to find the suitable for the workers and complete the assigned task.

The whole process of collecting crowd feedback which will be needed to involve all the verification. Moreover, developing the effective algorithm and the decision making

process, to guess the group of people and also to avoid a system bias about the correct answers that are substantial challenge according to the study. Mobile crowd sourcing utilization for different set of applications are available for both scientific processes and for the business purposes also.

Areas that include the environment monitoring and the disaster management processes, infrastructure monitoring, community healthcare, transportation sources, ride pooling, urban-sensing and social issues. Mobile crowd sourcing can be categorized under different labels as “Participatory” and “Opportunistic” based on the communication between the participants in actions.

Advantages of Crowd-sourcing

1. Large number of users provides their experiences.
2. Cost effective for the company
3. Lack of some biasness towards the company that can expect the testers
4. It saves time and money.
5. It helps in building contacts and data.
6. It offers higher probabilities of success.

Disadvantages of Crowd-sourcing

1. Communication between the end workers can be of a difficult level due to the time consumption or the language barrier.
2. The security issues are compromised by having the tests performed by a big group who will or will not have loyalty to the brand or the product or maybe the organisation.
3. There may be danger of internal conflict between the workers.

Steps for successful Crowd-sourcing:

1. Design the job and divide the workers for performing the job.
2. Write clear instructions about the project that needs to be done.
3. Choose a web platform where the work will be done.
4. Release the jobs for the people and recruit the appropriate crowd according to requirement.
5. Listen to the opinions of the crowd and manage the assigned job regularly.
6. Assemble the defined data of end worker and then create the full and final product.

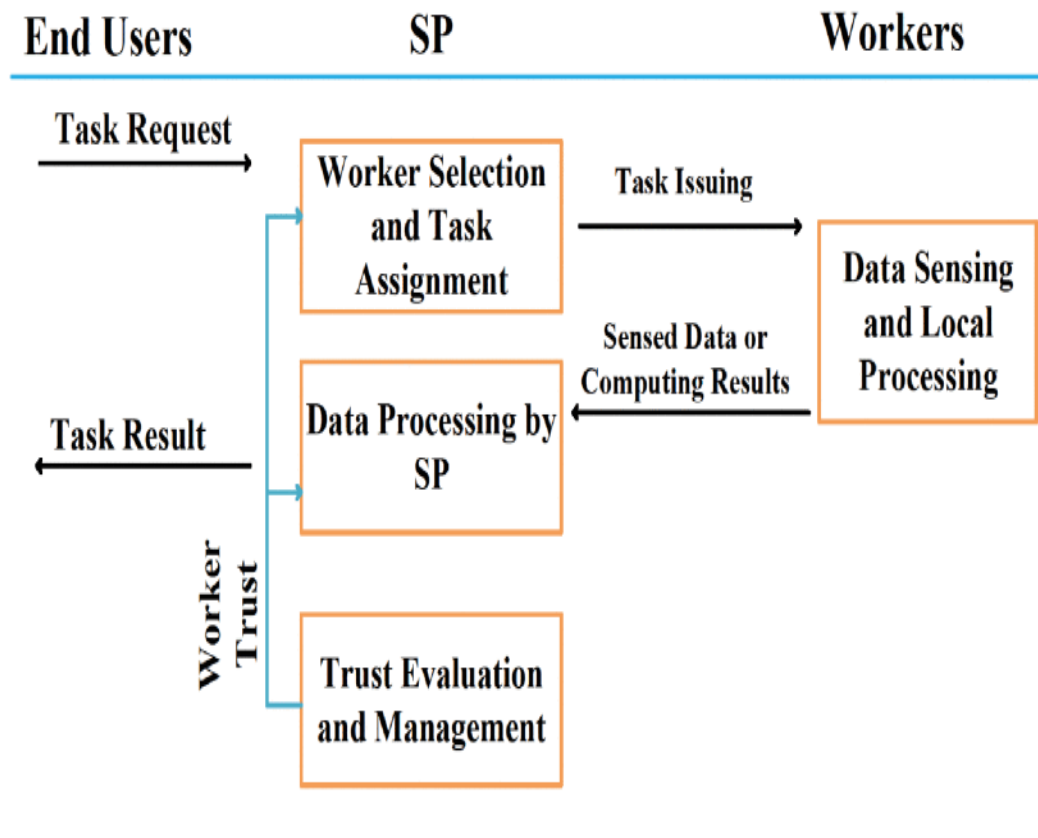


Fig. 1.2: Mobile crowd sourcing procedure

Architecture of Mobile Crowd-sourcing:

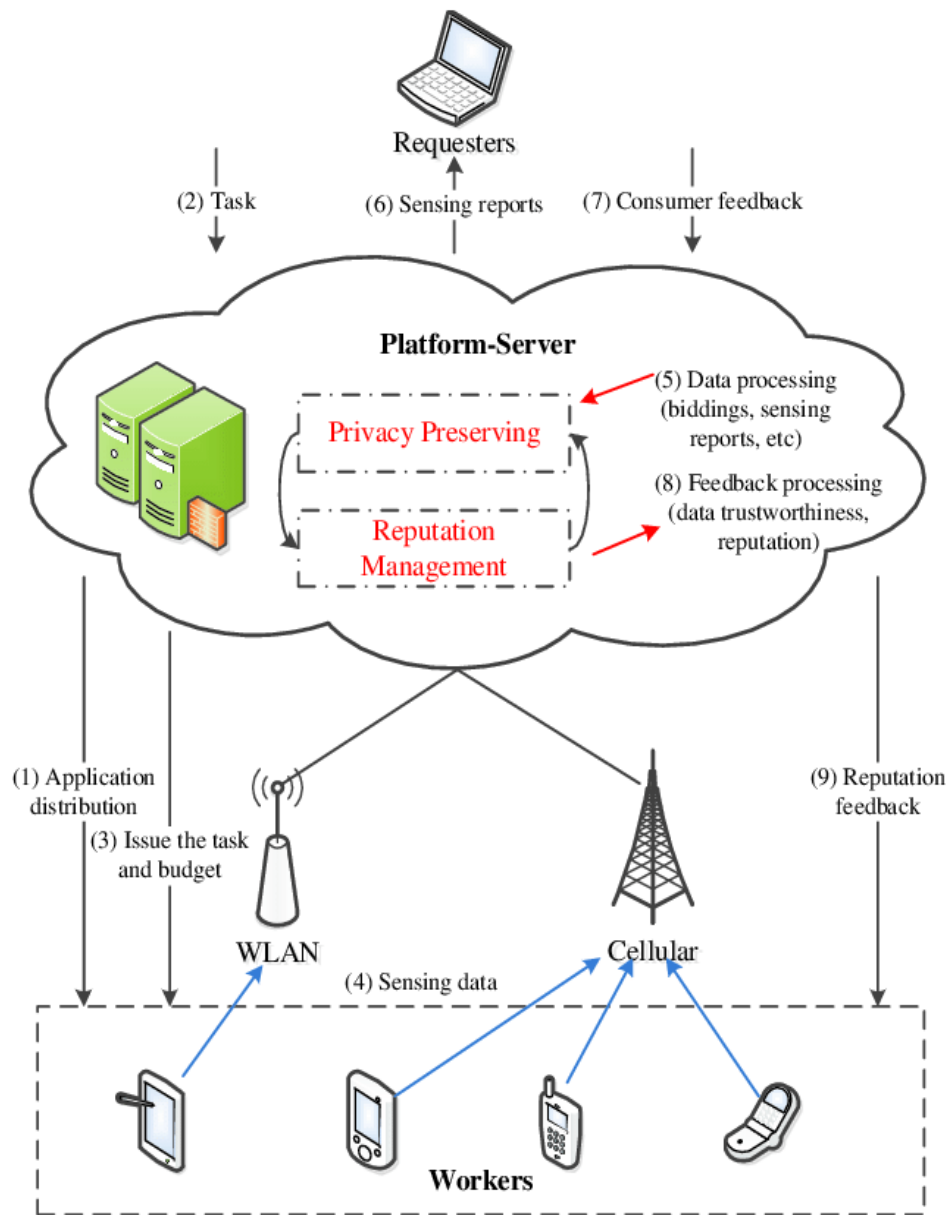


Fig. 1.3: Architecture of MCS

- **Security:**

Security basically means safety which is taken to protect the data and information from potential harm that can be caused by malicious users. Saving the important and the main data, the confidential information which should not be leaked, the network, the software, and the equipment is what security is all about.

Security is build up of three main objectives which are generally known as CIA which is the first Confidentiality, second Integrity, and last Availability.

- Confidentiality – this means that the information is not disclosed to the person who is not concerned or the entities and processes.
- Integrity – this means the maintenance of the accuracy and the degree of completeness of provided data hence means that the data cannot be altered by any unauthorized means of way or any user.
- Availability – this means the main information and data will be available to the people whenever needed.

Types of attacks:

1. Message Alteration
2. False report
3. Falsification Attack
4. Malware
5. Spam
6. Denial of Service

The Need of Security in the Field of Mobile Crowd-sourcing

There is an immense need for the security in crowd-sourcing as the data and various information collected from various end workers for the project can be easily edited and can be changed by some hackers, malicious users if there is no security provided in crowd-sourcing. There are various security threats and attacks that can occur in our data in crowd-sourcing which includes spam, pharming, phishing etc.

Malicious users who requests, they aim to collect solutions without even losing the deposit they have made, which is considered “false reporting” attack in essential. To gain this solution, they may do many things such as misreporting the evaluation of the solution as low level even if workers will contribute the high quality of the provided solution.

Malicious users who work attempts to get the rewards without paying even the sufficient and required efforts, which is “free-riding” attack.

If provided security is provided using any advanced technology will surely benefit the users as well as the workers. The Blockchain mechanism is widely used now-a-days for security purpose in crowd-sourcing.

Therefore, security issues in the field of crowd-sourcing plays an important role for the integrity, confidentiality of the data that can be used by various users around the world.

Hence, implementing the measures and system which are designed to protect and safeguard securely the vital information and the data ofcourse in crowd-sourcing is really important.

THE BLOCK CHAIN

As the name suggests “Block Chain” it is the list or the chain which grows continuously on the addition of the set of the records, which are called blocks linked to each other using different methods such as cryptography. Every node of the block chain which contains a cryptographic algorithm hash function for the previous block, transactional

data also and information, and a timestamp. By definition of design, the block chain is considered resistant to the modifications of the given data.

Block chaining can also be reviewed as the state machine based on transaction. Each of the state includes the information like balances of the account, data expressing information. It's only the updated form of a genesis state to the final state after the transaction for each block.

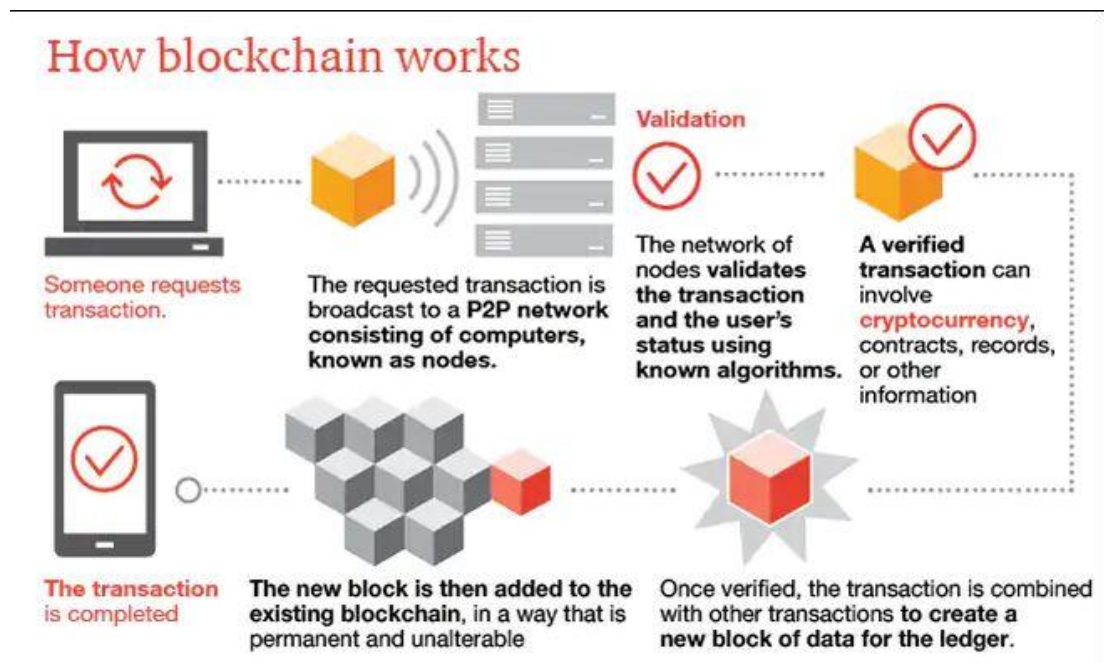


Fig. 1.4: Working of block chain

The data is added to the blocks of the block-chain, by connecting it with various blocks of the chain in chronological order and creating a chain of blocks linked together. Hence, data can only be added in a sequential order only. Hence, if data in any block is misused by any user it changes the hash of the block which doesn't match with the hash of the previous block. It helps to reduce the security threats that can occur to the confidential data of the users by protecting it from hackers, malicious users etc.

Blockchain's benefits and unknowns

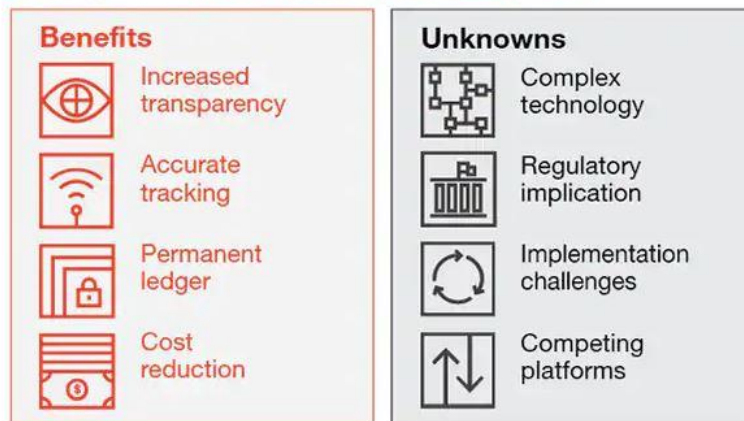


Fig. 1.5: Benefits of block chain

It helps in greater transparency, enhanced security, improved traceability, increased efficiency and speed of transactions, and reduced costs.

Architecture of Block Chain

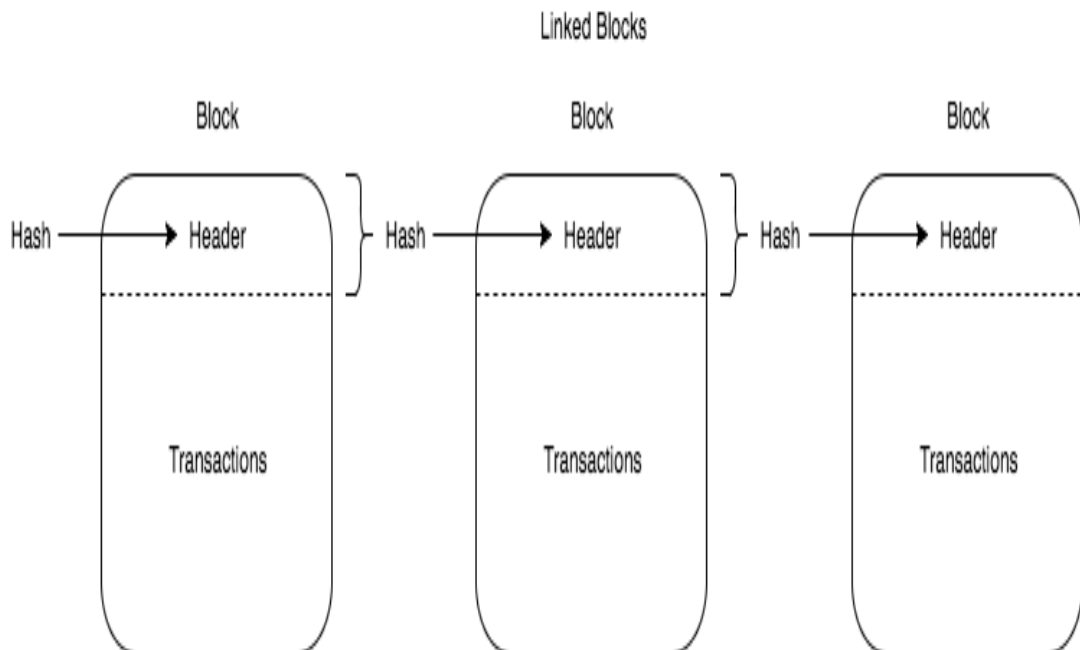


Fig. 1.6: Block chain Architecture

Chapter-2

Literature Survey

In this section, the report describes the various researches and trends in the field of mobile crowd-sourcing and block chain technology.

Paper 1: Crowd-sourcing Data from the Smart-phones in the Urban Space

In this paper, author J. Burke described how various mobile devices as the iPhones, Google Pixel has open doors for a novel for monitoring the landscapes which are urban and also known as mobile crowd-sourcing. Using this information, people can have the data from environment using their devices such as phones and they can share the same information using the existing infrastructures such as 3G/4G/WiFi. The data which is collected from the multiple people can be refined and combined to make a useful information for the interest which also extracts the important statistics.

The main trend of phones and the density of people areas with high level of diversity, crowd-sourcing technique can get a maximum coverage in both the spaces and obviously the time for observing events of interest spaces. Many exciting crowd-sourcing applications can have generated in the recent years.

The GPS trackers that can be one of the examples of crowd-sourcing which traces the data which is uploaded by the people and can be used to generate real time scenario. Video and images sample and street-level audios collected by pedestrians and travellers across the globe can be aggregated to create city geography. Wikipedia is also a great example of crowd-sourcing techniques which is widely used all across the globe.

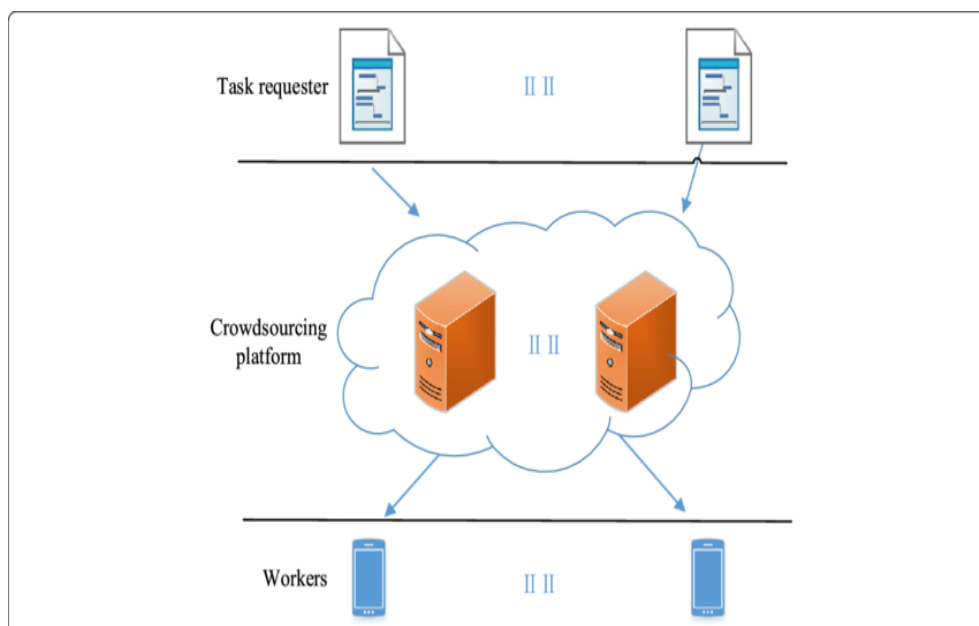


Fig. 2.1: Networking of mobile crowd-sourcing

Paper 2: Mobile Crowd-sourcing support for disaster management surveillance with appropriate response

The experiences with the major disasters which can tell us that person with the wireless equipments and the devices and social services that can work as effective moving human being sensors. A system which is named as CROSS that helps the crowd-sourcing disaster data and collected by end workers who explores the dangerous areas that have been developed by various researchers. The system aims to maintain a view of threatened areas prior and during disasters with the help from end workers who are volunteer to provide data and information to the system.

Internally, CROSS uses a graph to characterize the threatened area. Each node represents a place that needs a visit. The length of an edge between two nodes is the minimal time

required to travel between the places represented by the nodes. Given the graph and information about volunteers, the main frame work of the problem is to determine a route for each volunteer so as to maximize the visited nodes by all volunteers in the available time. It is a variant of the multiple travelling salesman problems.

This paper describes the concept and structure of CROSS, a system that supports crowd-sourcing the collection of disaster surveillance information: By coordinating volunteers in their explorations, the command centre can acquire disaster situation awareness quickly and efficiently.



Fig 2.2: Disaster surveillance system

Paper 3: Smart Notes: Application of Crowd-sourcing for the Detection of the Web based Threats

In this paper, Jaime G. Carbonell et al describes about a system that gave an alternate for the detection of web security threats over the internet. This is basically a crowd-sourcing system, called Smart Notes, which detects security threat attacks that can occur during browsing such as the Internet scams, the deceptive sales of products and the websites with intentions that provides wrong information to the end users. The main features of this system is combining the data from multiple different sources and combining the social book marking with questions and their answers to encourage the wider range of user participation.

The system which is developed helps the users to share their experiences which are related to threats related to web and attacks that occurred during browsing a particular website. The user can rate the websites, comment, ask and answer the relevant questions about the provided websites, provide surveys etc. This system has initially implemented as a chrome browser extension.

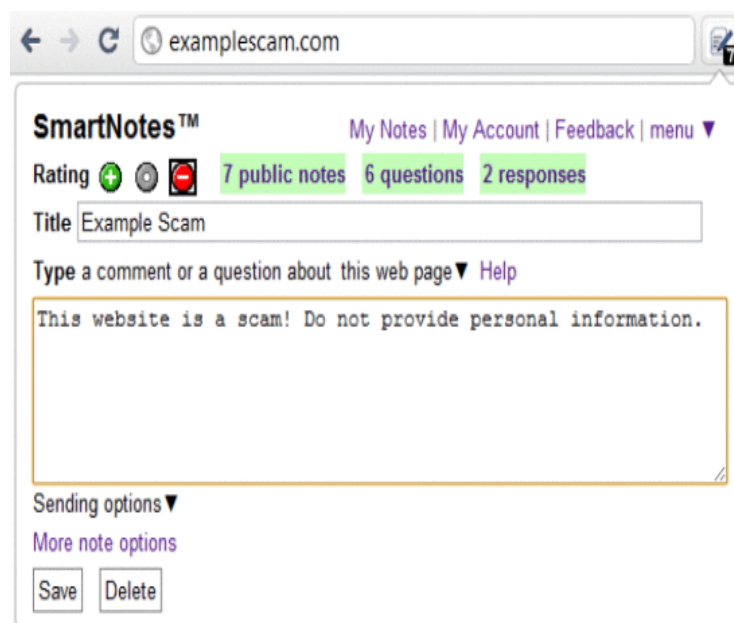


Fig.2.3: Smart Notes

When the user wants to post a comment or ask a question about the currently displayed web page, the user clicks the Smart Notes button on the chrome extension, which brings up the main window (Figure 5). The user can select the rating (positive, neutral, or negative) and add a free-text comment. Afterwards, the system sends these data to the server.

Paper 4: Block chain application for cyber security

The purpose of this research is to analyze and summarize the efforts of research in block chain applications for cyber security. Block chain features can be used to solve problems related to the security of devices such as mobile phones, networks and their end users. This will provide an understanding of the methods used to implement block chain in digital world for the purpose of security from different threats.

Block chain used encryption and hashing to store list of records and many of the existing cyber security solutions utilize very similar technology as well. The majority of existing security measures rely on a single trusted authority to verify information.

This leaves the system vulnerable to security attacks and can commit denial of service, inject malicious information and data. Block chain have the upper hand over current security measures in that true block chains are decentralized and do not require the authority or trust of an individual member of the group or network. The system does not require to trust each node in the network, or member, as it has a complete copy of all the historic information available.

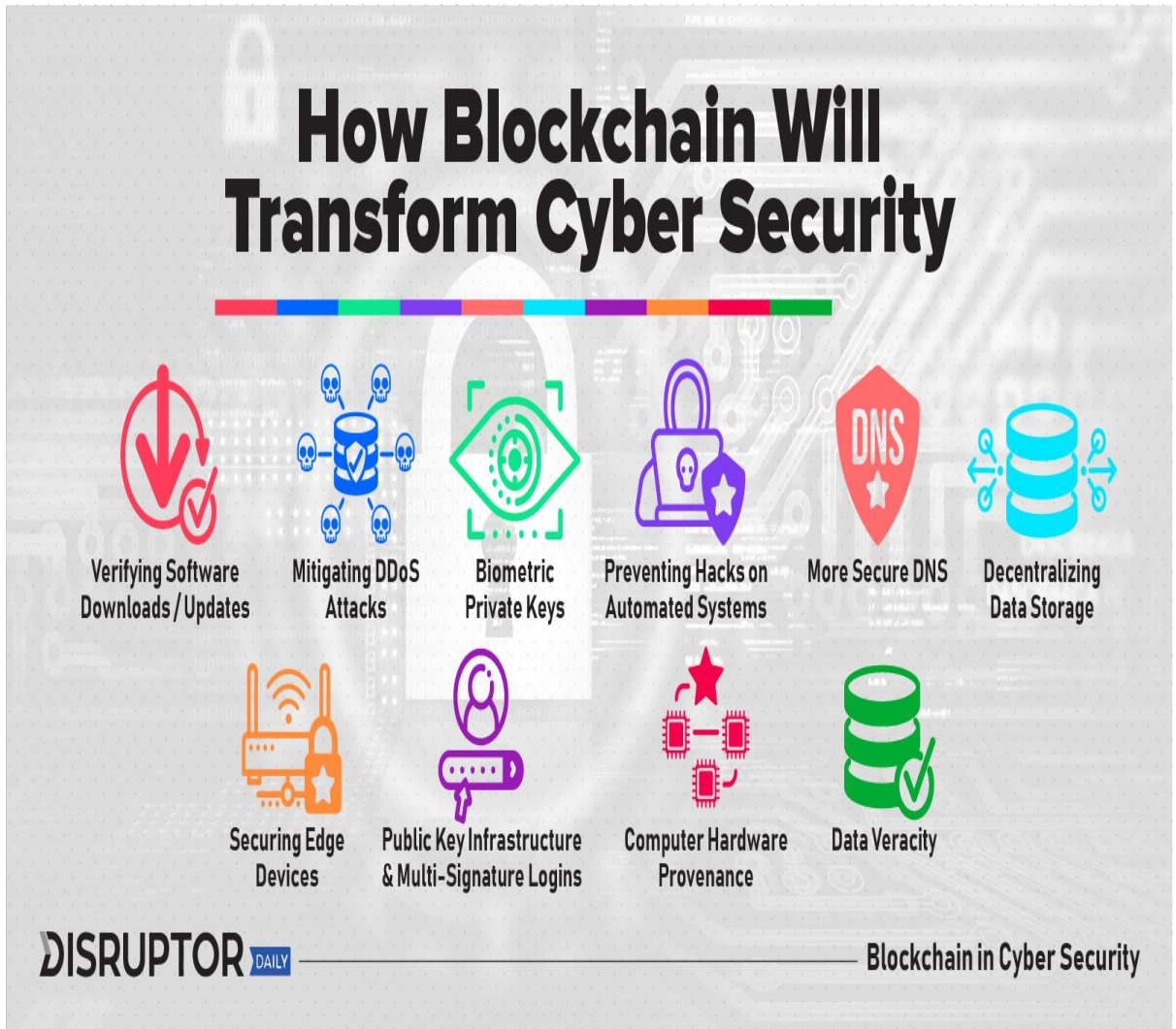


Fig. 2.4: How Blockchains transform Cyber security

The strength, robustness, reliability and trustless appeal of a block chain come from its “democratic” system. And due to this, the use of block chain has become a necessity. The more participating nodes there are and the better the mechanism to regulate behavior of mining nodes are, the better the decentralization and need for trust of individual nodes will be, which leads to improvements in block chain security and reliability.

BLOCKCHAIN IN CYBERSECURITY

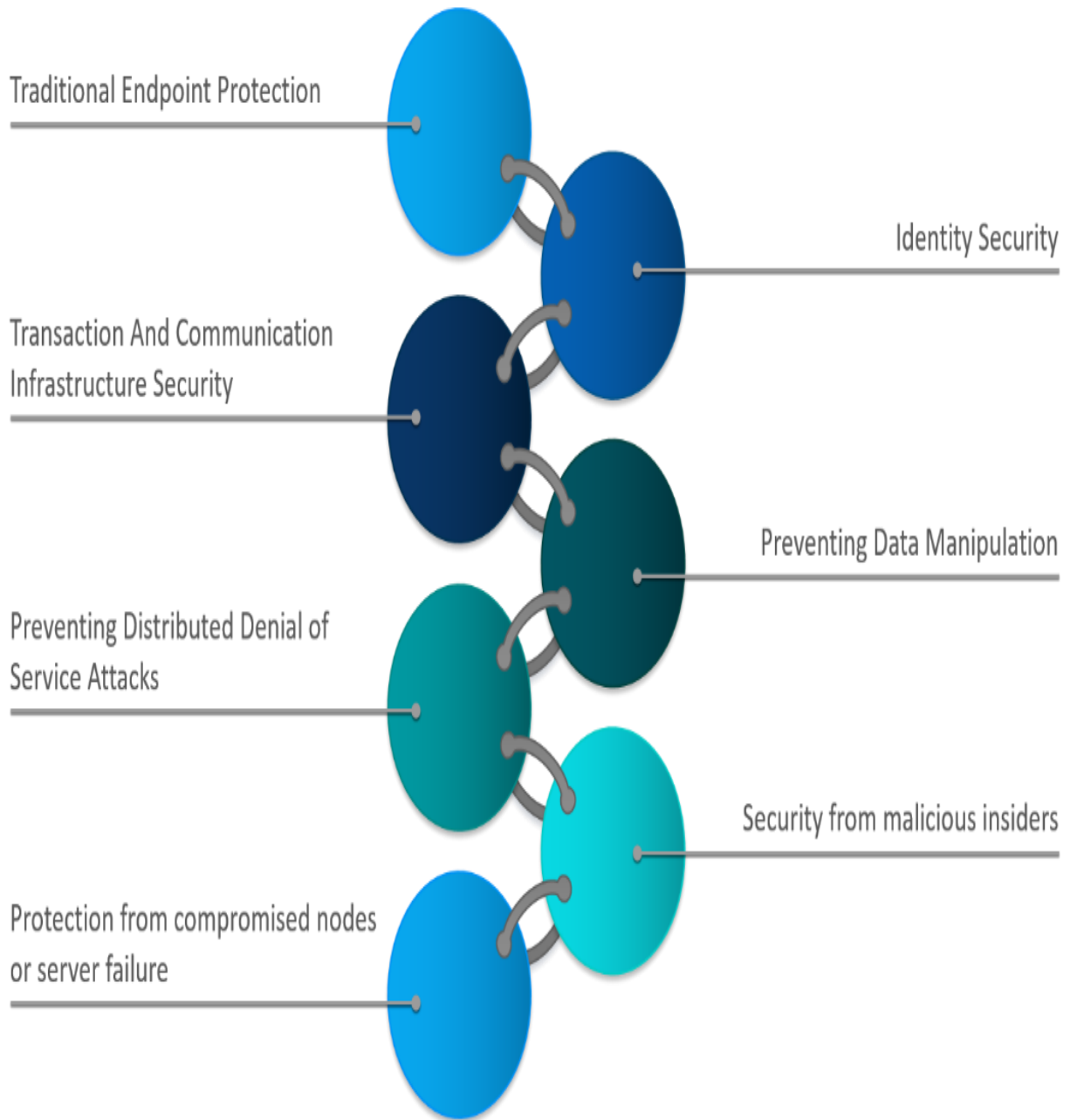


Fig.2.5: Blockchain in cybersecurity

Paper 5: Making sense of Bit coin, Block chain and Crypto Currency

This research paper discuss about how does Bit coin works and what is the use of crypto currency and block chain technology in Bit coin. The virtual currencies that aren't new online computer games have used them since so long — but with the development of the secure currency which is digitized without a issuer. It is maintained and supported by a network of miners whose are the computers which performs the calculations of the related stuff and then validates each and every transaction, and preventing the double spending and then they also earn a price of currently issued Bit coin.

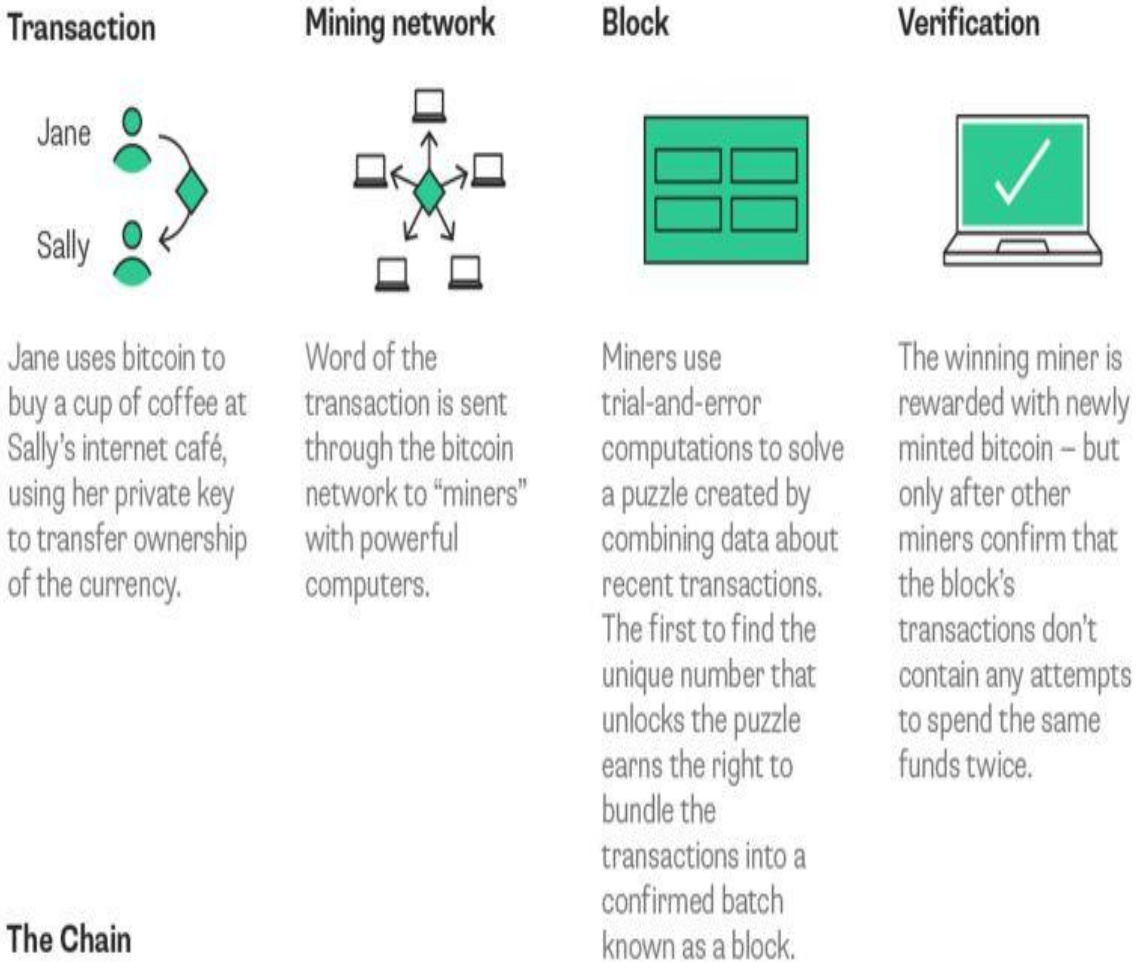
Bit coin's payment network (also called the bit coin block chain) is what makes it possible for us to transact with one another. When bit coin was initiated as an open source, then block chain was wrapped up against and together within the same set of solution.

Bit coin can refer to two main things. At first the bit coin network which keeps the track of the transactions and balances, and on the other hand the currency that we have used as the unit of value when we can transact.

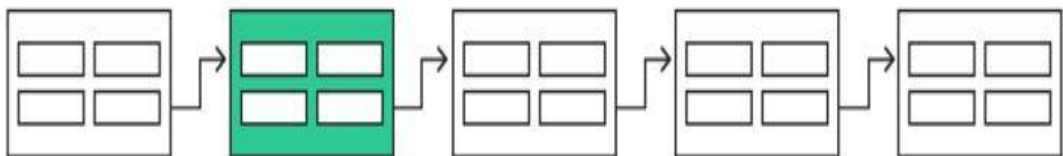
The block chain is a shared public ledger on which the entire bit coin network depends upon. All the conformation of the transactions are in the block-chain and then they are processed further. This allows the bit coin wallets which are used to calculate their whole balance which can be spend so that the transactions made are verified by ensuring that they are actually of a genuine spender. The cryptography process and the techniques are used for combining them in chronological order of the particular block chain.

How Blockchain Works for Bitcoin

When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.



The Chain



Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal Sally's bitcoin by rewriting the sequence of transactions.

Fig. 2.6: working of block chain for bit-coins

What is cryptocurrency?

Cryptocurrency

Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.



Has no intrinsic value in that it is not redeemable for another commodity, such as gold.



Has no physical form and exists only in the network.



Its supply is not determined by a central bank and the network is completely decentralized.

Fig.2.7: Visualization of Crypto Currency

Paper 6: A Survey of Crowd-sourcing Systems

In this paper, a survey on the crowd-sourcing technique has been provided which are categorized according to their applications, algorithms, performances and datasets. This paper provides a structured view of the research on crowd-sourcing till date. Crowd-sourcing is evolving as a distributed ledger problem solving and business model in the past few years. In crowd-sourcing technique, tasks are distributed to end users to complete such that a company's production cost can be greatly reduced up to a great extent. In 2003, Luis von Ahn and his colleagues gave the concept of "human computation", which takes human abilities to perform computation tasks that are difficult for computers to process at that time. Later, the term crowd-sourcing was given by Jeff Howe in 2006.

Since then, a lot of work in crowd-sourcing has focused on different aspects of crowd-sourcing, such as computational techniques and performance analysis.

An algorithm can help to formalize the design of a crowd-sourcing system. Yan et al. designed an accurate real time image search system for iPhone called Crowd-Search. Crowd-Search combines automated image search with real-time human validation of search results.

The experimental results showed that how time-independent variables of posted tasks affect completion time.

Mr. Singh proposed a game-theoretic framework for studying user behaviour and motivation patterns in social media networks. DiPalantino and Vojnovic gave a model of a competitive crowd-sourcing system, and showed that the participation rates are logarithmically increasing as a function of the offered reward.

This survey not only provides a better understanding about crowd-sourcing systems, but also gave future research activities and application developments in the field of crowd-sourcing.

Paper 7: Crowd-sourcing using Smart Phones

Smart phones can reveal crowd sourcing full potential and let users give their best to complex and novel problem solving. This emerging area can be shown through a technique that classifies the mobile crowd sourcing field and through three new applications that optimize location-based search and similarity services based on crowd-sourced information.

Crowd sourcing is a distributed problem-solving model in which a crowd of undefined size is collectively performing work to solve a complex problem. Crowd sourcing has still not fully been into the mobile workforce; however, the use of smart phones – which are always connected – will eventually reveal the full potential of this new problem-solving approach.

Smart phones devices offer a great platform for extending existing Web-based crowd sourcing applications to a larger contributing crowd, making contribution easier and friendly. Furthermore, smart phones abilities and capabilities – including geo-location, light, movement, and audio and visual sensors – offers a variety of new, efficient ways to collect data, enabling new crowd sourcing applications to perform well in real time systems.

Smart Phones feature different Internet connection services that provide various connectivity (such as Wi-Fi or 2G/3G/4G), as well as peer-to-peer (P2P) connection capabilities that provide connectivity to nodes in different ways such as Bluetooth, Portable Wi-Fi, or the new generation NFC. Each of these connection modalities requires different energy and has different data transfer rate characteristics and contains different requirements.

The various applications that can work on mobile crowd sourcing are:

1. -Smart Trace+, which enables similar functionalities which are without disclosing the user's personal data and personal information.
2. The crowd cast which is efficient in reporting to each user their k degree geographically nearest neighbours that is k neighbours..
3. SmartP2P, which exploits the main functions which helps in optimizing the dependent objectives on location of the search tasks in a social community.
4. Smart Lab is an programming cloud with an innovative ideas of more than forty real android smart phones and a large number of emulated smart devices deployed. Smart Lab provide an open and permanent test platform for developing and test the quality of smart phone apps via an web-based interface.

Chapter-3

System Development

The system involved in the process makes use of a block chain consisting of several nodes acting as the users. Each node has access to the block chain while maintaining a consistency throughout the entire chain. Each block in the block chain is identified by a unique value.

Crowd sourcing involves various attacks such as message alteration, false report etc. Each attack can hinder the overall process. The block chain uses the feature of the unique hash value to identify the nature of attack as well as the node that has been affected by it.

The entire block chain consists of various blocks along with their hash values and the hash value of the previous block. The block chain can be used to prevent any kind of malicious attack against the data as each modification requires verification from each node or block and any unethical transaction can be identified by a modified hash value that is accountable for when verified with the other nodes. The nodes or the network can be constructed using java based IDE or even with javascript. In the project we use eclipse for creating the block chain. The block chain includes nodes with each node containing some data, the timestamp, its hash value and the hash value of previous node.

The hash value is generated using SHA-256 which generates an encrypted form of hash data. SHA-256 generates a unique 256 bits string by taking in as input another string. The output data is in an encrypted form of data as the output reveals no information about the input and just appears as a form of randomized text.

The nodes can be used to relay information across the entire network of nodes and the data is duplicated across the entire network. The security in a block chain is what makes it so special. It acts as a public registry that is replicated. The attacks on block chain are highlighted with a hash value that is not present on the other nodes as the transaction

involved generates a new hash value for the block. Since, the hash value is a new value for the other nodes and thus the transaction can be considered as an illegal transaction.

The node involves a hash function that performs two functions. It generates a hash value for the node and then returns it. The previous hash value for the initial node is a null value while the consistency in the hash value of the current node being correctly displayed in the next node and the hash value of the previous node is being correctly displayed in the current node. This ensures that the block chain has been successfully created. The starting block is being referred as genesis block. In case the data has been modified the hash value of the modified block will display an error message showing that the block has undergone an unauthorized access.

Each block contains the hash value of its predecessor block in the chain. In case there is a mismatch of hash values the chain will be considered as an invalid chain. The block chain itself is considered as immutable i.e. the data once written on the chain cannot be modified and any new entry will require a new block to be created with a new hash value. Even if the data needs to be modified it has to be modified on the entire chain making it a difficult process altogether. Also the hacker will have to hash values of all the blocks within the chain in order to avoid detection.

Proposed Approach

In order to solve the various attacks associated with crowd sourcing the project uses the block chain as an efficient and powerful method. This fascinating technology brings a very notable feature along with it that is the transparency. The entire is duplicated across the whole network in order to maintain the consistency, thus data is available to the public. The block chain is a peer to peer network collectively following a per-defined consensus protocol. It acts as a public ledger where all the data is visible to the mass and any change in the data is reflected across the entire chain.

Each node in the peer to peer network enjoys the similar facilities as well as privileges i.e. they acts as both the consumer and supplier of the information. The main utilization of the

block chain technology in the crowd sourcing system is that any change doesn't go unnoticed so the data can be modified by authentic users only.

The chain also acts as a backup system so every node contains an instance of the data. In case of any unauthorized access at a certain node the data can be relayed through the other nodes while bypassing the affected node. So the regulation of the data is constant and is consistent. The transparency in all the transactions eliminate the problem of a middleman or an acting regulator.

The data is transmitted in encrypted form across the block chain with the possibility of adding additional cryptographic techniques to ensure data security. The hash value itself is generated using the cryptographic function SHA-256. In case a node is attacked other nodes can be used to check for the source of the attack or simply localize the source.

The block chain method is advantageous over the traditional method as a number of user or nodes act as a single unit. Each transaction or decision is taken as a collective decision such as smart contracts where each node submits its own response. The data present in a block chain is consistent, secure and transparent.

Need:

The main points associated with the block chain are

- Decentralized and distributed ledger storage technology
- The ledger is irreversible and rigid
- It is a real time system i.e. the transactions are in done and verified in real time which is an important factor in the crowd sourcing system
- It ensures the anonymity and privacy of the users as well the data involved

Crowd sourcing systems have been a victim of a plentiful amount of cyber crimes which mainly aims at compromising the data or to bring down the systems. In applications implementing crowd sourcing such as Uber there have been many cases of identity theft of the users or driver's personal data. In addition to this free riding and false reporting, in

order to avoid payments, are some forms of frequently occurring attacks on crowd sourcing systems. Thus there is a need of an efficient method to ensure the data security and utility of crowd sourcing platforms.

Each user in the block chain is identified by a digital identity and linking amongst these users is based on these digital identities without compromising the personal data of the users.

In systems involving smart contracts these digital identities can be quite useful so ensure privacy and to maintain the request worker relationship. Crowd sourcing involves a large number of people for its operations such as opinions on events, products etc. Block chain makes this possible thereby improving the quality of the overall process and the collected data.

Benefit:

The use of block chain in crowd sourcing is mainly due to its trustworthiness and the presence of a proper validation system along with ensured integrity of the data. The block chain system considers all the weaknesses associated with a crowd sourcing system while simultaneously increasing their application potential. The block chain database contains the complete, indelible, and immutable history of all the transactions, assets, and instructions executed since the very first one.

Using the block chain technology we eliminate the need of a central managing authority. The nodes supply the required information in return for a small reward. It is also beneficial in cases such as crowd funding. Equity crowd funding acts as new channel for raising money for startups.

Other benefits includes

- Transparency
All the data and nodes accessing the data are represented using digital identities which are visible to all the other nodes in the chain. All the transactions and computations are public for all the nodes.

- **Pseudonym**
The nodes are addressed with a pseudonym ensuring the anonymity of all the users. The hash of the nodes are generated in an encrypted form. Furthermore, the use of the digital signatures makes sure that one can send messages in the name of a block chain address, unless he has the corresponding key.

- **Reliability**
The data transferred across the block chain is received by all the connected nodes in the form of a validly signed transaction which is solicited by a block and written into the block chain. The multiple verification system helps in correct and authentic transmission of data across the block chain network.

- **Correct computation**
The block chain can be seen as state machine driven by messages within each block. Full nodes will persistently receive newly proposed blocks, and faithfully execute programs defined by current states with taking messages in new blocks as inputs. The result can reliably delivered to the entire chain.

- **Peer-to-Peer Network**
Block chain acts as a peer to peer network with each node acting as a peer or self operating system having same privileges as the other nodes. Each transaction requires validation from all the peers and each peer holds a copy of that transaction. This feature gives security and transparency while giving power to the users.

- **Immutable**
The immutable property of the block chain allows any unauthorized modification of the data present in the block chain. Each node contains the same data and any modification to the data will require repeating the same process throughout the entire chain. The nodes have a hash value associated with them and each

transaction creates a new hash value with it. This allows other nodes to detect then changed hash value. For a hacker, any modification will require him to change the hash values of all the nodes as each node contains the hash value or its previous node.

```

1 import java.nio.charset.StandardCharsets;
2 import java.security.MessageDigest;
3 import java.security.NoSuchAlgorithmException;
4 import java.util.Base64;
5 import java.util.Date;
6
7 public class Block {
8
9     private String version;
10    private Date Timestamp;
11    private String hash;
12    private String previousHash;
13    private String data;
14
15    public Block(String version, Date timestamp, String data) {
16        this.version = version;
17        this.Timestamp = timestamp;
18        this.data = data;
19        this.hash = computeHash();
20    }
21
22    public String computeHash() {
23
24        String dataToHash = "" + this.version + this.Timestamp + this.previousHash + this.data;
25
26        MessageDigest digest;
27        String encoded = null;
28
29        try {
30            digest = MessageDigest.getInstance("SHA-256");
31            byte[] hash = digest.digest(dataToHash.getBytes(StandardCharsets.UTF_8));
32            encoded = Base64.getEncoder().encodeToString(hash);
33        } catch (NoSuchAlgorithmException e) {
34            e.printStackTrace();
35        }
36    }
37
38 }

```

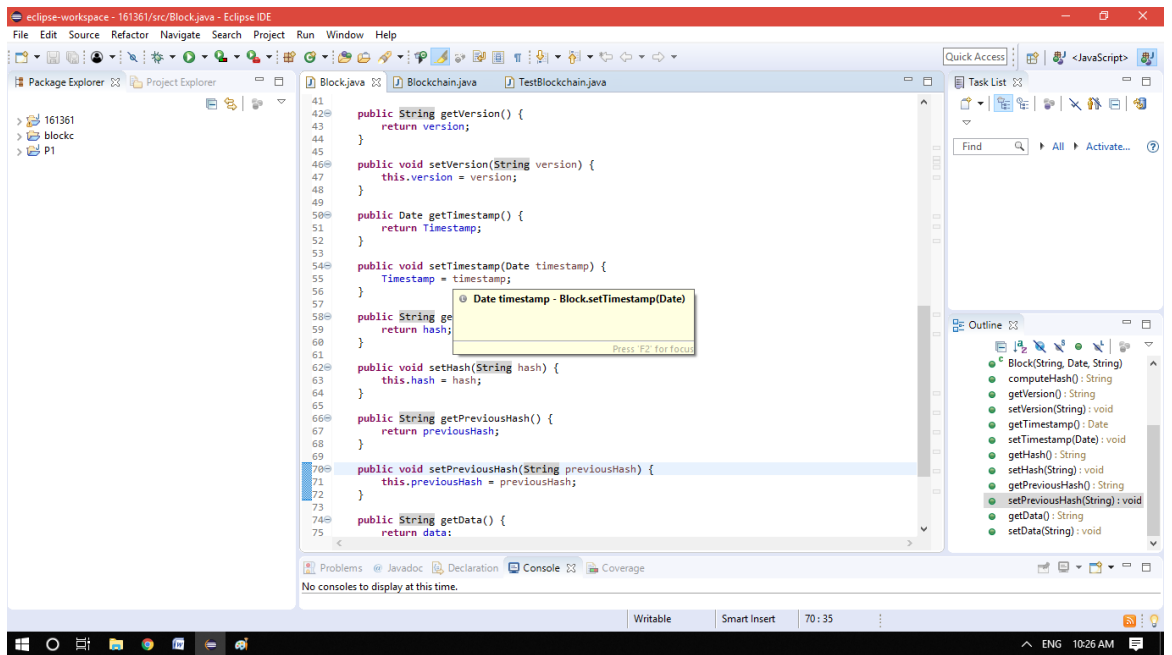
Initialization and hash computation method

```

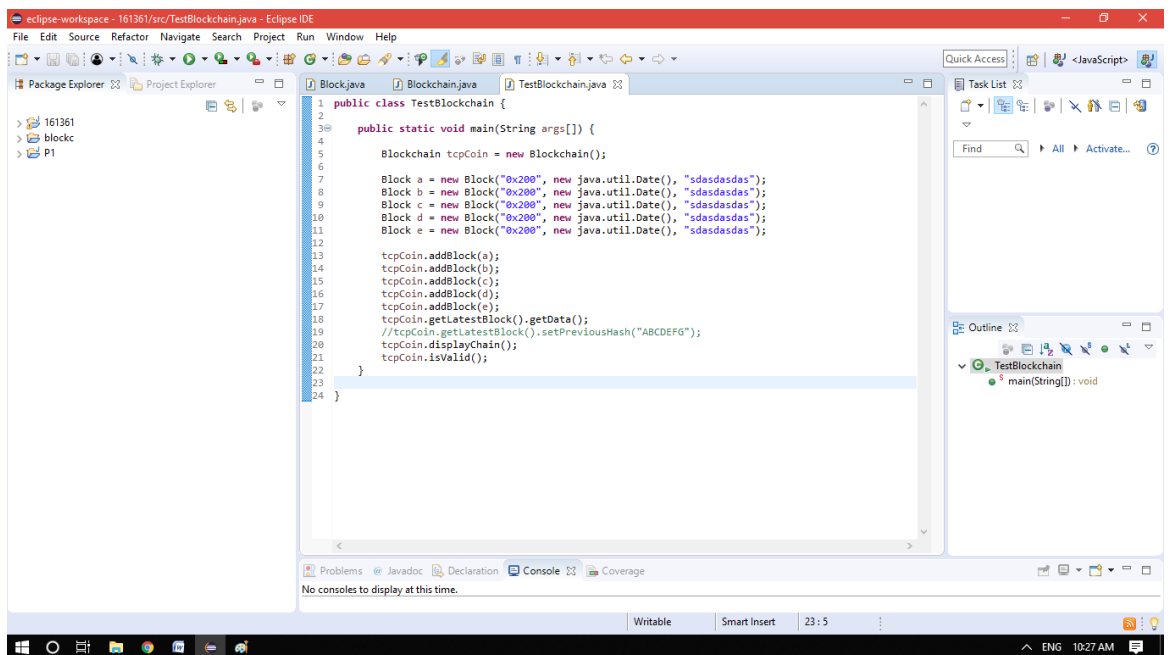
3
4 public class Blockchain {
5
6     private List<Block> chain;
7
8     public Blockchain() {
9         chain = new ArrayList<Block>();
10        chain.add(generateGenesis());
11    }
12
13    private List<Block> Blockchain.chain;
14
15    public Blockchain() {
16        chain = new ArrayList<Block>();
17        chain.add(generateGenesis());
18    }
19
20    public void addBlock(Block blk) {
21        Block newBlock = blk;
22        newBlock.setPreviousHash(chain.get(chain.size()-1).getHash());
23        newBlock.computeHash();
24        this.chain.add(newBlock);
25    }
26
27    public void displayChain() {
28
29        for(int i=0; i<chain.size(); i++) {
30            System.out.println("Block: " + i);
31            System.out.println("Version: " + chain.get(i).getVersion());
32            System.out.println("Timestamp: " + chain.get(i).getTimestamp());
33            System.out.println("PreviousHash: " + chain.get(i).getPreviousHash());
34            System.out.println("Hash: " + chain.get(i).getHash());
35            System.out.println("Data: " + chain.get(i).getData());
36        }
37    }
38
39 }

```

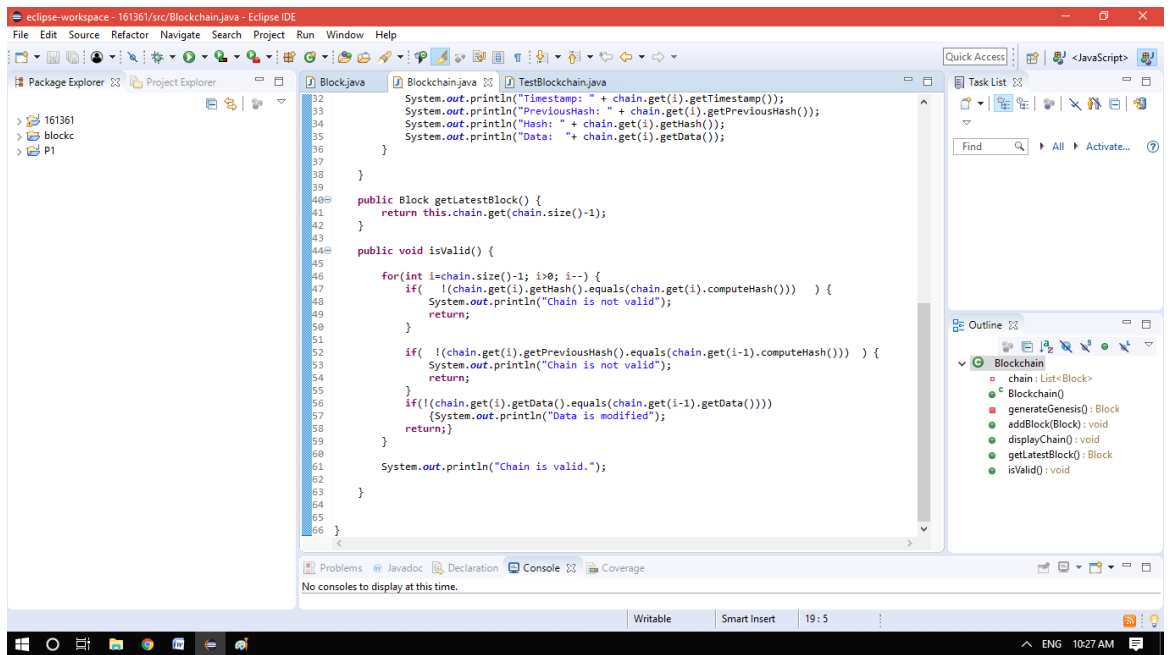
Genesis Block and display method



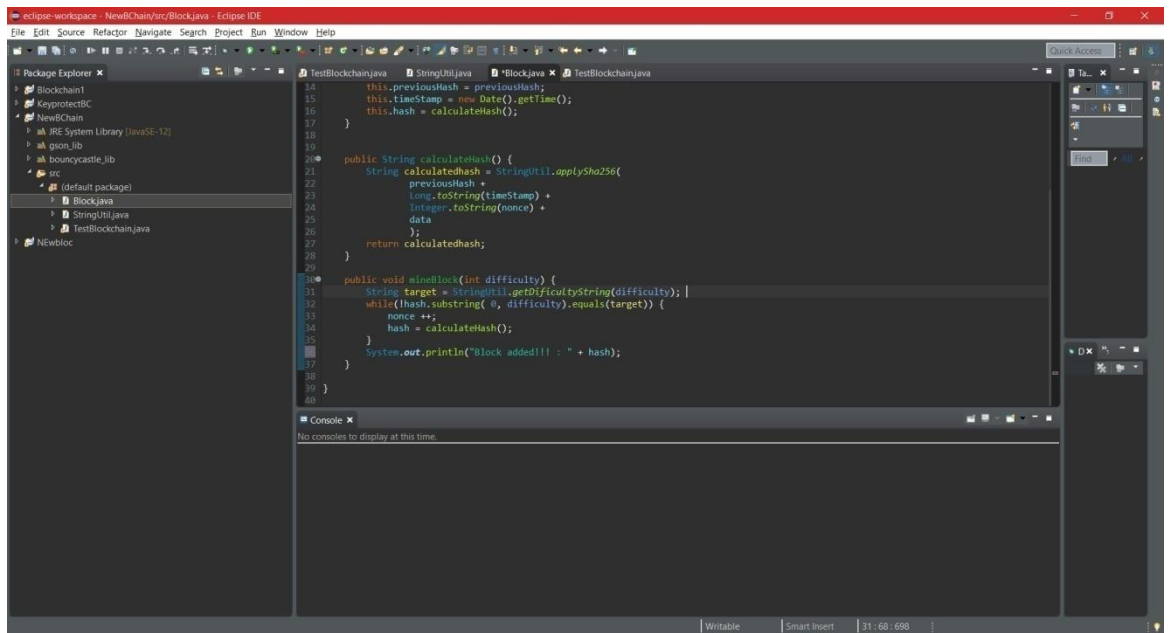
Getters and Setters for the blockchain



Blockchain creation



Chain validation



mineBlock method

Algorithm:

To construct a block chain

- Define parameters timestamp, hash, previous hash and data
- Define a compute hash method
- Generate a hash value for a block using SHA-256
- Declare getters and setters
- Set an array list for the chain
- Create a genesis block
- Pass the parameters in the genesis block
- Compute hash for the genesis block
- Create an add Block method
- Compute the hash for the block and retrieve the hash of the previous block in the chain
- Add the block to the chain
- Create a display method and pass the parameters of the block
- Create the blocks by creating objects of the main class and using the addBlock method

To verify the validity of chain

- Create a method getLatestBlock
- Change the previous hash value for the block
- Create a method to validate the hash values
- If the previous hash values are equal the valid message is displayed

To check for validity of data

- Modify data in any of the block
- A message will be displayed saying data has been modified

For the DoS attack or Spamming in a blockchain

- Create a new mineBlock method
- The mineBlock method takes a difficulty value as its parameter.
- The mineBlock method works such as it generates a hash with a number of 0's appended to the hash of the block i.e. equal to the difficulty.
- The hash value is then calculated such that the inputs to cryptographic hash function should generate a hash with the appended 0's.

The challenge and the proof of challenge take several computing cycles to generate such an input in order to give out the determined output. This is a brute force method and will require all possible combinations. A malicious user will require a computing power greater than the combined power of the nodes on the chain.

Chapter 4

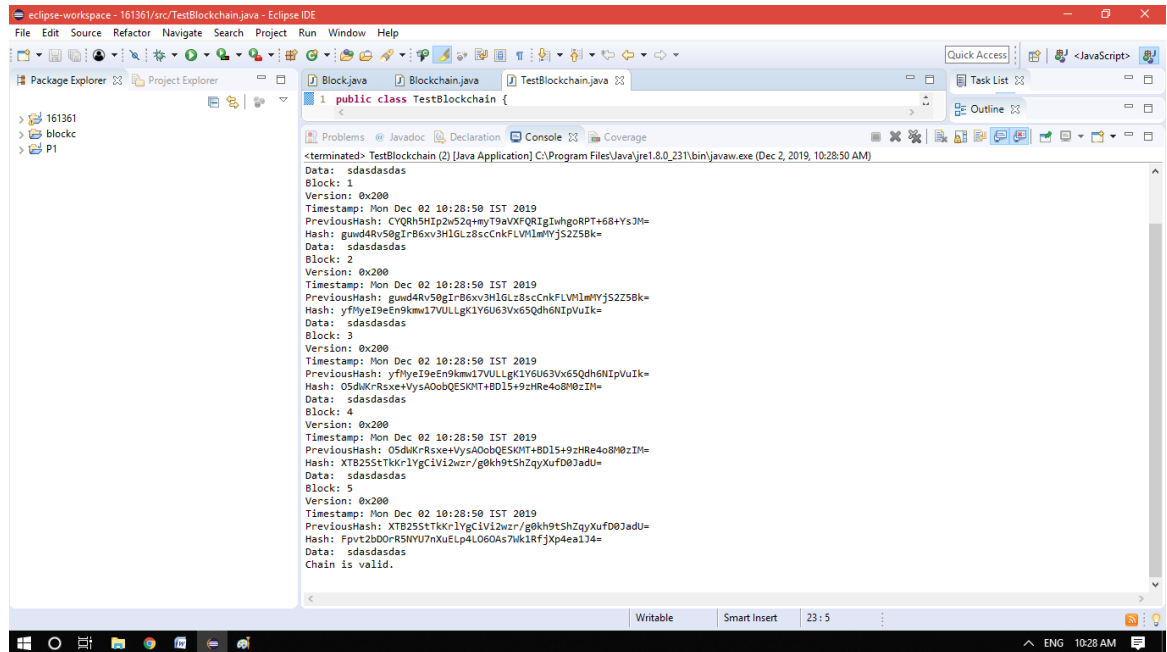
Performance Analysis

The block chain process is far more better than the primitive method of data collection in crowd sourcing as it protects the data as well as the users form any kind of malicious attacks. The efficiency of the block chain is better as it requires lesser number of computation steps thereby creating a lighter system to collect data. In terms of the privacy the block chain can be accessed only by the users present in the block chain, plus the digital signature method needs verification from all the members of the chain to process any transaction.

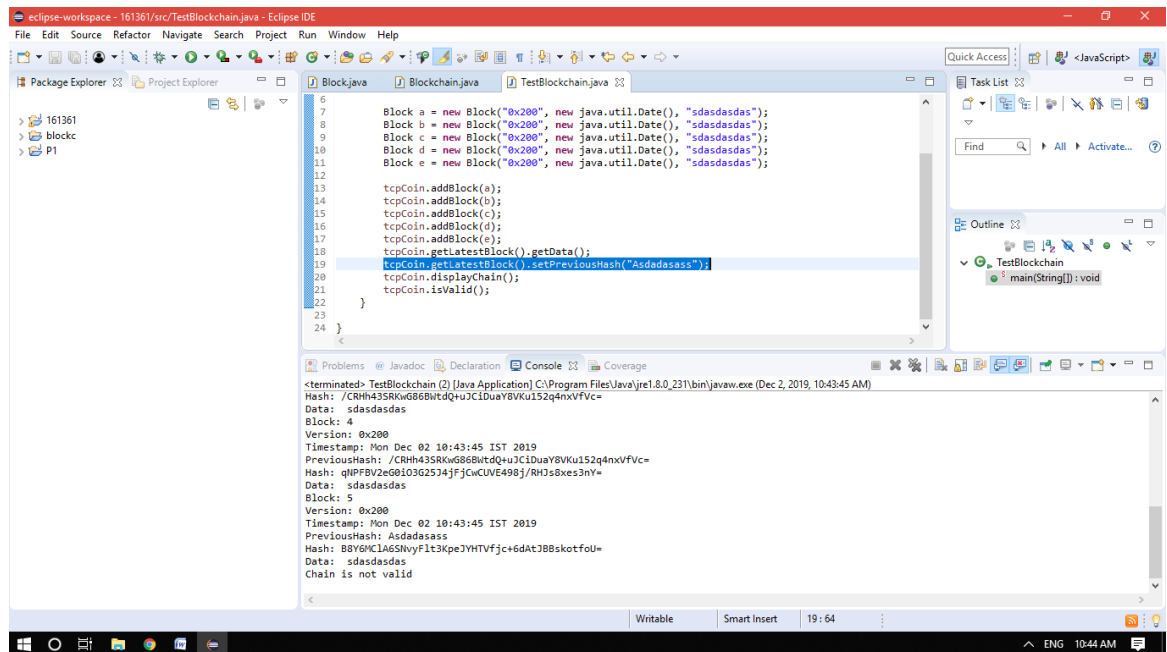
For the performance analysis of the method we make a different number of nodes and subject them to the various kinds of attacks present in the crowd sourcing workspace. We will further in this project take the performances of the system and then compare them with the ones when the nodes were in the form of block chains and whether we were able to counter the problems associated with the system. The attacks associated are denial of service, message alteration, false report, falsification attack etc. These attacks mainly aim at either rendering systems unavailable or to present false data. Block chain method can be beneficial in number of real world scenarios such as fake news detection, smart contracts that are verified through various peers and act without any intervention.

It increases the quality of journalism and helps in recruitment process for various kinds of product testing and their responses. The only disadvantage associated with the block chain method is the overall energy consumption neither through the data collection process nor through the verification process. Each transaction involves a number of nodes and permission from these nodes. The process can require a large amount of energy but can be significantly lowered by using algorithm involving a number of ledgers associated with each node. Each node uses multiple routes for these ledgers while decreasing the cost for the process.

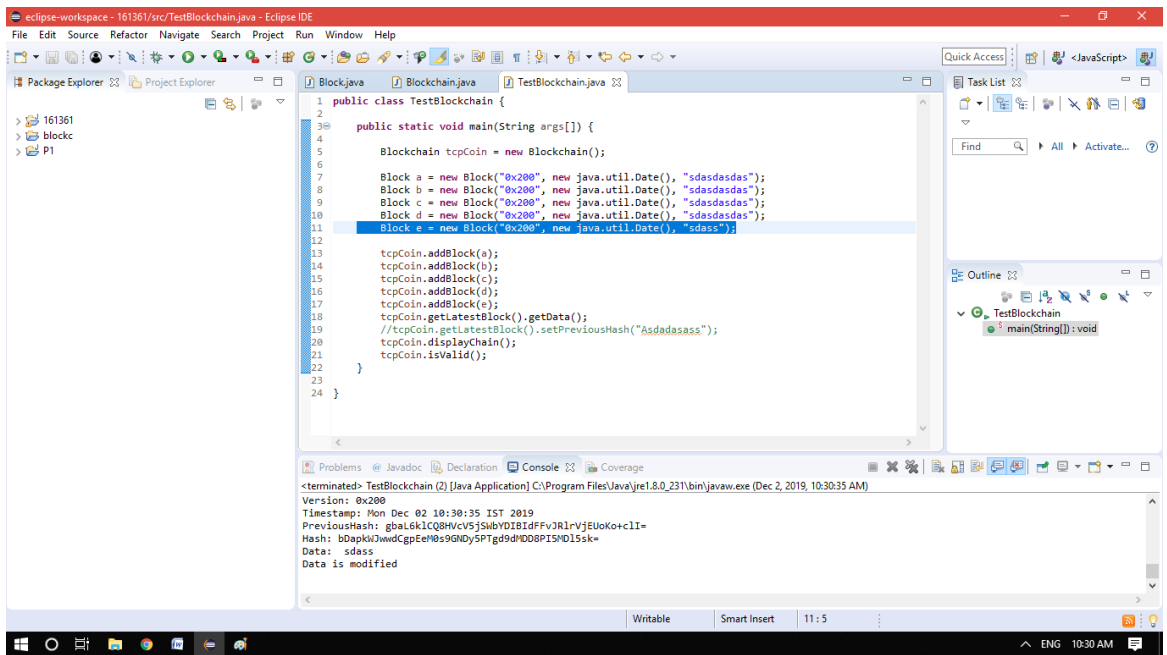
Attacks often include clogging up the network or leaking the data or even modifying the data. The proposed system ensures that the data that reaches its destination is the one that was intended and is precisely on time.



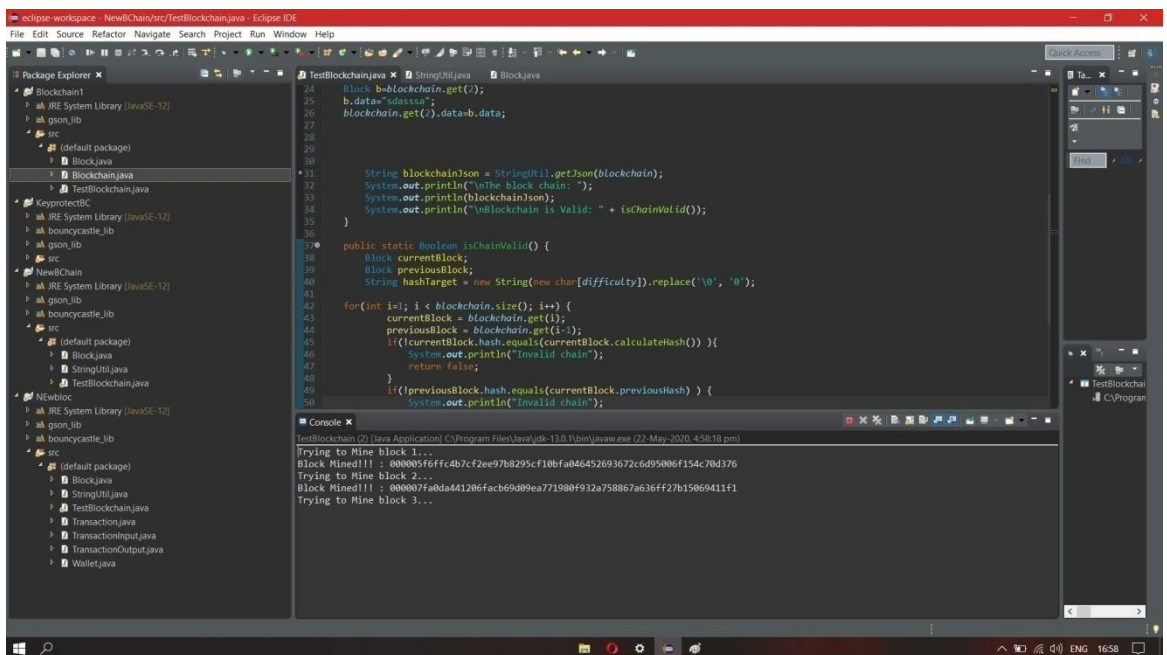
Blockchain with hash values



Invalid Chain



When data is modified



Adding block to the blockchain

ATTACKS:

- Denial of Service:

Denial of service means to bring down a system or to prevent a system from providing results to any of the queries it receives. Denial of Service is generally done through exposing the network to a huge amount of traffic in a centralized system the network is managed through a single controller and any authorized to the controller could compromise the entire network. Even with state-of-the-art encryption techniques the centralized systems are vulnerable in one way or another. In DoS a system receives multiple requests or messages or in case of a network a server.

The blockchain method helps to counter this problem as there is no need for a centralized system in a blockchain. Blockchain involves a number of users or nodes each enjoying the same level of privilege and each transaction needs verification from these nodes. This removes the need for a central authority as each node acts as a peer in the network. The devices associated within the network will require a cryptographic authentication key for communication and the extra traffic cannot be introduced.

Blockchain method uses private keys for any kind of modification within the network and in case any key logs the login request is available for all the other nodes to be seen. Since, blockchain itself acts as a peer to peer network, any hacker will need an access to all the nodes within the network making it practically impossible. Several companies are using the blockchain method to transfer bandwidth to server that is currently under attack. The extra bandwidth then helps the server to withstand the attack.

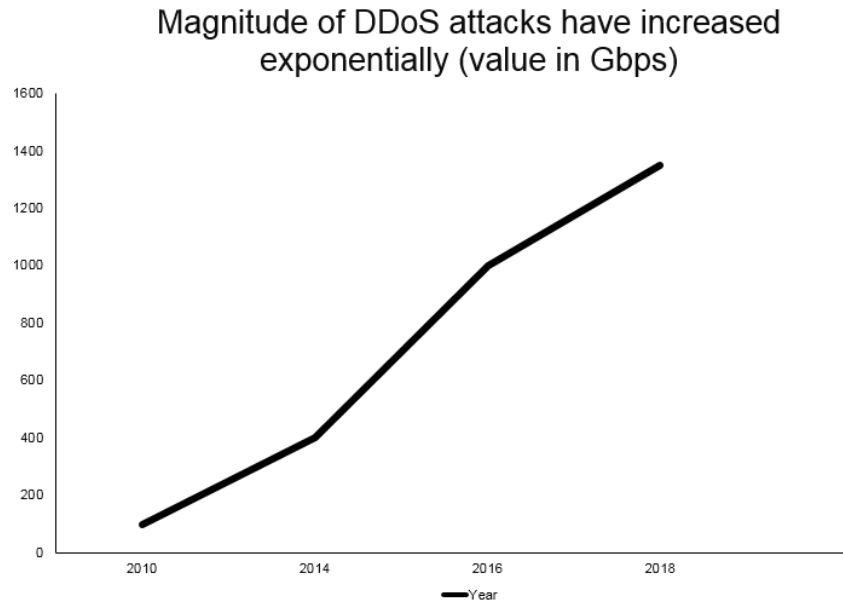


Fig. 4.1: Graph representing DDoS

Blockchain can completely eliminate the DoS problem by replacing the use of existing servers or the client-server architecture model with the P2P nodes. The data can be fragmented and stored on a large number of nodes connected to each other. Multiple cases have been reported such as 5050 skatepark, rokenboketc where the main reason for the attack was inadequate security measures. The DoS attacks can cause a large amount of damage to systems or businesses such as banks or stock markets.

- **Message Alteration:**

Another major attack associated with the crowdsourcing method is message alteration. The hacker intercepts the message during transmission and modifies it either in small amount or completely. The attacker then can either transmit the message to its destination or change its destination path. The attacker sometimes delays the message so that the message produces an unauthorized effect. The introduction of blockchain can prevent this type of attack.

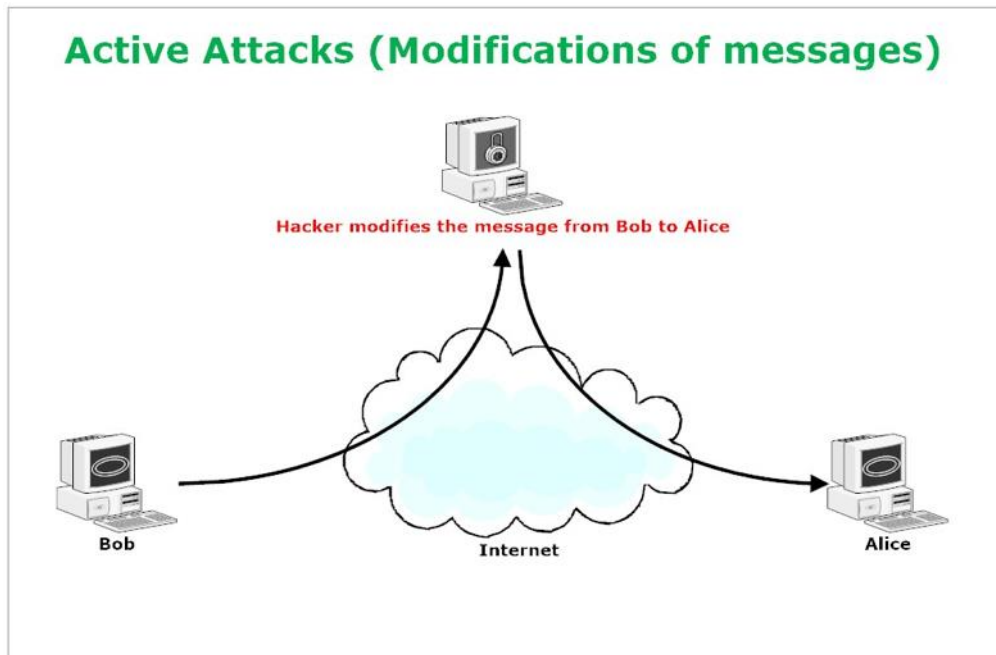


Fig.4.2: Active attacks

The transactions need an authentication form all the nodes connected to the network and each block or node has an encrypted hash value. Each transaction within the network gets its own hash value and the instance of the transaction is received by all the nodes. Each node contains the duplicated data so each node can verify any change in the data done by any attacker. Furthermore, the modification itself will generate a new hash value for the transaction which will be easily detected by the other nodes within the network.

The Free-riding and the False reporting in crowd sourcing of mobile is based on the auction theory. So starting with a brief introduction of the Auction theory this report will explain the above-mentioned terms.

The Auction Theory:

The Auction is an effective and an efficient method in the field of markets which deals in trading, with their benefits in finding the whole item-price of tasks or products for the

people who like to buy and people who like to sell. The Auctions also involve the one-to-one communication with a large number of gathered people and are known as the Double Auctions. While determining the cost prices for both the parties, there is a constant fear that all the prices might be changes and hampered according to individual to make this market free and vulnerable to individuals who are dishonest i.e. buyer and sellers. Many economics property, such as being truthful, budget-balance, rationality, computationally efficient.. These are explained below:

- Property of Truthfulness: auction is truthful for both the parties i.e. buyer or seller if and only if no such utility could achieve which is higher than the previous one by reporting an amount deflection from its original value of the bid or to ask from another individuals present in the auction.
- Individual's Rationality: Auction is dependent on individual rationality if for any receiver or seller; it will not get utility which will be further considered negative by leaking its original value or amount paid to the trading units.
- Budget-balancing: auction is known as budget balanced only if person presenting the auction always makes a profit which is positive..
- Computationally Efficient auction: This will be computationally efficient and effective in process if the auction can be conducted within bounds of poly-nomial time.

The Free-Riding technique and The False-Reporting technique in Crowd-sourcing:

The truthful and the precision of auction can be prevented by an individual's personal benefit from not speaking the truth on the prices of the products. False reporting and free riding, which are related to each other closely whenever the amount is paid and the service provider gets their money. This makes the process so open to dishonest people who provides services and the people making requests to make personal benefits.

If the amount of the product is paid after the work is complete, a service-provider may have incentives to have the payments from the customer and give no equal work to get the solution of the given task, and is generally known as "free riding". And on the other

hand, the whole amount is paid after the work is being done, the person asking may always have the incentives to equally deny the payments by speaking lie about the outcomes and results of the work and this is known as false-reporting. Some extra precautions are always needed. Many of the ongoing and current works are focusing on avoiding freeriding and false-reporting by making up the reputations systems or gradings software for both the trading parties. These mechanisms may result in discouraging such dishonest behaviours of the trading people overall, but when we consider assumptions it seems that all individual are patient in nature and would definitely stay. And talking about reality, some of the dishonest individual and trader may only reside in system for a small span of time according to their personal benefits, and get rewards for being not honest. On the other hand, many non patient user may leave platform again for their personal benefit.

Privacy Threats:

The flow of data in just sensing the tasks which are different from the one used in computation tasks in MCN. Talking about sensational tasks, the data is first sensed by the sensing-crowd and then transferred to the services providers and stores the system which is managed by the service provider or sent to end-users. And in computing tasks, the input data may come from different sources, for e.g., the system is being managed by the service providers and the storage systems is managed from the end-users, storage systems is also purchased by end-users or the service providers, sensor-enabled mobile devices, and many more. The output of computing tasks are sent back to the service provider first and then finally to the end users after the task re-composition is being done.

- Privacy of senses data
- Privacy of computing inputs
- Privacy of computing results
- Privacy threat from tasks
- Task privacy of participants

Reliability Threats:

In MCN a crowd-sourced task can be accepted by anyone a mobile device or a computing devices. Due to the task crowd-sourcing and humans involvements in this process, it is immensely difficult to guarantee each and participant to provide reliable data or computing results. These are some the reliability threats:

- Reliability of Sensed Data
- Reliability of Computing Results
- Reliability of Transmission

The availability threats:

The extensive research had been done on some denial of service (DoS) problems for classic networks within the literature, such as network congestion because of message floods. Several different and unique DDoS problems are raised due to task crowd-sourcing

- DDoS by Malicious Participants: some dishonest participants may accept all of the crowd-sourced duties but refuse to provide valid consequences or even forget about their duties. This may also cause the DDoS where legitimate crowd-sourcing members cannot get any duties considering that the total quantity of crowd-sourced obligations and must-do duties are usually constant.
- DDoS by Honest but Selfish Participants: a DDoS assault may additionally occur even if all the individuals are honest. For instance, a participant who's egocentric and hopes to get hold of extra rewards may additionally accept all of the computing responsibilities and complete them over a long term length because of its confined computation skills. This can even put off the benefit of numerous individuals in crowd-sourcing as the consequences are from the identical person.

51% attack:

A 51% attack refers to a user or multiple users in the blockchain trying to take over the blockchain by controlling than 50% of the chain or its computing power. The users in control of the blockchain can now block new transactions from initiating or being confirmed. The 51% percent attack can alter the nodes by not allowing the correct answer to the proof-of-work.

The users in a network need to solve a particular puzzle in order to add data to the blockchain. The malicious users on the other hand can solve the puzzle and can keep an own copy of the blockchain. The blockchain generally accepts the chain with longest computing power. The malicious user with a control over the 51% percent of the blockchain can add blocks to his own version of the blockchain at a much faster rate and can later broadcast it over the network. The new chain is now accepted as the legitimate chain and the original chain has now been replaced with the corrupt one.

Sybil attack:

A Sybil Attack is an attempt to manipulate a peer-to-peer network by creating multiple fake pseudonym accounts. All the other users in the blockchain consider these different fake identities as regular users, but in fact, a single user is in charge of all these fake entities altogether. This type of attack is important to consider in manners involving online consensus or voting. Social networking platforms are also vulnerable to these Sybil attacks as they can create multiple fake accounts and influence public discussions or forums.

Sybil attacks can also censor other users in the network. Malicious attackers can surround the user and prevent it from accessing the network or receiving any data. This form of Sybil attack is known as an “Eclipse attack”.

Selfish mining attack:

Selfish mining attack refers to an attack on the blockchain's integrity by a malicious user. Selfish mining attacks occur when a user within the network tries to withhold a successfully validated block from being broadcast to the rest of the users within the network. After the attacker is successful in withholding their successfully mined block from the rest of the users, they continue to mine the next block, resulting in the selfish miner having demonstrated more proof-of-work as compared to the other users within the network.

A solution is to determine the timestamp of the block on which it was added to the blockchain. In case any user adds multiple blocks to the blockchain then the rest of the users on the network would validate those blocks against the timestamp on which they were hashed and the timestamp on which they were reported to the network.

Chapter-5

Conclusion and Future work

In this project, we have designed a blockchain based framework for mobile crowdsourcing. We analyzed that the traditional mobile crowd sourcing system suffers from privacy disclosure, single point of failure and high services fee, security attacks and various threat associated to it.

Crowd sourcing has emerged as an effective and useful way to perform tasks that are easy for humans but remain difficult for devices. Many solutions to various tasks using end workers has become increasingly popular in recent years. This trend enables individuals to sense, collect, process and distribute data around the users at any time and place all over the world. Naturally, The mixing smartphone based mobile technologies and crowdsourcing offers vast resources of computation and calculations which is collectively known as called Mobile Crowdsourcing (MCS). MCS sensing is an emerging area of interest, as smart phones are becoming the basic communication devices in people's everyday lives.

So, we created a basic chain of blocks also called as nodes and how by changing the hash of one block can make to differ with the hash of previous block. We have described how the various nodes are connected to each other as list of records where each node contains a timestamp, hash of previous block and information or data. If any message alteration or any other security threat occurs in any block of the blockchain it can be easily detected using blockchain technology in mobile crowdsourcing which was earlier a limitation in mobile crowdsourcing when no security was provided to it.

The DoS attack or the spamming attack can be resolved using the concept of proof-of-work in the blockchain. The proof-of work concept involves a challenge and a solution to

the challenge such that any user that needs to add a block to the blockchain must provide the solution to the challenge. This takes several computing cycles as the solution can be generated using only brute force method and a malicious user won't invest such energy in the attack. It also makes sure that blocks to the blockchain are added in a specific interval and the blockchain is not spammed. The digital signature can verify that each transaction in a blockchain is made by a valid user and can be validated by other users in the blockchain. The digital signature involves a user's private and public key. The secret private key is used by a user to digitally sign a message or generate a signature. The signature can then used along with the public key of the user to validate the authenticity of the sender. The signature for a message depends on the message itself and any change in the message will alter the signature.

The 51% attack can be resolved by using a penalty system for the blockchain. Any delayed addition to the blockchain will cost the user and will prevent a user from adding multiple blocks at once.

The Sybil attack can be solved using a cost factor to add users in the blockchain. Each new user identity will be associated with a certain cost. The cost should be balanced in such a way that it is low enough for new users to access the network but high enough so that multiple identities in a short period of time cannot be created.

In future, we see mobile crowdsourcing as an expanding and mainly utilized technology in many organisations to perform their projects. We see a larger number of people associated with and using it as the main platform to generate data collectively.

References :

1. J. Howe, "The rise of crowdsourcing," *Wired magazine*, vol. 53, no. 10, pp. 1–4, Oct. 2006
2. H. Zhu and Z. Z. Zhou, "Analysis and applications of blockchain technology," *crowdsourcing Innovation*, vol. 2, no. 1, p. 29, 2016.
3. R.K. Ganti, F. Ye, H. Lei, "Mobile crowdsensing: current state and future challenges", *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32-39, 2011.
4. Y. Wang, Y. Huang, C. Louis, "Respecting user privacy in mobile crowdsourcing", *SCIENCE*, vol. 2, no. 2, 2013.
5. B. Guo, Z. Yu, X. Zhou et al., "From participatory sensing to mobile crowd sensing", *Proc. of PERCOM Workshops*, 2014.
6. M. Allahbakhsh, B. Benatallah, "Quality control in crowdsourcing systems: Issues and directions", *IEEE Internet Computing*, vol. 17, no. 2, 2013.
7. K. Farkas, A.Z. Nagy, T. Tomás, T et al., "Participatory sensing based real-time public transport information service", *Proc. of IEEE PERCOM Workshops*, 2014.
8. F. Fuchs-Kittowski and D. Faust, "Architecture of mobile crowdsourcing systems," in *Collaboration and Technology (Lecture Notes in Computer Science)*, N. Baloian, F. Burstein, H. Ogata, F. Santoro, and G. Zurita, Eds. Cham, Switzerland: Springer, 2014, pp. 121–136.
9. B. Guo et al., "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 7:1–7:31, Aug. 2015.
10. M. Hamilton, F. Salim, E. Cheng, and S. L. Choy, "Transafe: A crowdsourced mobile platform for crime and safety perception management," in *Proc. IEEE Int. Symp. Technol. Soc. (ISTAS)*, May 2011, pp. 1–6.
11. S. Ruiz-Correa et al., "SenseCityVity: Mobile crowdsourcing, urban awareness, and collective action in Mexico," *IEEE Pervasive Comput.*, vol. 16, no. 2, pp. 44–53, Apr. 2017
12. S. Ruiz-Correa et al., *UrBis: A Mobile Crowdsourcing Platform for Sustainable Social and Urban Research in México*. Cham, Switzerland: Springer, 2018, pp. 19–37.

13. S. S. Kanhere, “Participatory sensing: Crowdsourcing data from mobile smartphones in urban spaces,” in Proc. IEEE 12th Int. Conf. Mobile Data Manage., vol. 2, Jun. 2011, pp. 3–6
14. B. Guo, Z. Yu, X. Zhou, and D. Zhang, “From participatory sensing to mobile crowd sensing,” in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops), Mar. 2014, pp. 593–598.
15. D. Geiger, M. Rosemann, and E. Felt, “Crowdsourcing information systems: A systems theory perspective,” in Proc. Australas. Conf. Inf. Syst. (ACIS), Sydney, NSW, Australia, 2011, pp. 1–12.
16. W. Yufeng, J. Xueyu, J. Qun, and M. Jianhua, “Mobile crowdsourcing: Framework, challenges, and solutions,” *Concurrency Comput., Pract. Exper.*, vol. 29, no. 3, p. e3789, 2016.
17. R. I. Ogie, “Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: From literature review to a conceptual framework,” *Hum.-Centric Comput. Information Science*, vol. 6, no. 1, p. 24, Dec. 2016.
18. R. K. Ganti, F. Ye, and H. Lei, “Mobile crowdsensing: Current state and future challenges,” *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 32–39, Nov. 2011.
19. E. Harburg, Y. Kim, E. Gerber, and H. Zhang, “CrowdFound: A mobile crowdsourcing system to find lost items on-the-go,” in Proc. 33rd Annu. CHI Conf. Hum. Factors Comput. Syst. CHI Extended Abstr. Publication, vol. 18, 2015, pp. 1537–1542.
20. N. Kaufmann, T. Schulze, and D. Veit, “More than fun and money. Worker motivation in crowdsourcing—A study on mechanical turk,” in Proc. Amer. Conf. Inf. Syst., 2011, pp. 1–12.
21. E. Schenk and C. Guittard, “Towards a characterization of crowdsourcing practices,” *J. Innov. Econ. Manage.*, vol. 7, no. 1, pp. 93–107, 2011.
22. G. Barbier, R. Zafarani, H. Gao, G. Fung, and H. Liu, “Maximizing benefits from crowdsourced data,” *Comput. Math. Org. Theory*, vol. 18, no. 3, pp. 257–279, Sep. 2012.

23. T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma, "PRISM: Platform for remote sensing using smartphones," in Proc. 8th Int. Conf. Mobile Syst., Appl., Services (MobiSys), 2010, pp. 63–76.
24. N. Agarwal, S. Chauhan, A. K. Kar, and S. Goyal, "Role of human behaviour attributes in mobile crowd sensing: A systematic literature review," Digit. Policy, Regulation Governance, vol. 19, no. 2, pp. 168–185
25. X. Peng et al., "CrowdService: Optimizing mobile crowdsourcing and service composition," ACM Trans. Internet Technol., vol. 18, no. 2, pp. 19:1–19:25, Jan. 2018.
26. C. Qiu, A. C. Squicciarini, B. Carminati, J. Caverlee, and D. R. Khare, "CrowdSelect: Increasing accuracy of crowdsourcing tasks through behavior prediction and user selection," in Proc. 25th ACM Int. Conf. Inf. Knowl. Manage. (CIKM), 2016, pp. 539–548.
27. L. Schmidt, "Crowdsourcing for human subjects research," in Proc. CrowdConf, San Francisco, CA, USA, Oct. 2010, pp. 1–7.
28. Y. Tong, L. Chen, and C. Shahabi, "Spatial crowdsourcing: Challenges, techniques, and applications," Proc. VLDB Endowment, vol. 10, pp. 1988–1991, Aug. 2017.
29. J. Wang, Y. Wang, D. Zhang, and S. Helal, "Techniques in mobile crowd sensing: Current state and future opportunities," IEEE Commun. Mag., vol. 56, no. 5, pp. 164–169, May 2018.
30. Y. Chon, N. D. Lane, F. Li, H. Cha, and F. Zhao, "Automatically characterizing places with opportunistic crowdsensing using smartphones," in Proc. ACM Conf. Ubiquitous Comput. (UbiComp), 2012, pp. 481–490.