Blockchain Applications for Disaster Management and National Security

by

Mohit Singh Panesir

June 1st, 2018

A thesis submitted to the

Faculty of the Graduate School of

the University at Buffalo, State University of New York

in partial fulfillment of the requirements for the

degree of

Master of Science

Department of Industrial and Systems Engineering

This page intentionally left blank

DEDICATION

This thesis work is dedicated to my parents Jaswinder Singh and Balveer Kaur, who never stop giving of themselves in countless ways and believing and supporting me with all my decisions. My sister, Sonal Singh, for showering me with all her love and blessings. My friends, Jasleen Kaur Dhanoa and Jerry Shaji Punnoose for giving me hope when I was lost and of course Wendy's for the 4 for 4.

ACKNOWLEDGEMENT

It is not a fair task to acknowledge all the people who made this thesis possible with a few words. However, I will try to do my best to extend my great appreciation to everyone who helped me scientifically and emotionally throughout this study.

I would like to acknowledge my indebtedness and render my warmest thanks to my supervisor, Dr. Jun Zhuang, who read my numerous revisions and helped make some sense of the confusion and made this work possible. His friendly guidance and expert advice have been invaluable throughout all stages of the work. I would also wish to express my gratitude to Dr. Bina Ramamurthy for extended discussions and valuable suggestion which has contributed greatly to the improvement of the thesis.

Special thanks to my manager at Rich Products Corporation, Mr. Jeffrey Stevens and my colleagues for being supportive and understanding about my work and being extremely enthusiastic and excited about this study. The people with the greatest indirect contribution to this work are my parents, Jaswinder Singh and Balveer Kaur, my sister Sonal Singh and Jasleen Kaur Dhanoa, who has taught me to believe in my work and me, provided constant encouragement and always offering support and love.

This thesis has been written during my stay at the Industrial and Systems Engineering department at the University at Buffalo, the State University of New York. I would like to thank the staff, all the professors and every member of my research group for providing feedback, encouragement and excellent working conditions.

ABBREVIATIONS

PoW: Proof of Work

PoS: Proof of Stake

PBFT: Practical Byzantine Fault Tolerance

DPoS: Delegated Proof of Stake

WHO: World Health Organization

FEMA: Federal Emergency Management Agency

WMD: Weapon of Mass Destruction

UNO: United Nations Organization

DHS: Department of Homeland Security

CBP: Custom and Border Protection

EMDAT: Emergency Management Database

KYC: Know your customer

AML: Anti Money Laundering

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Natural phenomena such as floods, storms, volcanic eruptions, earthquakes, landslides have affected our planet in an unpredictable way. However, these phenomena are merely classified as a hazard when they may affect people and the things they value (Cutter, 2005). The involvement of many agencies and the public is important in planning for disaster relief, in rescuing victims, and in managing the event. A lot of individuals are deprived of help due to poor coordination, late assistance and uneven distribution of food, water, medical assistance, clothes, and vehicles. The need for a proper disaster relief plan is crucial to overcome these challenges. On the other hand, identity theft is one of the most bizarre and rapidly growing crimes present in the world. Identity thieves are active more than ever as the e-commerce trading keeps on growing. Earlier the thieves used to buy pieces and parts of someone's personal identification information but now they could have hold of everything. Similarly there has been an increase in illegal immigration, smuggling of weapons and terrorist activities noticed in last 2 decades in the United States. This study focuses on the current condition of disaster management, identity theft, border security and controlling the misuse of weapon of mass destruction. It proposes the use of advanced technological methods like Blockchain to overcome the loss of time and cost to provide a quick response to the victims and to provide secure ways to store personal identification information and better national security. The study helps to understand how better disaster management and national security can be achieved by using various use cases and implementation models. By implementing these models, the border security can be improved and proper handling of weapons of mass destruction can also take place.

CHAPTER 1

INTRODUCTION

One of the most prominent scholars in disaster research, Quarantelli, emphasized that whenever we want to research or discuss the consequences of any phenomenon, we need to have a clear idea of what that phenomenon is (Quarantelli, 1985). 50% of the problems in the world result from people using the same words with different meanings. The other 50% comes from people using different words with the same meaning. (Kaplan 1997) To describe and classify disastrous events, researchers have proposed a hierarchy of terms generally taking into account organizational involvement (Quarantelli, 1985). Unfortunately, the conundrum of definitions often creates disagreement and confusion (Perry, 1989). After carefully examining various definition for disaster through extensive study of literature, we use the following definition of disaster fits perfectly with the scope of this study: 'A disaster is an event, which is caused by natural or man-made agents, which disrupts a large number of living organism in a society in such a way the available resources and local emergency capacities are unable to provide effective help to the affected population.

Providing effective rescue operations and disaster management is one of the major ways of reducing the devastating outcomes of the crisis situation. Emergency management, which is defined as the discipline and profession of applying science, technology, planning, and management to deal with extreme events which are called disasters (Drabek & Hoetmer, 1991) is the main component of providing relief in such conditions.

When it comes to identity theft, it is one of the rapidly growing crimes taking place at this point in time. Identity theft has a simple definition which lies with the scope of this study, The usage of someone else's identification information for various purposes without the permission or knowledge of the respective owner is termed as identity theft. Most of the times the people targeted by the identity thieves are unaware of their identity being stolen for months until they get a bill or a receipt of unauthorized transactions or a criminal case against their name. "The imagination and creativity of a human when it comes to stealing things are endless," (Keane, Papadimitriou, 2017) which implies that there are various methods that the identity thieves are using to steal important data.

Motivation

The major drawback of preparing for the disaster is that we can only predict how severe it is going to be and how many individuals and a group of people will get affected by it. So, at times it becomes difficult to provide proper rescue operations, communication amongst the family members, proper medical help, provision of food, water, medicines and shelter as the condition may be more severe than what was predicted. The main focus of the study is to develop a model providing a way of the transaction which is safe, secure and fast which eventually leads to a reduction in losses due to corruption, improper handling of assets, information and data. In the last few decades, we have seen an increase in the number of disasters taking place in the world, leaving a huge amount of people struggling for basic needs of life. The National Oceanic and Atmospheric Administration claimed that 2017 was the costliest year on record for natural disasters in the United States with a price tag of at least $306 billion (National Oceanic and Atmospheric Administration, 2017).

The relief and rescue operation during such events are scattered and ineffective because of an improper relay of information and utilization of funds. According to government executive's web page; A congressional committee is investigating potential abuse of federal funds and resources provided to local municipalities in Puerto Rico, citing red flags raised by the FBI (Katz, 2017). With such a huge amount of residents left in grave need of basic supplies, it is essential that the assistance from the federal government is provided in the most efficient and effective manner possible. But such cases of corruption, where the funds are rather used by a specific group of officials for their personal benefits are a matter of deep concern.

On the other hand, when it comes to identity theft there has been a huge increase in the severity and the frequency of the crime. According to the 2017 Identity Fraud Study, released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion and 13.1 million victims a year earlier. In the past six years, identity thieves have stolen over $107 billion. Identity theft tops the list of consumer complaints that are reported to the Federal Trade Commission and other enforcement agencies every year. The identity thieves use various techniques of stealing the information but lately they have been targeting big companies from where they can get an abundance of data and information at once which they can use and would be difficult for the respective owners to recover from and as the number of complaints would be higher it would be difficult for the organization dealing with the complaints to work efficiently as the number of complaints would be high. The victims of identity theft fraud often have to go through a long and frustrating road to recovery. Depending on the severity of the identity theft fraud damage, the recovery process can take up to years.

This attack affects the credit score of the victim and makes it extremely difficult for them to obtain loans and finding employment (Insurance information institute). This study provides a better understanding of the topics like disaster management and identity theft and methods of providing secure and safe storage and transaction of information, finances and, data.

Research questions

In this study, we developed different models using blockchain network concepts and utilized its ability to store information and data safely and making the transaction secure and anonymous. These models are further utilized in the process of providing better communication between two parties during a disastrous situation and using these models in order to provide secure storage of private information by the respective organization. We have also focused on the ways to provide more efficient National Security using emerging techniques like Blockchain.

More specifically, this study is interested in the following research questions:

- What is blockchain and how does it work?
- Can a blockchain network provide better disaster management?
- Can a blockchain network be used for safer storage of private information and reduce the possibilities of identity theft?
- Can blockchain network and technology be used to provide better national security in terms of border security and the weapon of mass destruction?

Structure of this thesis

The rest of this thesis is organized as: in Chapter 2 we discuss the literature review and detailed explanation of blockchain, disaster management, border security and identity theft along with the work related to our research. The current status and prediction of the events in future are explained in Chapter 3. In Chapter 4, the proposed model for the disaster management, rescue operations, and proper information storage to reduce identity theft along with methods to provide better national security using blockchain concept is explained. Finally, in Chapter 5, conclusions and potential future research directions are discussed.

CHAPTER 2

LITERATURE REVIEW

2.1 Blockchain

"What the internet did for communications, I think Blockchain will do for trusted transactions." This was told by the CEO of IBM Ginni Rometty in June 2017 (Rapier 2017). Blockchain technology has become popular since the introduction of bitcoin as a digital currency. The bitcoin mechanism was introduced by Satoshi Nakamoto in 2008 in a paper entitled Bitcoin: A peer to peer Electronic Cash System (Satoshi Nakamoto, 2008). This paper described a peer to peer version of electronic cash that allows online payments to be sent directly from one party to another without any intermediary financial institution. The technology behind this idea is Blockchain. Though Blockchain technology is typically associated with Bitcoin and other virtual currency platforms, the underlying innovation of Blockchain is likely how societal disruption will occur (Kevin D. Johnson, 2018). Blockchain has the potential to completely change the way international trade, taxation, real estate, and even healthcare takes place (Alexis, 2017). Almost any system of recording, transferring, storing and the processes built around it can be replaced by Blockchain (Knight, 2017; Johnson, 2018).

A Blockchain is a shared, distributed, tamper-resistant database that every participant on a network can share, but no one controls it entirely. It has two fundamental features: The Blockchain is public. Anyone can view it at any time because it resides on the network and not within a single governing institution which has the responsibility of maintaining and recording of any event. It is also encrypted. Encryption is one of the most important functioning/ feature of Blockchain. Even though the information and records of all the events, transactions or communication are present in the network and available for everyone, it uses encryption involving private and public keys in order to provide better security.

It can be defined as an incorruptible digital method of transacting anything and everything of value. It is shared by a group of network participants and all of them can provide new records for inclusion. However, these new records can only be added if the majority of the group agrees on that. The record once created cannot be changed or manipulated. Transactions such as payments, notarization, voting, registration, contracts etc. are key in the operation of government or any other organization. Traditionally, these transactions are done and supported by a central unit which is a third party such as government agencies, legal firm, brokers, banks and service providers. Blockchain provides a different method to validate and perform these transactions. Instead of trusting third parties, it depends on the majority of the members of the network and the accuracy of their shared platform.

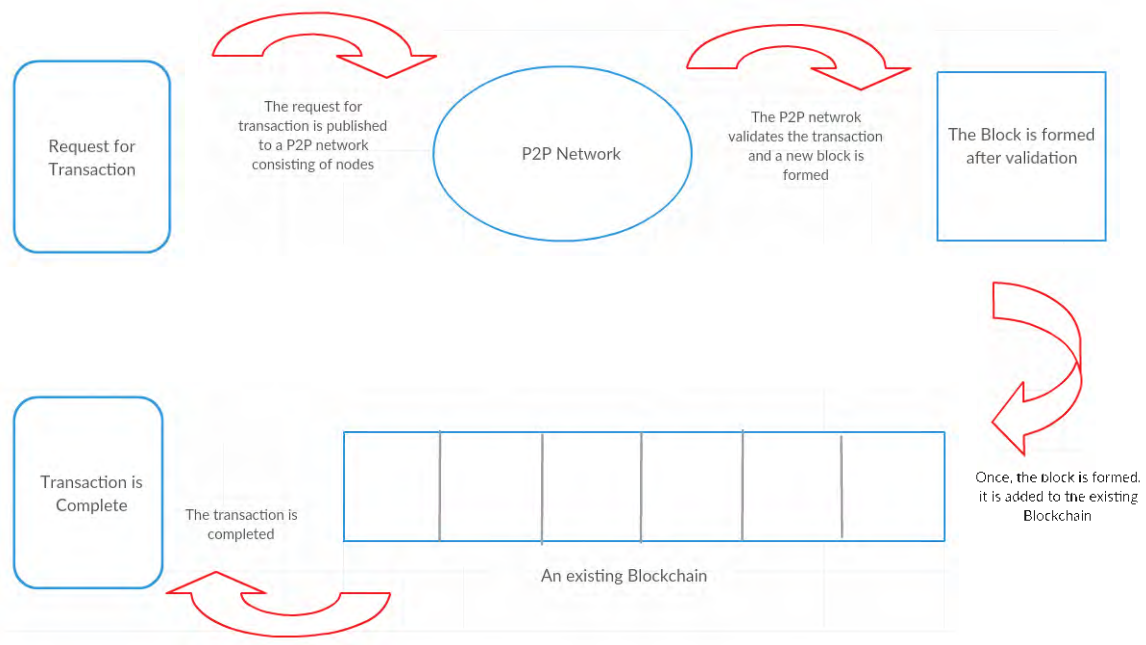

Figure 2.1 The explanatory functioning of a blockchain network

A Blockchain works on a distributed ledger technology, which was publicly introduced for the transfer and record keeping of Bitcoin. The major advantage of the technology is that it provides a trustable path to transfer an asset without the need of a third party which acts as a central authorization. In order to work efficiently, it requires a secure protocol to transfer assets, protection against assets being transferred twice, and a sacrosanct record of ownership that can be automatically updated.

2.1.1 Blockchain functionalities

Peer to Peer networking and distributed data storage (P2P Network)

It provides all the participants in the system with multiple copies of a single ledger so that a shared history of all the transactions in the system is available to all the members of the network.

Cryptography

It provides a secure way to initiate a transaction that helps verify ownership and availability of the asset to transfer in the form of hashes and digital signatures.

As such, Blockchain innovation is basically a progression of encrypted records affixed together over a distributed environment that enormously limits the odds of extortion.

Table 2.1: Conversion of a certain entity into a secure hash function

INPUT	OUTPUT OF SECURE HASH FUNCTION
Service Provider 1	7D09E44H7791247AEBHG80T0TT174D
Service Provider 2	0000BF113HHJKI2220OOPTOPLJE45K0

2.1.2 Design principles

Blockchain establishes the new era of the digital economy, there are seven design principles for creating software, services, business models, markets, organizations, and even governments on Blockchain. These are detailed below:

Security

Cryptography must be used by everyone who wants to be a part of Blockchain network. A public key infrastructure is an advanced form of asymmetric cryptography, in which the user is provided with two keys which have completely different functions: Encryption and Decryption.

Preserved rights

In a Blockchain network, individual freedoms are respected and recognized. It can actually work as a public registry, a site that creates and registers cryptographic information about anything and everything present in the Blockchain network. The hash of the document is calculated on the user's or the member's machine thus reducing the chances of fraud, providing better security.

Distributed power

The system does not have a single source of control and uses peer to peer networks to distribute power. No single party or member of the system can turn the system down. Even if one of the members is cut from the network the system will still work and survive.

Integrity of network

The consensus is reached in a Blockchain network algorithmically and records it cryptographically on the Blockchain. Integrity is encoded in each step of the process and is distributed throughout the system.

Participants can exchange values directly with the expectation that the other party will act with integrity. It is more traceable than cash as no one can hide a transaction.

Inclusion

There is a very low barrier to participation in Blockchain. Thus allowing distributed capitalism. Satoshi designed a system that worked efficiently on the internet but Blockchain can work without internet as well. The KYC (Know Your Customer) and AML (Anti Money Laundering) check is still to be performed.

Value

In Blockchain the value is rewarded by incentives. For example, if a miner mines a block after solving the pre-determined mathematic algorithm he gets rewarded for the value he provided to the Blockchain network.

Privacy

There is no single party that governs or control all the information about the members of the network. Individuals control their own data. Blockchain provides the ability to maintain any degree of personal anonymity; they don't have to attach any personal identity details. The transaction layer is completely separate from identification process.

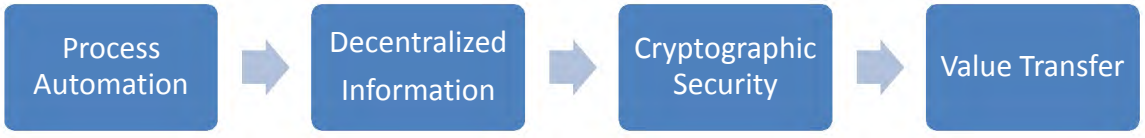

Figure 2.2 Characteristics of Blockchain Application (Capegemini Group, 2016)

2.1.3 Types of blockchain

Private blockchain

In a private blockchain, the ability to perform or record a function is limited to one organization / user. Whereas, the ability to read may be public or can be restricted to any extent. Private Blockchain is a way of capitalizing on Blockchain technology by establishing groups and participants who can verify transactions from within the system.

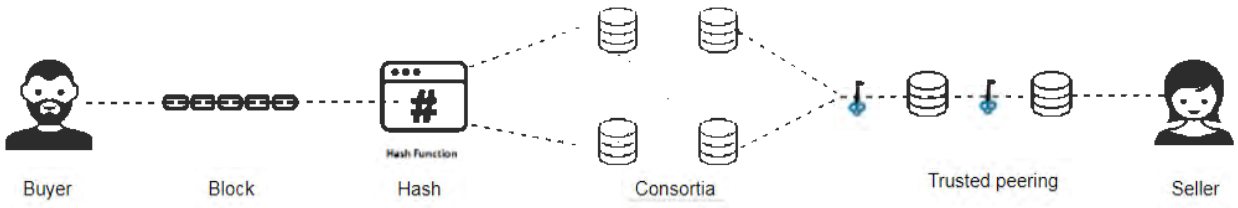

Figure 2.3 The characteristics of a private blockchain (geek4geek, SteemKR,2017)

Examples of private Blockchain would be: Hyperledger and Multichain.

Public blockchain

Public Blockchain network provides the ability to anyone in this world who is a part of the network to access the data. This includes writing, developing and recording of blocks, information, and transactions. Public Blockchain network is secured by the concept of crypto economics and is an open source system. It is a framework based on calculations, algorithms, and processes such as proof of work (PoW) and proof of stake (PoS).

In this type of Blockchain network new blocks can be added to the Blockchain, but already present blocks cannot be replaced or removed. Bitcoin is a very good example of Public Blockchain.

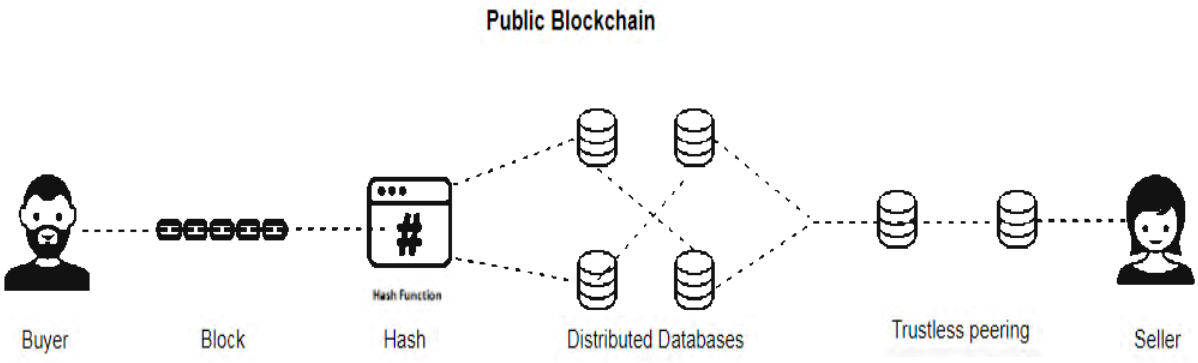

Figure 2.4 The characteristics of a public blockchain (geek4geek, SteemKR, 2017)

Table 2.2: Characteristics of private and public Blockchain

Characteristics	**Private**	**Public**
Identity	Known Identities	Pseudonymous
Security	Participants are pre-approved	PoW/ PoS
Access	Permission needed to access the database	Open source, access to the database
Speed	Faster	Slower

2.1.4 Consensus

A consensus is a process that enables "a set of distributed process to achieve agreement on a value or an action despite a number of faulty processes" (Correia, 2011). Blockchain requires verification and acceptance by all the members of the network, usually called as consensus.

To achieve consensus in distributed mechanism there are four algorithms that can be applied. In a blockchain network, a consensus is utilized to obviate mendacious actors from inditing potentially invalid information to the database (Swanson, 2015).

The concrete consensus mechanism utilized for any given blockchain depends on a number of posits, including the amount of trust between parties and the alignment of their intrigues, as well as factors concerning the shape and synchronization of the network (Correia, 2011).

Proof of Work (PoW)

The most widely used algorithm in Blockchain is the PoW consensus algorithm. Proof of Work concept existed before bitcoin. It was originally published by Cynthia Dwork and Moni Naor back in 1993, but the term "proof of work" was coined by Markus Jakobsson and Ari Juels in a document published in 1999 (Blockgeeks, 2017). In the case of Bitcoin proof of work assumes that all members in the network votes by utilizing their computational power by solving the PoW and construction and validating the block. Proof of work can be considered as the main component in order to define an expensive computer calculation, also called mining that has to be performed in order to generate a new block.

Mining servers for two purposes: To verify the legitimacy of a transaction and to avoid double spending.

Bitcoin employs a hash-based PoW. The value of the hash has to be smaller than the current target value. Other members of the network verify the PoW by computing and comparing the

hash value with the target value. Consensus requires that the target value or the given value should be greater than or equal to the calculated value.

Proof of Stake (PoS)

Proof of stake is a different way to validate transactions predicated and achieve the distributed consensus. It is still an algorithm, and the purport is identically tantamount to the proof of work, but the process to reach the goal is quite different. The PoS algorithm aims to supersede the subsisting way of achieving consensus in a distributed system; in lieu of solving the PoW, the node that engenders a block has to provide proof that it has access to a certain amount of transactions before being accepted by the network (Vasin, 2015).

Therefore, only those who can provide the PoS can participate in the process of maintaining the blockchain. In terms of energy saving, PoS deliver more efficiently on energy consumption compared to PoW (Kikitamara, 2017).

Practical Byzantine Fault Tolerance (PBFT)

This consensus algorithm was developed to tolerate Byzantine faults, for instance, the arbitrary behavior of the node, joining and quitting the network at any time that usually occurs in a distributed system. This algorithm presents a state machine replication technique to cope with

Byzantine faults. Theoretically, it uses a state machine replication algorithm with only one message round trip to execute read-only operations and two to execute read-write operations. Also, it uses an efficient authentication scheme based on message authentication codes during normal operation; public-key cryptography is used only when there are faults (Castro and Liskov, 1999).

Delegated Proof of Stake (DPoS)

The major difference between PoS and DPoS is that PoS is a direct democratic process, while DPoS is representatively democratic—stakeholders elect delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block can be confirmed quickly, meaning the transaction can be confirmed quickly (Zheng, 2016) and (Kikitamara, 2017)

2.1.5 Blockchain architecture

Block

For recording transactions, a distributed ledger is facilitated by the Blockchain, attributing them to a specific node in a network, and ordering them in time. Blocks are the files which have the data stored in them in a network. It generally records most recent transactions that have yet to be recorded in prior blocks.

A block consists of the block header and block body (Zheng, 2016). Three sets of block metadata combines together to form the header of the block i.e. block header. First, there is information regarding the previous block hash, which connects the block to the previous block in a blockchain. The second being difficulty, timestamp, and nonce in the case of Bitcoin, relates to

the mining competition. The last being Merkel tree root, a data structure used to summarize all the transactions in the block (Antonopoulos, 2005).

Digital signature

In order to create and authenticate the transaction on the blockchain, a digital signature is required. The signing phase and the verification phase combine together to be a part of a typical digital signature.

For example, when a member who is part of the network wants to sign a transaction, s/he will first generate a hash value. This hash value is later encrypted with the help of the user's private key and sends the other person or member who is at the receiving end of the transaction process. The other users/ member verify the transaction by decrypting the hash using the first person public key and the hash value will be the same for the received data as well.

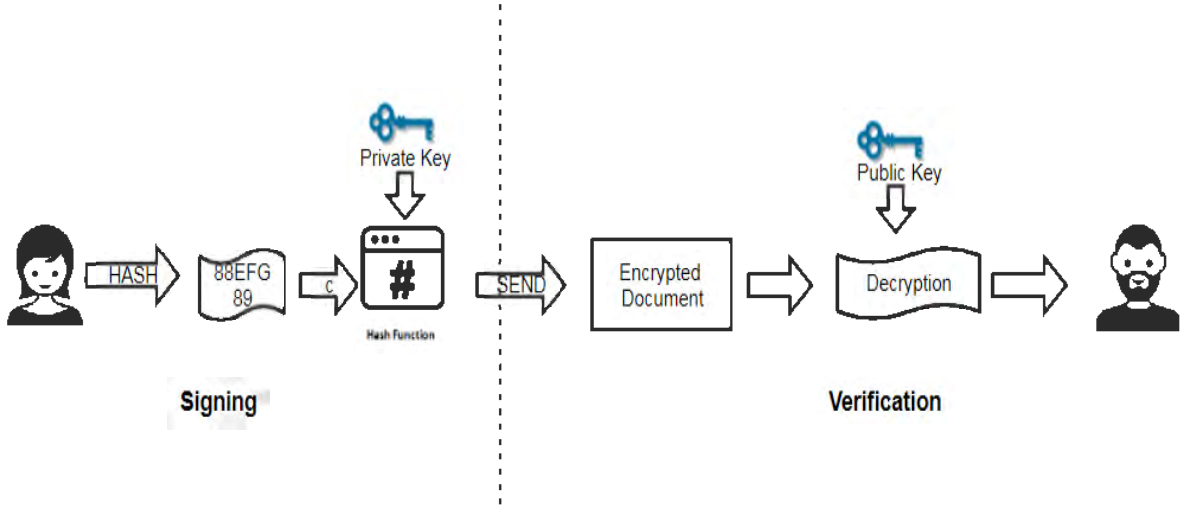

Figure 2.5: Digital Signature Used in Blockchain. Adapted from Blockchain Challenges and Opportunities (Zheng, 2016)

Decentralized network

A decentralized network as the name suggests is a type of network with no central authority or governing unit. Every member of the system is a part of an open transaction process which is visible to everyone and need verification by the network members in order to complete the transactions (Kikitamara, 2017). The interactions among user on blockchain principally use a decentralized network in which each user represents a node at which a blockchain client is installed. When a user performing a transaction with another user or when a node receives data from another node, it verifies the authenticity of the data. It then broadcasts the validated data to every other node connected to it. Within such a mechanism the data spreads across the whole network.

Fig 2.6 Centralized and Decentralized network

(Adopted by: http://www.truthcoin.info/blog/measuring-decentralization)

At first blockchain technology was commonly seen as bitcoin's main technological innovation. But, today this technology has more advanced practical usage and implementation than bitcoin. This ranges from financial transactions like smart contracts, digital payment, decentralized IOT, supply chain, insurance, disaster management, national security, healthcare and many more.

2.2 Disaster management

According to the International Federation of Red Cross and Red Crescent Societies; a disaster is a sudden, calamitous event that seriously, disrupts the functioning of a community or society and causes human, material and economic or environmental losses that exceed the community's or society's ability to cope using its own resources.

(VULNERABILITY + HAZARD) / CAPACITY = DISASTER

As World Health Organization (WHO) defined in other words that, a disaster is an occurrence disrupting the normal conditions of existence and causing a level of suffering that exceeds the capacity of adjustment of the affected community.

In the past few years, there has been an increase in the devastation caused by natural disaster, leaving an enormous amount of victims which were forced to seek shelter in places like churches, fire halls, auditorium etc. A natural disaster is a type of phenomenon that we all understand properly and know that it may have a direct impact on the welfare of the specific region and households where it occurs. Depending on where we live, natural disasters like earthquakes, floods, droughts, wildfire, etc. are a threat to lives, properties, assets and social designators. In the United States, the rate of large, costly natural disasters has increased drastically over the last three decades leaving a lot of people homeless and in search of help.

2.2.1 Impact of disasters

An innumerous amount of people get affected by disasters every year. From the eradication of property to the elevation in disease spread, disasters can devastate entire region in a very less amount of time. Disasters have affected living organism throughout history. The tales of floods, earthquakes, volcanic eruptions, wildfire, famines etc. have been passes down for generations. With time the world has noticed an increase in the occurrence of disasters. At the individual level, the impact of a disaster can often be felt physically, mentally, and emotionally. After experiencing a natural disaster, many individuals develop severe post-traumatic stress disorders or withdraw into states of depression (Sharrieff, 2018)

The other immediate effect of natural disasters is displacement of population. Many people have to leave their house and community and shift to a completely new place and start a new life altogether. This large number of people migrating may disrupt the accessibility of healthcare, education, and supply of food and drinkable water. The secondary effect can be the health risk that such a devastating event brings with it. Without proper rescue and disaster management death tolls may rise even after the immediate threat has passed leaving a huge amount of population vulnerable.

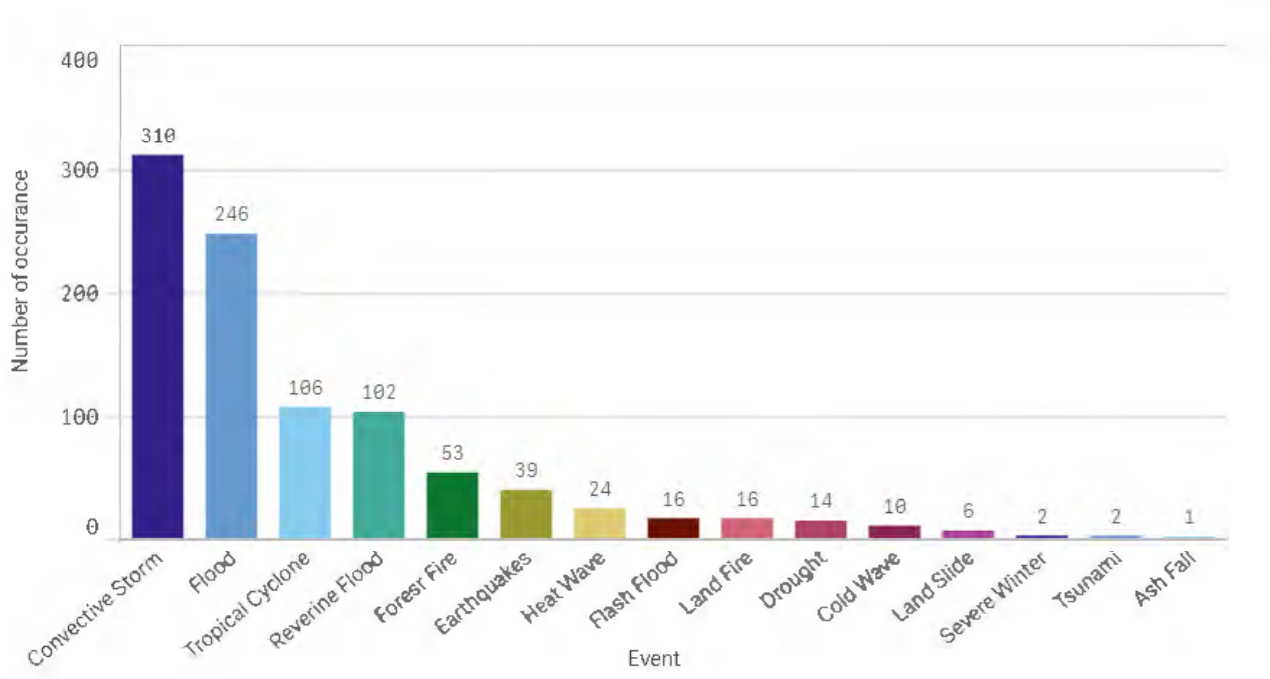

Figure 2.7 Number of natural disasters in the United States by type from 1900 -2016, (EMDAT, 2017)

When it comes to such situations, the main area to focus on in such conditions is Disaster Management. According to the International Federation of Red Cross and Red Crescent

Societies; Disaster Management can be defined as the organization and management of resources and responsibilities for dealing with all humanitarian aspects of emergencies, in particular, preparedness, response and recovery in order to lessen the impact of disasters.

Disaster management includes the development of disaster recovery plans, (for minimizing the risk of disasters and for handling them when they occur,) and the implementation of such plans.

Disaster management usually refers to the management of natural catastrophes such as fire, flooding or earthquakes. Related techniques include crisis management and risk management.

The discipline of avoiding and dealing risk is termed as disaster management. It is a combination of disaster response, supporting and rebuilding society after the crisis and preparing for the disaster before it happens.

2.2.2 Disaster management phases

Disaster Management consists of four well-defined processes:

Mitigation

Any activities that can prevent an emergency, reduce the damaging effects of the hazard or reduce the likelihood of occurrence are Mitigation. The mitigation phase is different from other phases because it focuses on long-term measures for reducing or eliminating risk. The implementation of mitigation strategies can be considered a part of recovery process if applied after the disaster occurs (Pulwarty, 2007).

This phase can be of two types; structural or non-structural. It is one of the most cost-efficient methodologies for reducing the impact of hazards. The main activity for the mitigation is the identification of risks. The process of identifying and evaluating hazards is referred as risk assessment. Each hazard poses a risk to the population within the area assesses. The hazard-specific risk (R_h) combines both the level of impact and probability.

$$R_h = V_h \ * \mathrm{H}$$

(Component of Risk Management)

Where V_h = vulnerability and H = Hazard

Preparedness

It means to be prepared and ready to face a hazardous situation by developing plans for what to do, where to go, or who to call for in case of occurrence of any hazard.

Any actions that could improve one's chances of successfully dealing with a hazard would be considered a part of preparedness. Common preparedness measures include communication plans with easily understandable terminology and chain of command, development and practice of multi-agency coordination and incident command, proper maintenance and training of emergency services, development and exercise of emergency population warning methods

combined with emergency shelters and evacuation plans, stockpiling, inventory, and maintenance of supplies and equipment (BNET Business Dictionary & Pulwarty, 2008)

Preparedness measures can take many forms including the construction of shelters, installation of warning devices, a creation of backup life-line services (e.g. power, water, sewage), and evacuation plans.

Another aspect of preparedness is causality prediction, which is the prediction of the number of injuries and death to expect because of the hazard which helps to generate a proper plan in order to provide necessary resources for that specific hazard.

Response

The ability to act responsibly and safely in a crisis situation in order to protect one's family, oneself and individuals around you at the time of disaster would be considered a response. It includes the mobilization of the necessary emergency services and first responders in the disaster-affected area. The emergency services include medical suppliers, firefighters, police, food suppliers, and ambulance crew. They may be accompanied individuals who are compelled to volunteer directly after a disaster.

Recovery

Recovery is best defined as the ability to quickly resume a normal life by rearranging your life and the environment after the hazard and the immediate danger is over. The recovery phase starts after the immediate threat to human life has subsided. The aim of this phase is to restore the affected area to its original state.

Recovery efforts are primarily focused towards constructing the damaged property, repair of infrastructure and providing employment to people who lost their source of income because of the event. During reconstruction, it is recommended to consider the location or construction material of the property. And proper mitigation procedures can be applied.

Figure 2.8: The comprehensive approach to disaster management (Queensland Government)

The government makes a plan and provides rescue operations in order to save citizens from these hazards. They plan to provide resources like food, medical attention, water, vehicles, helicopters etc. in order to keep them safe. The Federal Emergency Management Agency (FEMA) is involved in providing training programs and research information on the latest and more effective mitigation measures. FEMA provides financial assistance at the time of hazards to the affected area. FEMA usually provides resources when the affected states or the area does not

have sufficient resources to protect their citizens. It is a principal source of help and education during a disaster.

2.3 Identity theft

Identity theft can be visualized from multiple aspects but they all boil down to one basic definition, which says that it is the illegal or unauthorized use of personal information belonging to someone else for one's own benefit (Irshad, Soomro and Merriam Webster, 2017). Identity theft is made possible by the nature of modern payment systems. Identity theft involves acquiring enough data about another person to acquire goods while attributing the charge to another person's account. Customarily, it was something known as "dumpster jumping", where the identity thieves needed to physically circumvent snooping in junk containers to search for individual data, for example, disposed of bills and records that distinguished a man. There were various customary courses going from extremely complex to completely straightforward that a character criminal could use to access individual information (spamlaws.com). The development of identity theft can be found in Table 3 from as ahead of schedule as 1800's to anticipated state in 2020 (Velasco, 2016 and Irshad, Soomro and Merriam Webster, 2017).

Table 2.3: Evolution of Identity Theft ((Irshad and Soomro, 2018)

Era	Types of Identity Theft
1800-1918	Killing used to take place in order to impose someone's identity
1919-1921	People were threatened by powerful politicians and their identity was stolen to cast

	multiple votes
1922-1930	The smugglers murdered people to attain legal documents to create new identities
1931-1959	Fake ID were made by youngsters who were underage in order to buy liqour
1960-1969	Credit cards gave criminals new ways of identity theft
1970-1989	Different con artist stole identities to cash cheques and withdraw money
1990-1998	Technology advancement increased cases of identity crimes
1999-2000	Introduction of Internet led people to give away personal information
2001-2003	Reporting agencies started providing credit reports to customers to prevent fraud
2004-2015	New form of identity theft came into knowledge
2016	Identity Theft was the most popular consumer complaint for 15 consecutive years
2017	Criminals started using other platforms for stealing identities as the security was tightened
2018-2020	Technology is evolving; so that thieves are gaining more and more access to personal information through it

2.3.1 Stages of identity theft

Identity theft has been categorized into three stages by the researchers. A particular identity theft crime may include one or all of these stages

Acquisition of the identity

Collecting the documents having identification information of the victim through theft, computer hacking, fraud, trickery, force or even by legal means is known as an acquisition of the identity.

Use of the identity

The most common use of identity is for financial gain or to avoid criminal charges by presenting identity documents to someone else. Someone else's identity can be used to take over existing accounts, usage of victim's credit card or debit card, fraud tax filing, Insurance fraud etc.

Discovery of the theft

Albeit numerous abuses of credit cards are found rapidly, identity theft may take from half year to several years to discover. Proofs recommend that the more it takes to discover the theft, the more prominent the misfortune acquired by the casualty, who could possibly include law implementation. Impressively more research is required around there (Newman and Mcnally, 2007).

2.3.2 Ways of identity theft

Data breaches

A data breach is an episode wherein data is stolen or taken from a framework without the learning of the system's proprietor. Stolen data may involve sensitive, proprietary, or confidential information, for example, credit card numbers, customer data, trade secrets exchange privileged insights or matter of national security. Most of the time, data breaches are

credited to hacking or malware attacks. While these assaults assume a major part, they represent a fourth of the greater part of the revealed occurrences.

Other frequently observed breach methods include the insider leak: where a trusted individual or person of authority with access privileges steals data.

Payment card fraud: payment card data is stolen using physical skimming devices. Loss or theft: compact drives, workstations, office PCs, records, and other physical properties are lost or stolen. Unintended exposure: through slip-ups or carelessness, touchy information is uncovered. In a little of number of cases, the genuine rupture technique is obscure or undisclosed (TrendMicro, 2016).

ATM overlays

Specifically programmed devices at the ATM machines and gas pumps can be installed by thieves to glom your account information when you swipe or insert your card.

Mail theft

Mail can be stolen directly from unlocked and low visibility mailboxes by thieves, enabling them to access your personal information from bills, statements, W-2, etc.

Dumpster diving

Thieves will sort through h garbage to find old bills, recent receipts, and other discarded personal information. These thieves can collect a lot of information by dumpster diving by stealing pre-approved credit card offers, street address, Social Security number, telephone number, email

address, bank account information, employment history and other personal information (Lifelock & White, 2013)

2.4 Border Security

The politician has been talking about border security in the United States of America since the passage of the Immigration Reform and Control Act of 1986 (Jones-Correa and De Graauwe, 2013). America is considered as the land of immigrants. There has been a mixed response regarding immigrants moving to this country in order to find better education, jobs, or the life standards. For the last three decades, the government has been trying really hard to strengthen US border security policies. They have increased the work power, resources and funding related to border security (Victor M. Manjarrez, Jr., 2015).

Border security is the measures taken by a country to monitor or regulate its border. The main functioning of the border control is to regulate immigration, control the movement of citizen and execute proper and fair custom operations. The idea of border security was pursued at a great pace by the government of the United States of America after the terrorist attack on September 11, 2001. Even though none of the known people involved in that attack is supposed to have entered the United States of America illegally, but after that day illegal immigration is considered to be a threat to national security. Currently, the Department of Homeland Security and Congress are debating different methods to provide better border security.

Over the years it seems that the United States of America has become more populated and unsafe from the illegal immigrants, smuggled goods, harmful viruses, drugs and weapons that travel across the border.

The border patrol is responsible for patrolling the 6,000 miles of Mexican and Canadian land borders and 2,000 miles of coastal waters (United States Custom and Border Protection). The border security without coordinated exit-entry controls leads to people overstaying their visa in violation of immigration law. There have been a lot of cases reported for the illegal transportation of weapon and people. There are cases where people have stolen the identity of someone else in order to enter the United States of America. While unlawful movement and border security are really two distinct issues confronting the United States of America, both without a doubt have noteworthy bearing and impact on each other (Bach, 2005). Lessening their multifaceted nature relies on understanding the relationship between them. The fundamental start is that outskirt districts that have overpowering levels of illicit migration make a situation that is both turbulent and jumbled, overpowering the capacities of border requirement substances. Shrewd criminal associations frequently misuse this defenseless condition by mixing in with genuine action to avoid recognition. Furthermore, this same riotous and jumbled condition makes the outskirt powerless against misuse by fear-based oppressor associations. This is the genuine risk of an uncontrolled border (Manjarrez, Jr., 2015).

A nation without borders is not a nation. The borders of a country enable it to have control over its resources, people, and facilities. It is therefore mandatory for the United States to have good

border security and control its borders for the purposes of reducing the number of illegal immigrants in the nation. The government of United States has tried endeavors to guarantee border security for the reasons for making an outskirt control framework that guarantees that lone the individuals who are lawfully permitted to enter the United States will have the capacity to do as such. There is still a huge amount of work to be done in this field in order to secure the national borders

2.5 Weapon of mass destruction

A weapon of mass destruction is a nuclear, conventional, biological, chemical, cyber, viruses that can demolish cities, assets, and human beings leading to a huge destruction. The term weapon of mass destruction was used by Cosmo Gordon Lang of Canterbury in 1937 (Majumdar, 2017).

International politics have been focusing on the weapon of mass destruction and the destruction they can cause. The term is used to characterize a variety of weapons that has two key features: the indiscriminate nature of their effects and their potential to cause large-scale destruction (Reed, https://www.hampshire.edu/pawss/weapons-of-mass-destruction).

Powerful countries are producing nuclear weapons, radiological weapons, hydrogen weapons, chemical weapon and biological weapons in order to show the world that they have power. One of the most known weapons, the atom bomb, has the potential to kill thousands of people and destroy a whole area or city for decades. We can see a perfect example of this in history through the events of Hiroshima and Nagasaki. According to the United States army and researchers, this weapon has an explosive energy of nearly 20,000 T.N.T explosions.

The chemical weapon can be traced in Syria today and have the potential to spread quickly and cause injury and even death to those affected. Similarly, biological weapons have been used since the beginning of 20th century. These weapons continue to threaten the world as they lead to immense risk in relation to peace, security and the survival of mankind.

The proliferation of weapon of mass destruction (WMD), and their delivery systems could have unmeasurable consequences for global, national and regional security. Prevention of Weapons of Mass Destruction Proliferation and Terrorism believes that the chances of an attack with a biological weapon are more likely than with any other weapon of mass destruction. This seems strange considering our culture is focused on the big boom that would wipe out the majority of the population. But this would be a silent but deadly terrorist attack using one of the world's most lethal diseases to cause a worldwide epidemic that would kill millions of people (Suk, 2014).

The immense assorted variety of potential organic specialists represents a tremendous challenge to our security. By a few evaluations, there are more than 300,000 types of microbes and no less than 5,000 sorts of infections that unfavorably influence people. For quite a long time, social orders have attempted to pick up the high ground in counteracting and controlling flare-ups, directing immunizations against polio, smallpox and other destructive illnesses, educating the significance of cleanliness in keeping the spread of irresistible infection (Henry Stimson Center).

In addition to the dangers posed by existing storing of the weapon of mass destruction (WMD), significant problems arise from the proliferation of WMD and related technologies to additional countries, nongovernmental performing artists, and non-state fear based oppressor organizes through, robbery amid transport, underground market offers of weapons and related innovations.

Linton Brooks (security official) said that "The convergence of heightened terrorist activities and the associated revelations regarding the ease of moving materials, technology, and information across borders has made the potential of terrorism involving weapons of mass destruction (WMD) the most serious threat facing the Nation. Preventing WMD from falling into the hands of terrorists is the top national security priority of this Administration."

In spite of the inescapable vulnerability encompassing any push to assess the heap dangers related with WMD, specialists are consistent in their conviction that we confront grave dangers that are probably going to increment over the long haul, excepting essential changes in current approaches at the nearby, national and global level. However, past this wide accord, a wide inlet stays amongst pundits and supporters of current U.S. government arrangements concerning the U.S. atomic stores and methodologies for WMD non-multiplication (Reed, https://www.hampshire.edu/pawss/weapons-of-mass-destruction).

According to the Deputy Secretary-General of the United Nations, Eliminating weapons of mass destruction is the only way to prevent non-state actors from acquiring them. This is among the most important responsibilities of the international committees. The countries which are capable of developing or obtaining all types of weapons of mass destruction (Chemical, Nuclear, Biological and Missile) are USA, Russia, Israel, France, China, India, North Korea and Pakistan.

The world is working together to develop policies which could help to reduce the theft and misuse of such weapons by terrorist organizations but still a lot of development in this field is still to be done.

Chapter 3

CURRENT STATE

3.1 Current approach towards disaster management

The production of arrangements with the help of which an individual, a group or individual or a community diminish the risk and adapt to disasters is known as disaster management. It doesn't take out the danger but provides a strategy to how to provide better safety and help to the individuals who got impacted by it. As of now 60 percent of organizations in the United States of America don't have an effective disaster management plans (Environment pollution and climate change).

The climate is changing due to various reasons such as global warming and chances of occurrence of a sudden, unpredictable disaster is high. Thus, in order to prevent losses not just in terms of assets, property, and property but also lives a proper disaster management or emergency management plan should be implemented. Disaster management in the United States of America has utilized the function all-hazard approach from last two decades, in which the strategist plans for all type of disaster and crisis situations and how to deal with it, rather than working towards or focusing towards a single event and preparing for it. As different events may require different approaches, relying on one leads to improper help provided to the victims. Most of the disaster

management are local, which means that they are handled by the local authorities. If the event becomes overwhelming for the local authorities, the state officials are involved and then the national authorities in order to provide better help and faster rescue operations. The Federal Emergency Management Agency (FEMA), which is a part of the Department of Homeland Security (DHS), is the lead federal authority to deal with disasters and disaster management.

3.1.1 Statistics related to disaster management

According to National Centers for Environmental Information (NOAA), in 2018 (as of April) there has been 3 weather and climate disaster events with losses exceeding $3 billion dollars across the United States of America. These events lead to a death of 34 people (reported) and had significant economic effects in terms of assets and property. There has been a high number of disasters taking place in the world. According to the (Emergency events database) EMDAT:

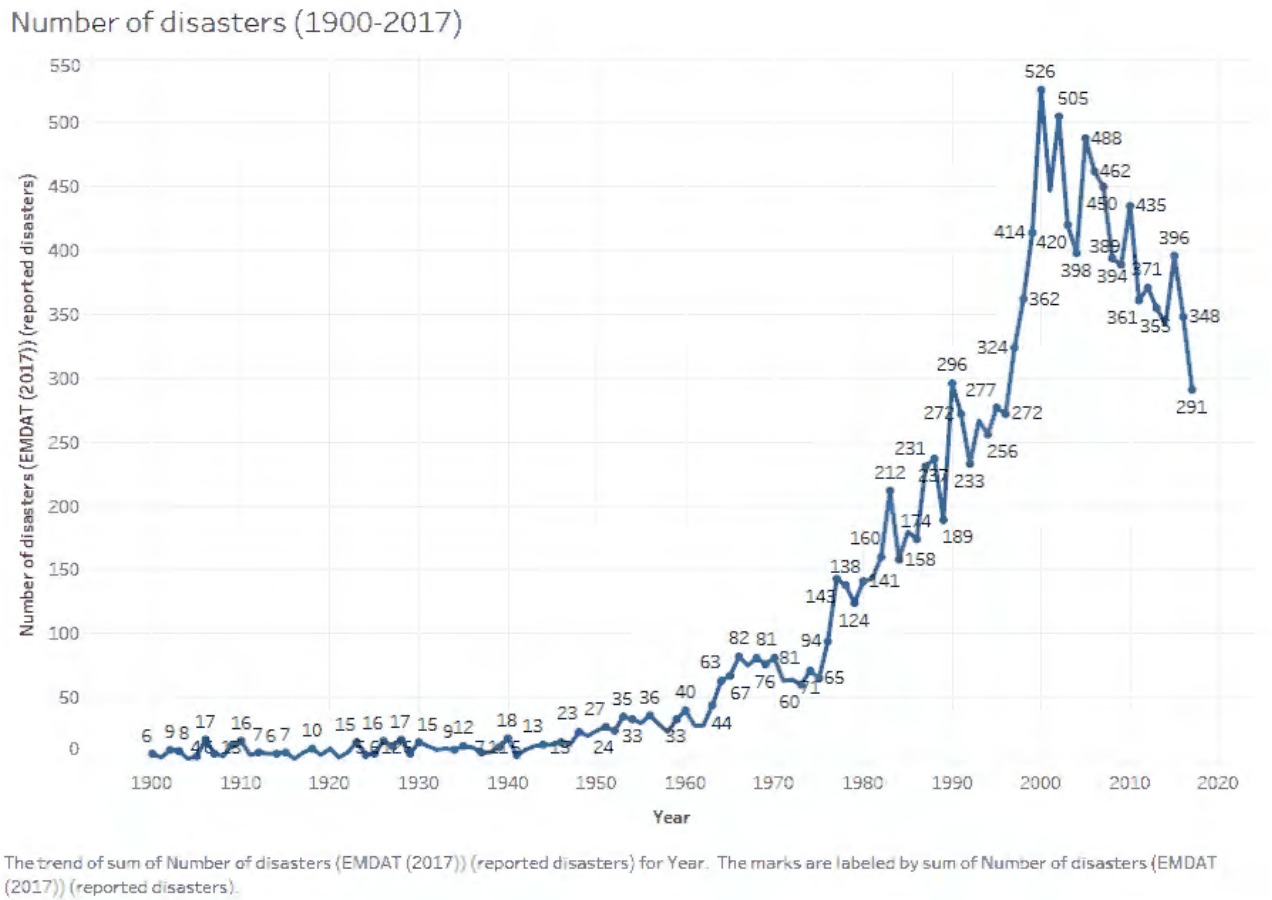

Figure 3.1 The number of disasters from 1900-2017 throughout the world (EMDAT, 2017)

After performing a time series forecasting using the linear forecasting model, the following trend was generated which suggested a linear growth in the occurrence of disasters.

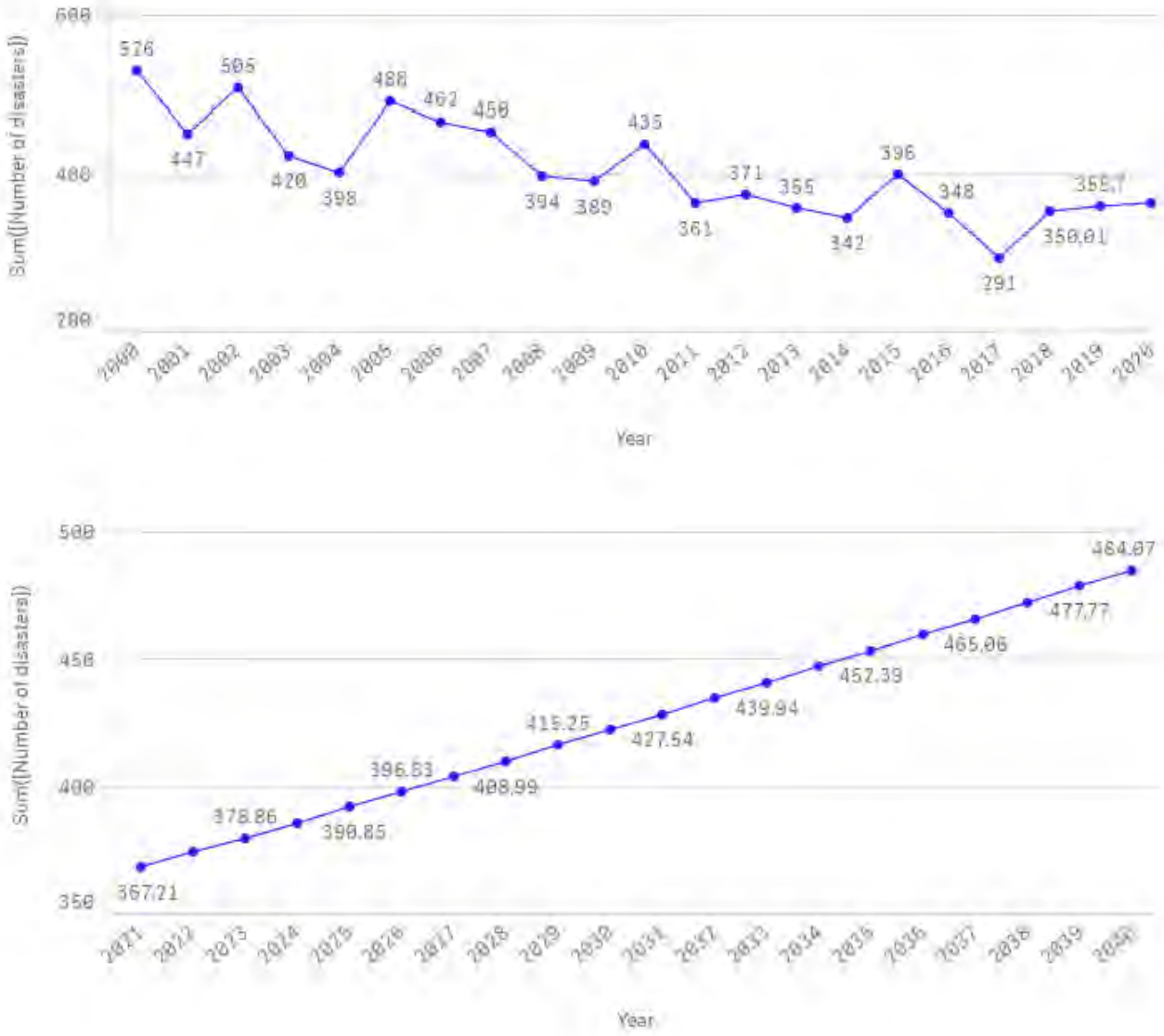

Figure 3.2 Forecasted model for the occurrence of disasters till 2040

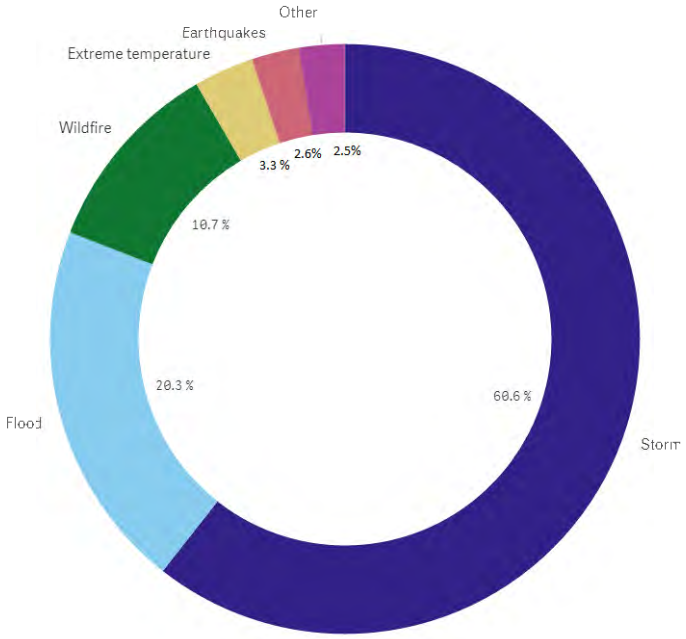

Figure 3.3 Frequency of disasters from 1990-2017 in the United States of America

(Prevention web, EMDAT, 2017)

It has been noted that storm is the most frequent disaster in the United States of America with a 60.6% occurrence percentage in last 2 decades. Flood being the second frequent with 20.3% occurrence rate. Wildfire being the third frequent disaster with 10.7 % of frequency rate. Extreme temperature and earthquakes being fourth and fifth respectively with 3.3% and 2.6%. There has been a lot of losses in terms of lives reported since the beginning of 20th century throughout the world. The biggest loss due to disasters is considered to be that of life. All the rescue operations and disaster management have the common goal of providing safety to the people affected by the event.

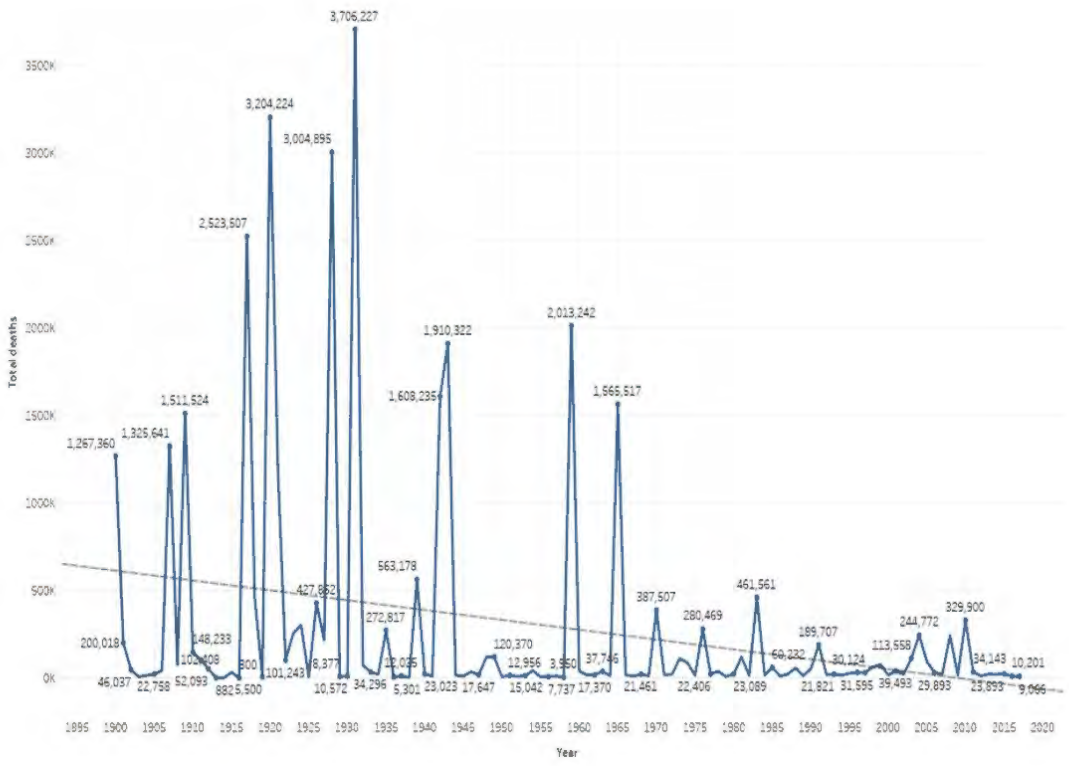

Figure 3.4 Number of death reported throughout the world because of all sort of disasters (EMDAT, 2017)

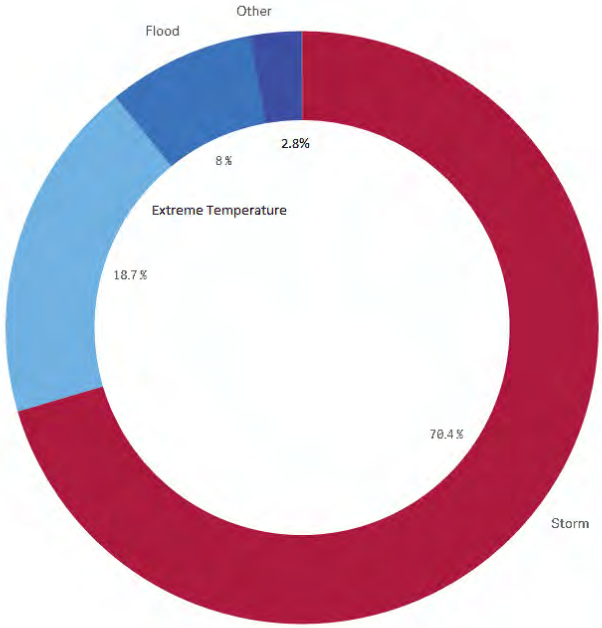

Figure 3.5 Reason of mortality due to disasters in USA (Prevention web, EMDAT, 2017)

The type of disaster with the highest percentage of mortality in the United States of America is a storm with a high percentage of 70.4. Extreme temperature being second with 18.7% mortality rate and flood being the third major cause of death when it comes to types of disasters.

3.1.2 Current approach towards disaster management

Disaster management in today's era follows the centralized network system where a centralized authority is responsible for all the necessary transactions between two parties.

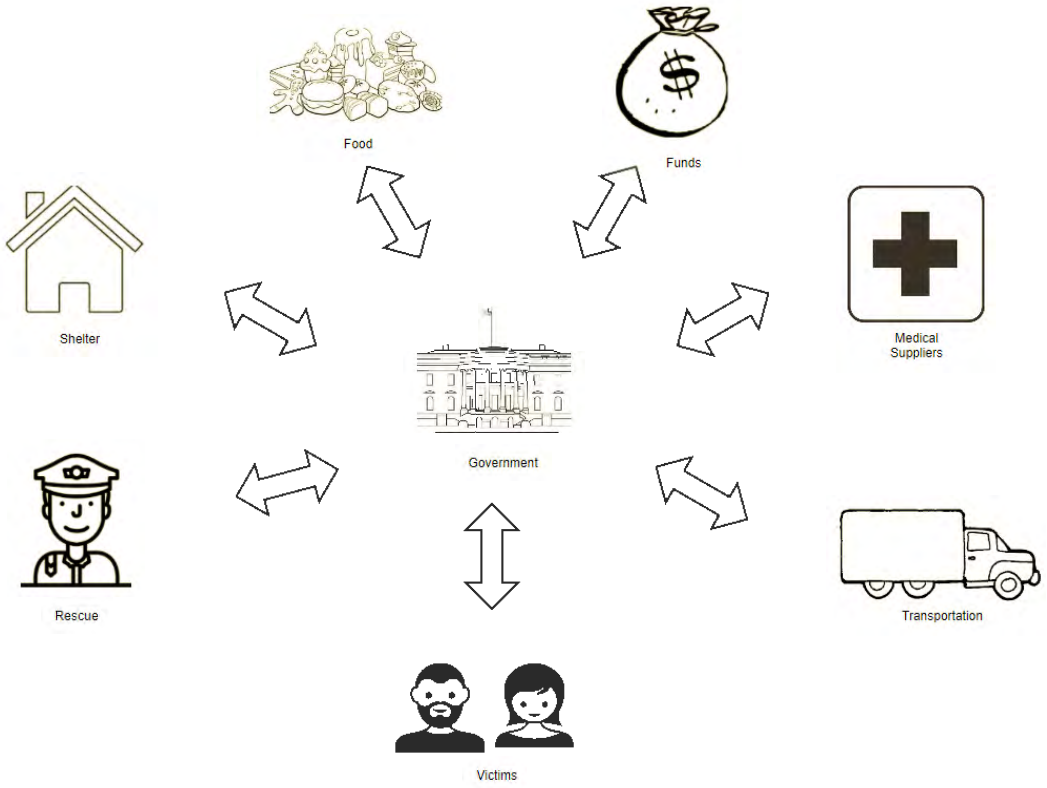

Figure 3.6 Central authority controlling all the transactions of information, requests and funds

As mentioned earlier, a disaster management is first tried to be performed by the local authorities and if it becomes overwhelming for them to handle the situation, the state and federal government is involved in order to provide better disaster management and rescue operations. The Federal Emergency Management Agency (FEMA) is the federal organization which looks into the whole strategy and planning of the disaster management from the ground up level including distribution of help and funds.

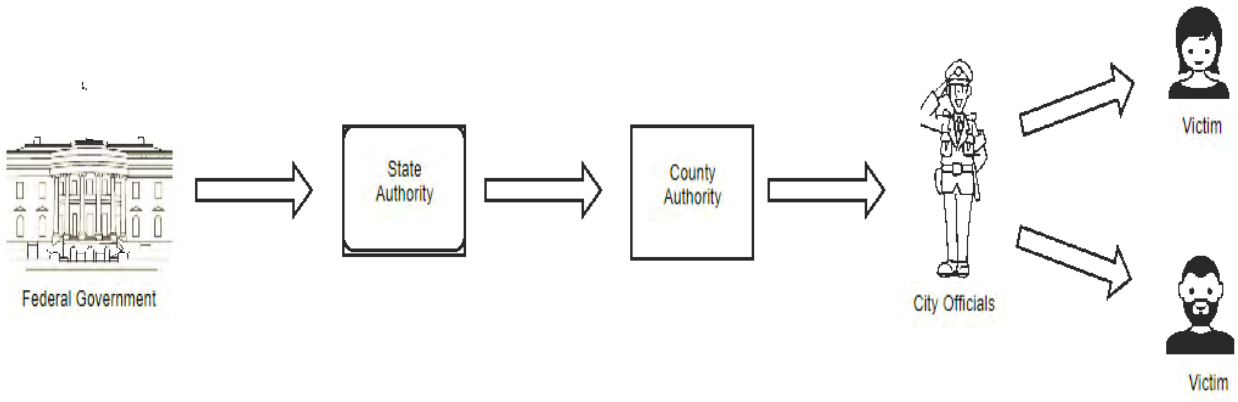

Figure 3.7 Flow of information, help and funds for disaster management

As we can understand from the working model that chances of corruption are way too high in this way of the transaction of money and funds from FEMA or government agencies to the victims. It has been noted that the wake of a natural disaster creates many new opportunities for fraudulent appropriation by public officials, thereby increasing corruption (Milyo, 2013).

Data related to these corruption convictions can be drawn from two distinct sources. The first being the annual report to Congress by the Public Integrity Section (PIN) of the Department of Justice (DOJ).

The second is a research organization affiliated with Syracuse University (TRAC). It maintains a comprehensive database that contains records on all publicly available criminal cases prosecuted in federal courts, including cases brought against federal, state, and local public employees for offenses related to corruption (Cordis, 2013). There have been several complaints filed which are related to corruption during the time of disasters.

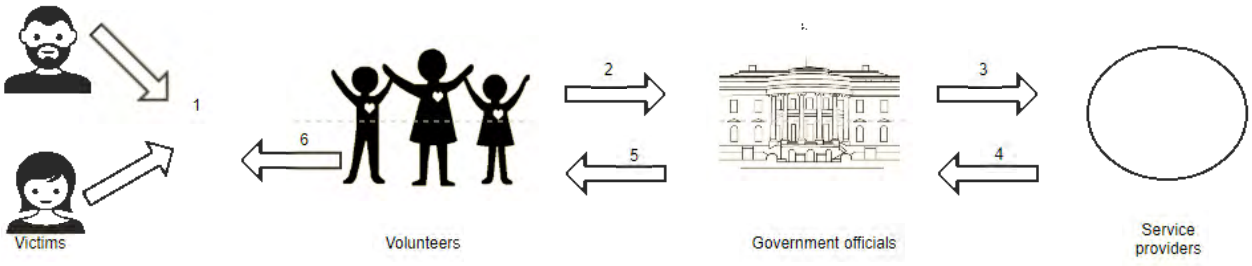

Figure 3.8 Request and delivery of services between the victims and the service providers

Where,

1. Request of services from the victims to the volunteers
2. Volunteers forward the request to the government official (local to state to federal)
3. Government forward the request to the service providers
4. Service providers respond back with their information to the government officials
5. Government officials provide the information to the volunteers
6. Volunteers contact the victims regarding the aid being provided to them

The current model takes a lot of time which eventually delays the process of rescue operations and aid provision. Whereas, the chances and possibilities of corruption are high leading to improper help being provided to the people who actually need them. Because of delay in the rescue operations and improper communications between different service providers, it is comparatively difficult for them to work together and provide better services.

3.2 Current approach towards identity theft

Identity theft happens more often than we might think and it's a very serious crime. It's a crime when your personal information anything from your driver's license, Social Security Number or even your name is stolen or hijacked by a person who plans to impose your identity. With all that information, someone might commit crimes and leave false criminal records in your name. With your social security number, someone can easily get false lines of credit and this might lead to a significant debt in their name.

Identity theft can have a significant effect on the individual's life. It takes a really long time to recover from identity theft. It's hard for the victim to get loans as the credit history would not be proper. There have to be enough justifications for all the false criminal records on his/her name. This leads to a lot of inconveniences and mental trauma for the victim and it affects their lives drastically. There are ways with which one can try to keep their identity safe but there is no surety to the fact that it can actually be saved.

3.2.1 Statistics related to identity theft

Identity theft is a big problem in the financial world and the technology advancements that make it more convenient for thieves to steal one's personal information. There are approximately 12,157,400 victims of theft each year and over 1 Billion records get leaked every year, making all the information vulnerable and open to theft. The Equifax data breach exposed the sensitive personal information of approximately 143 million Americans. The identity theft cases have increased throughout the years; it went up from 10.2 million per year from 2007 to 15.6 million in 2017.

It has been reported that International Revenue Service has paid $5.8 billion in tax fraud to thieves using random Social Security Numbers to file a return. There are 19 victims per minute reported of identity theft in the United States of America (Forbes, credit.com, 2017).

Figure 3.9 Top three identity theft report by types from 2013-2017 (Federal Trade Commission, 2017)

There have been 228,739 reports filed for phone or utilities fraud in 2017, there have been 435,192 reports filed for credit card fraud in 2017. The employment or tax-related fraud in the most frequent occurring identity theft cases reported with 676,054 in 2017. There are other different types of identity theft recorded in 2017.

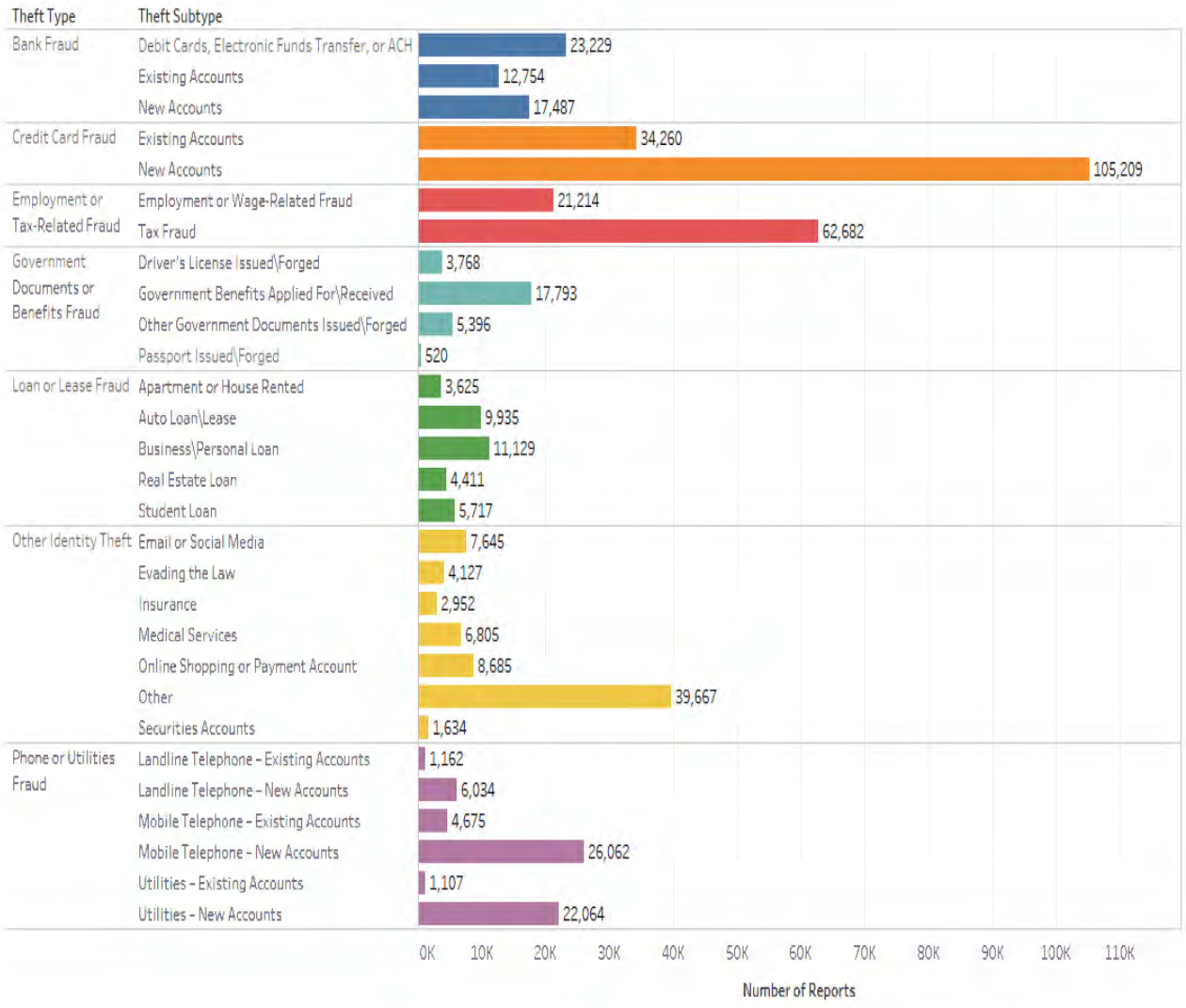

Figure 3.10 Types of identity theft report in 2017 (Federal Trade Commission, 2017)

The identity theft reports can be classified on the basis of the age of the victims. According to figure 4.10, the highest number of reports in 2017 was filed by the victims of age 30-39 years which is 80,467 followed by the range of 40-49 years, third being the age range of 50-59 years. The next being the range of 20-29 years with 61,114 reports in the year 2017. The next range is 70-79 years with 15,979 reports filled. Children below the age of 19 have 13,852 reports filled and 5,359 reports for people above 80 years.

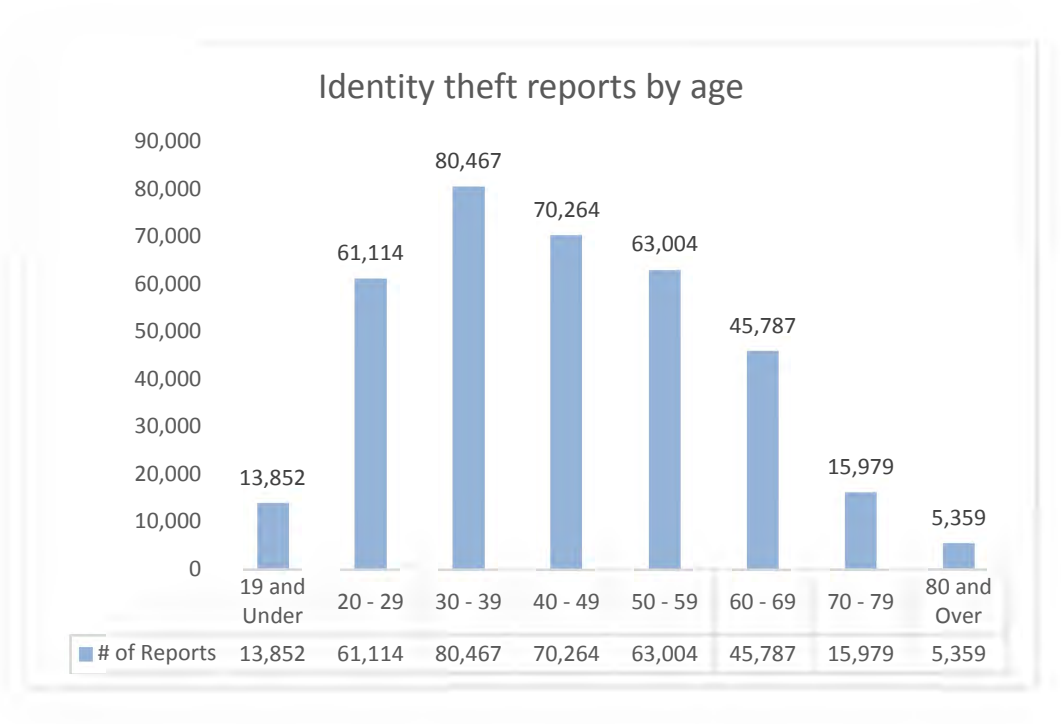

Figure 3.11 Identity theft reports by age in 2017 (Federal Trade Commission, 2017)

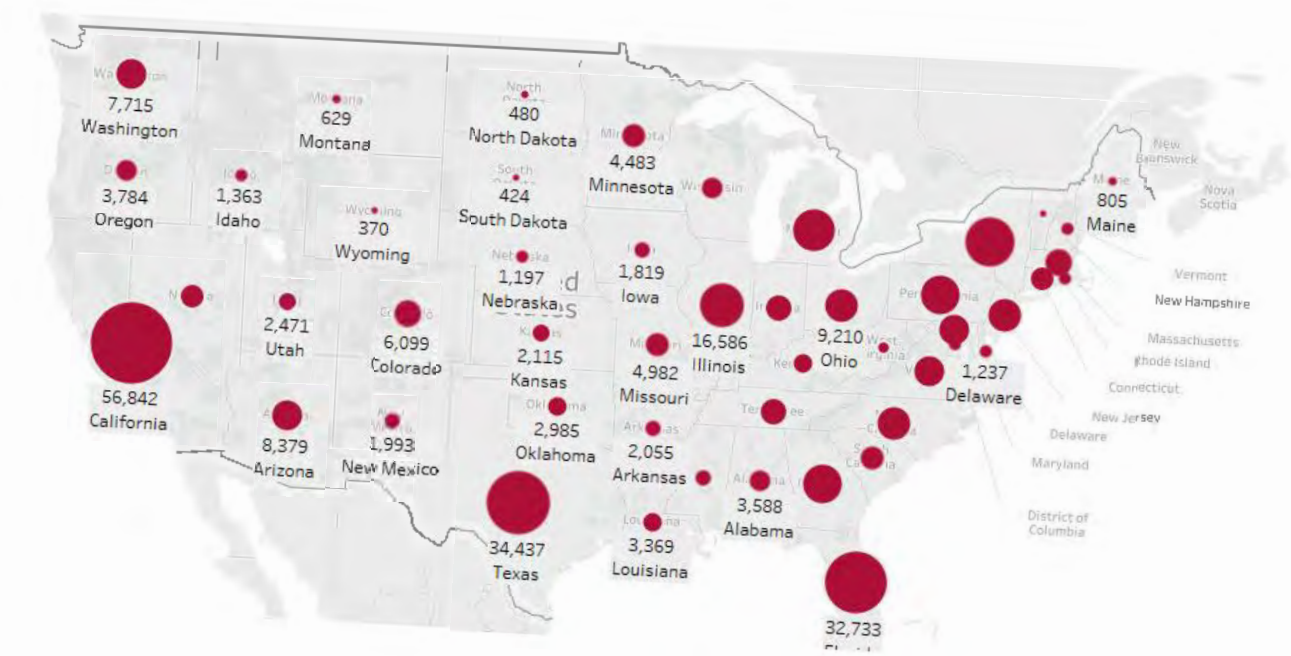

Figure 3.12 Identity theft reports by states (Federal Trade Commission, 2017)

As we can see from figure 4.11 that California is the state is the one with the highest reported identity theft in 2017, followed by Texas with 34,437 reports in 2017. Florida being third with 32,733 reports in 2017. These are the number of thefts that got identified and reported whereas there would be few which are yet to be identified and reported.

The United States federal government is a huge part of the problem with regard to identity theft. They routinely issue erroneous tax return and identity documents. All this information is sent by mail to the respective owner which makes it easy for people to steal it from the mailbox. In 2017, Equifax data breach has proven that absolutely no one is immune to cybercrime.

Most identity theft complaints per capita are reported from District of Columbia and then Michigan and Florida.

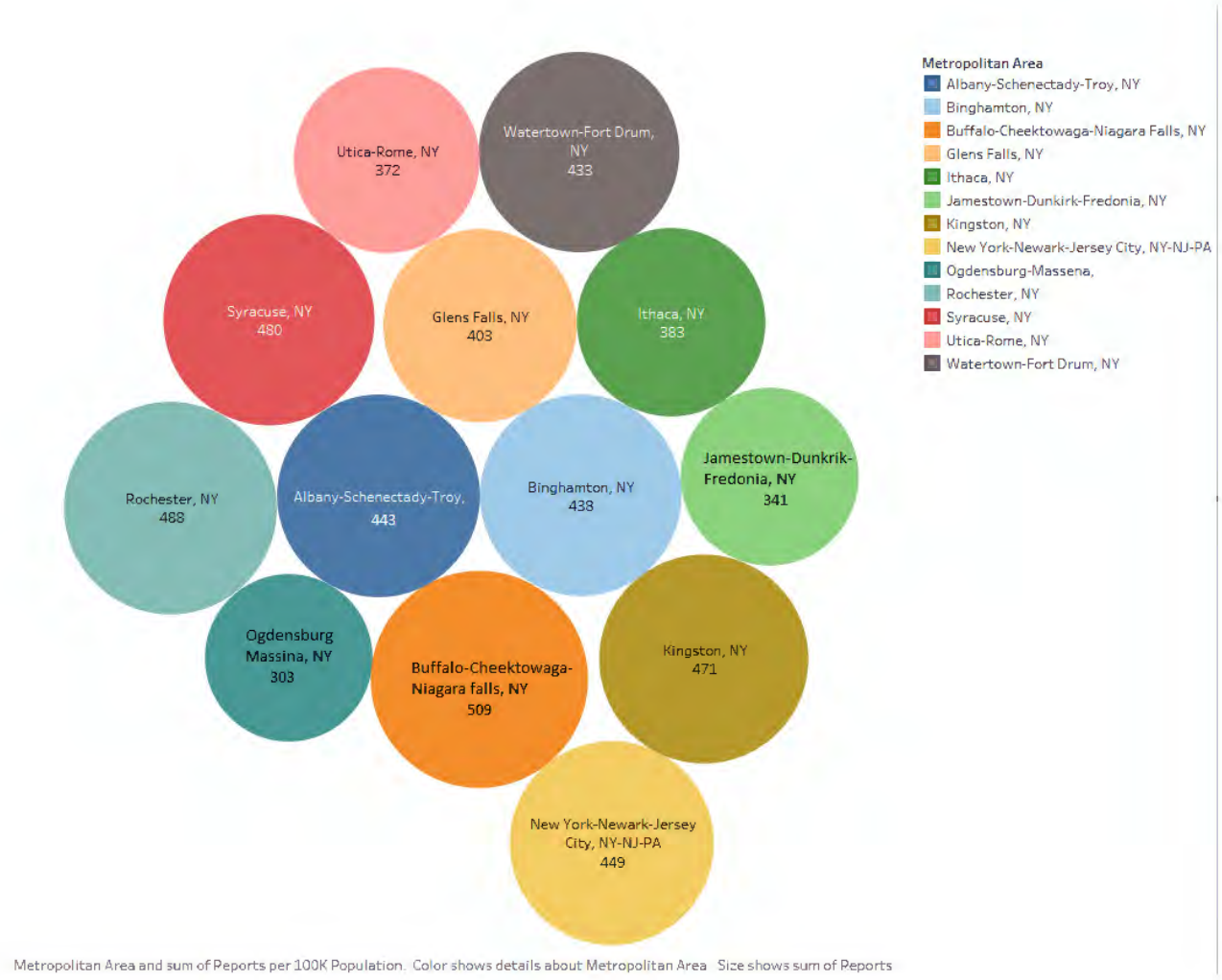

Figure 3.13 Identity theft reports for metropolitan cities in the state of New York (Federal Trade Commission, 2017)

3.2.2 Current methodology of storing identification information

Storing the personal information in today's era follows the centralized network system where a centralized authority is responsible for all the storage of necessary documents and information. But this centralized authority is not limited to the government in all the cases.

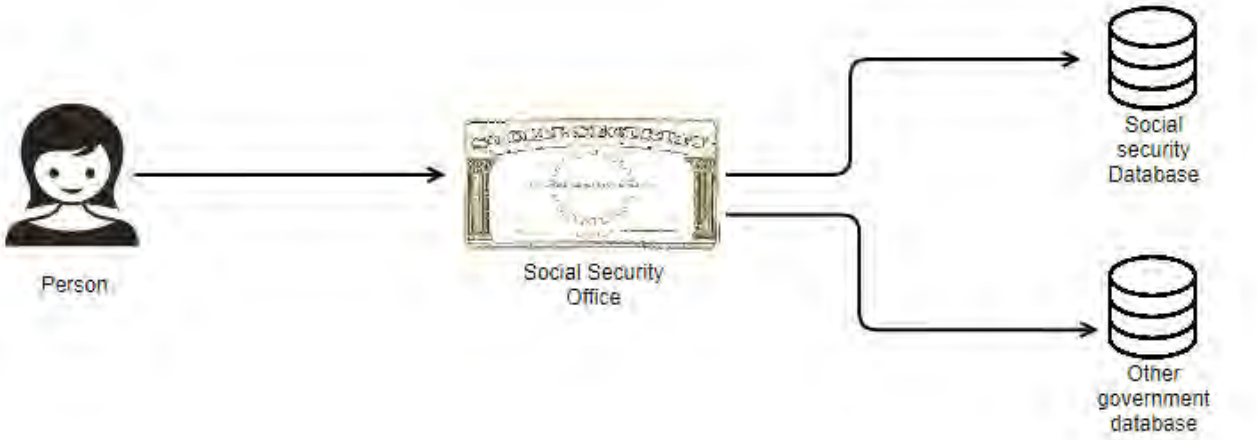

Figure 3.14 Personal information storage by the Social Security Office

All the personal information that is required for the generation of the Social Security card is collected by the Social Security offices and stored in the Social Security database and shared with other governmental agencies which store that data in their respective databases. The personal information required for the generation of the card along with the generated Social Security Number is added to the databases and transferred so that the individual can be identified by the number in case of inquiry.

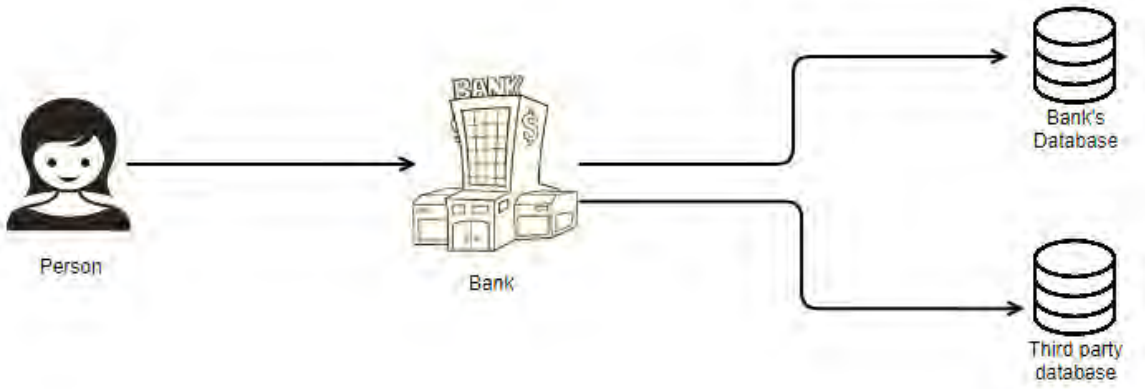

Figure 3.15 Storage of personal information by the banks

All the personal information that is required for the generation of a new bank account is collected by the respective bank officials and stored in their database and shared with other third-party agencies which store that data in their respective databases. And in general, a person has more than one bank account at different organizations. This lead to storage of data at various data bases and keeping a track of it is extremely difficult. Similarly, in case of other services, the central agency or unit stores the data in their respective databases in order to identify the customer in the time of any type of inquiry.

In the United States of America, the three main credit organizations are Equifax, Experian, and Transunion. They also store the information regarding all the citizens of America at their respective databases.

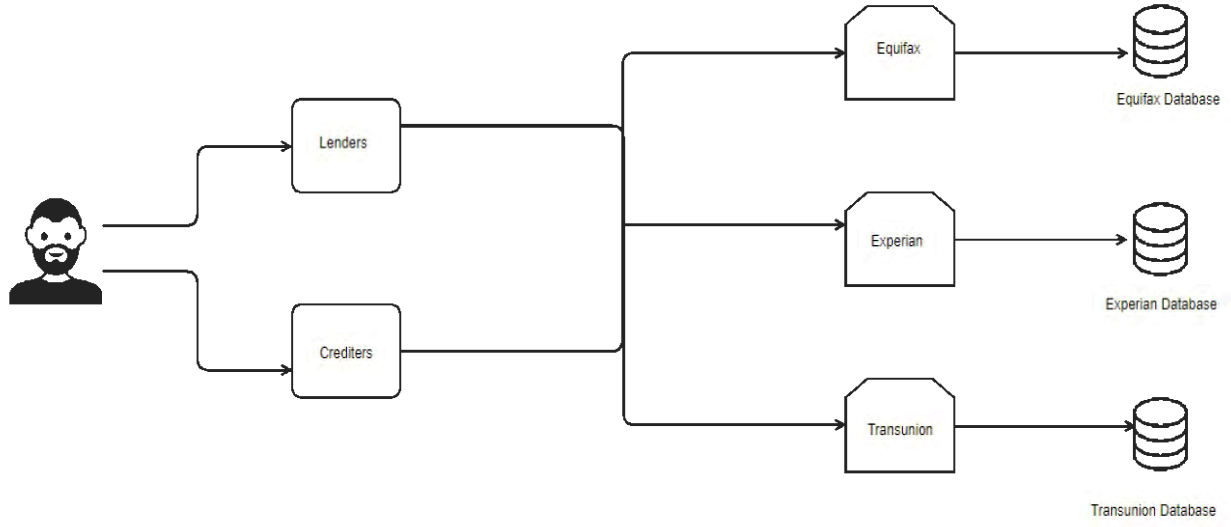

Figure 3.16 Personal information storage by the credit unions

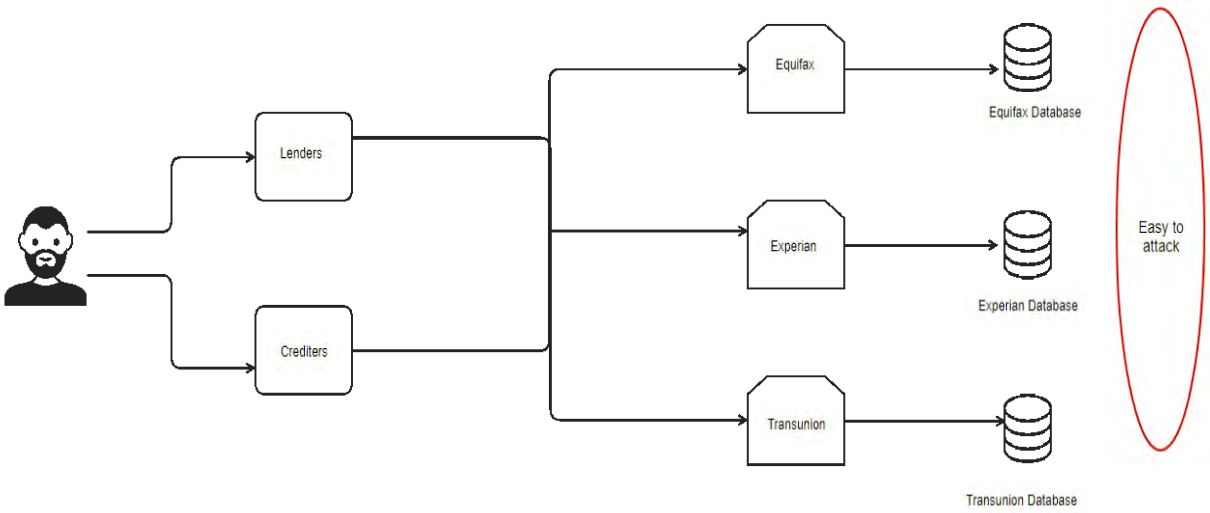

Figure 3.17 Weakness of the personal information storage methodology by the credit unions

All this information is very personal and if leaked can cause a lot of trouble to the person being attacked. The storage of this sensitive data at the various organization and their databases makes it easier for someone to hack the database or manipulate the database in order to retrieve the information and use it for their benefit. The world is getting advanced technologically every other day and it is getting really difficult for organizations to secure their data. As mentioned earlier that the Equifax data breach proved that nothing is safe in this technologically advanced world. Even though the federal government in recent years has taken more aggressive measures to build up our defenses, criminal strategies continue to evolve and grow in sophistication, keeping consumers vulnerable to identity theft and fraud.

3.3 Current approach towards border security

The United States of America is a nation of immigrants and has greatly benefited from legal immigration. The United States Border Patrol (USBP) is an American federal law enforcement agency. Its mission is to detect and prevent illegal aliens, terrorists, and weapons including weapons of mass destruction from entering the United States of America (cbp.gov). This agency works towards maintaining borders that work-facilitate the stream of lawful migration and products while keeping the illicit trafficking of individuals.

The current border security model relies mostly on paper-based documents in order to justify the legality of the immigrant. But the fake paper-based documents can be created in order to commit a fraud. The government of America has spent more than $100 billion dollars over the last decade to fund security measures along the border but the border is still not secure.

There have been a lot of cases reported of illegal immigration and transportation of weapons into the United States of America.

In certain areas and aspects, the border has become more dangerous and lawless over the years which have made the United States of America susceptible to terrorist activities.

In order to truly protect the United States of America and its border, the illegal immigration should be reduced. According to the Custom and Border Protection (CBP) department of the United States of America, the number of traffickers apprehended at U.S borders has steadily increased to nearly half a million from around 200,000. The border patrol are doing an exceptional job at reducing the illegal drug transfer into the U.S at all its borders as understood by the data collected from CBP website. Unfortunately, despite the fact that there are a high number of drugs seized, they are as yet finding their way crosswise over and have a significant effect in numerous states.

At the border security points, it has been noticed that terrorists and people with bad intentions generally steal the identity of someone else, in order to enter the country which makes it easier for them to sneak in the United States of America and work towards their ill goals. Paper-based verification can lead to a high number of frauds and as the information is stored in a centralized unit, it can be manipulated with a little effort by using various technologies.

3.4 Current approach towards weapons of mass destruction

A weapon of mass destruction is a nuclear, radiological, biological, chemical, or other type of weapons that can kill or bring harm to a large number of individuals, property and the atmosphere. According to the Homeland Security, the United States of America faces a rising danger from terrorists and other countries looking forward to using a weapon of mass destruction. There is a specific department that works towards the protection of the country from these harmful weapons, The Office of Weapons of Mass Destruction Terrorism (ISN/WMDT).

Its key mission is to counter the nuclear smuggling. Terrorists could acquire and use smuggled nuclear materials and use them for mass destruction. The office of Weapon of Mass Destruction and Terrorism works in collaboration with partner countries to achieve a common understanding of the smuggling threat in order to prevent, detect and respond to smuggling activities (United States Department of State). In 2016, the top U.S Intelligence official declared gene editing as a weapon of mass destruction as well. The outbreak of a deadly disease may result in a lot of deaths and genetics editing can also lead to a similar result if used with wrong intentions.

The current model has a very little transparency; the most common way of getting radioactive material illegally is by stealing it during its transportation. The radioactive materials are being used at a huge amount in the medicine and other types of industries. They transport it from one place to another and this leaves an open window for the thief to steal it during the transportation.

On the other hand, as the genetics editing is also considered as the weapon of mass destruction, and if any such process is taking place, it is relatively hard to figure it out. Suppose that the research institute that has the deadly viruses stored for further scientific research purposes makes any change to the viruses or someone tries to steal them and use for destruction purposes, no one can actually monitor that. According to the government policies, in addition to zero international reporting requirements, there are zero enforced international standards for storing and transporting radioactive materials (Nuclear Threat Initiative).

CHAPTER 4

Proposed Models

4.1 Disaster management using blockchain

Even though different governmental and non-governmental organizations of a country are quick to respond to the disaster strikes, these efforts often fail because of lack of transparency between different functionality. There is no doubt and denial of the fact the mankind has come way ahead in terms of progress in the field of disaster management and rescue operations. Different countries, various NGO's and people within the affected country and from around the world make sure that the disaster-stricken country is not the lone fighter in the battle against the disaster and crisis situation. They try to donate in one way or another to the affected community. The help is generally in the form of food, shelter, money, medicines, rescue operations, transportation etc.

Governmental organizations that are sent to hazardous situations regularly include defense forces which are, by nature, not enthusiastic about giving insights into their frameworks of activity. Sadly, this sensible hesitance to uncover sensitive data can prompt conceivably lifesaving data being deferred or out of reach. The best quality of these joint efforts can likewise turn into their most prominent shortcoming (Rohr, 2017). She said that:

> "Disaster situations call for the absolute transparency that only a distributed network can provide"

Blockchain technology can be a boon in the area of disaster management as it can behave as the central system of all the operations. All the respective parties can come together and join the blockchain network making it a transparent and distributed way of help provision.

A blockchain solution empowers the key players/associations during disaster management to communicate adequately and follow up on time. It enables the associations to utilize their current ecosystem to facilitate a service and distribute on this system. All transactions are recorded on the system. The record once generated cannot be edited or tampered once created. This way blockchain provides a secure environment. This leads to a generation of trust which supports governance and accountability. Thus blockchain makes sure that a shared distributed ledger is used which ensures transaction, information and data reaches all parties as soon as they are created which leads to early settlements (Mohan, 2017).

The main components of the new proposed method of disaster management using the blockchain technology are the government, medical suppliers, shelter providers, food providers, telecom service providers, residents, transportation providers

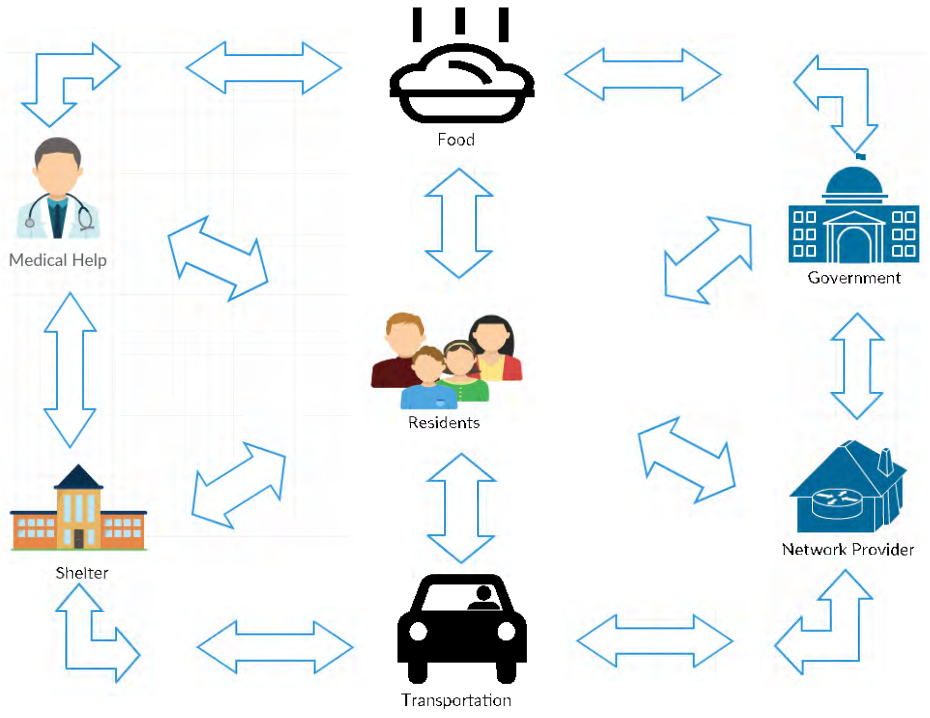

Figure 4.1 The main components of Disaster Management Model

Government

The government should develop an application based on Blockchain where all residents can register by providing their basic information. This application should contain a list of financial institutions, telecom service providers, medical support providers, transportation, relief centers and shelters that individuals can access. With the help of this application, the government can analyze the conditions of the hazard affected citizens in real time and can provide help.

Furthermore, with this Blockchain enabled application, victims can request to locate a missing person. The application can identify a missing person if present in any of the registered shelters. Additionally, this application will be connected to the database in the Blockchain network which would make it next to impossible to tamper with available information. The government can request for the GPS location of the missing people from telecom network providers and then move forward with rescue operations. As the information flow is directed to the government from telecom service providers, rescue time should decrease for affected persons.

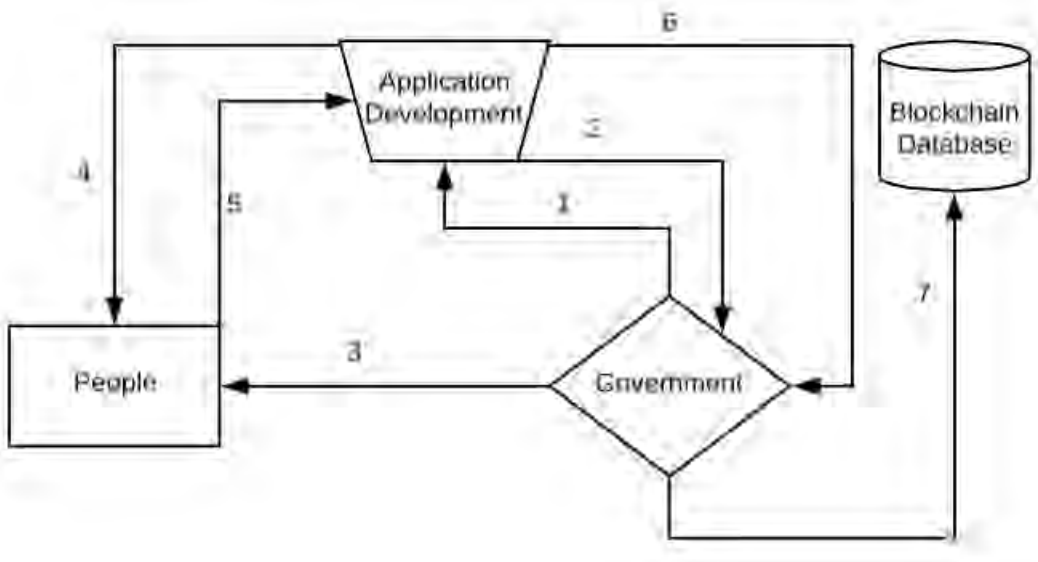

Figure 4.2 Application development model including government

Where,

1. Request of generation of application by government to the application development team
2. The confirmation of generation and active working of the application
3. Government reaching out to people to download and register themselves using their personal information on the application
4. The application development team reaching out to people with the installation details
5. Confirmation of downloading and registering over the application from people
6. All the information regarding the registered users are provided to the government
7. Information gets stored in the blockchain database

Telecom service providers

Service providers can join the application and become a part of the Blockchain network. The Blockchain developers can add the new service provider into the network by updating their contract of operation. The telecom service providers are one of the most important pillars of advanced disaster management as they verify the registered resident's identity and enroll them as the part of the network. These registered service providers should have the ability to share spectrum as the number of people using the network would be higher during crisis situations. The service providers should offer satellite phones and other sorts of wireless communication devices in case the phones of affected individuals stop working. These phones can be used to track their locations and might turn out to be an important tool in the rescue operations. They can also provide emergency wallet to all their registered users and with the help of Blockchain can transfer a certain amount of fund to their wallet, which would be a secure, safe and fast way of performing the transaction (Mohan, 2017).

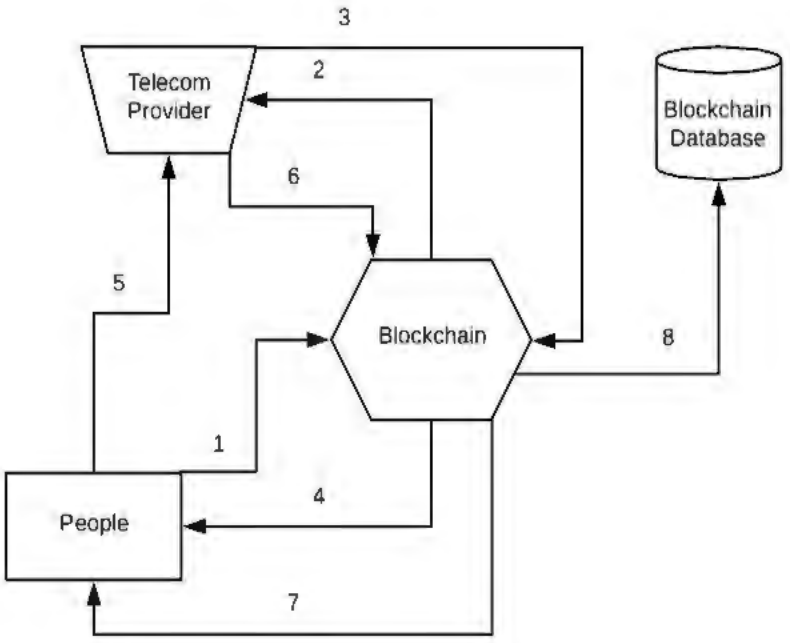

Figure 4.3 Telecom service providers joining the blockchain network

Where,

1. People registering themselves over the blockchain operated application using their mobile number, and other identification details
2. The respective telecom provider is notified regarding the registration
3. Information regarding mobile wallets is provided to the people through blockchain network
4. The information is further made available for people through blockchain network
5. People register for mobile wallets
6. Funds and money are transferred to the mobile wallets through blockchain
7. Money is provided to the people without any extra charges and delay

Shelter

An individual, a group of individuals or an organization that wants to provide their services by offering shelter to affected people can register themselves on the application and give proper information about the type of services they have, examples of that would include information such as the number of beds they have, the amount of food, the types of food and medicines available etc. The application can then match the shelter seeking people to the nearby shelter according to their need. The shelter can constantly update the vacancy information over the app so that more people have knowledge about the availability of space. With the help of this application and the Blockchain network a shelter can directly communicate with the government regarding necessary fund or with the other service providing organizations about their needs and since the communication is direct without the involvement of any third party the needs can be fulfilled faster and without any confusion. The shelter can also notify the government about any individual present at the shelter whose missing report has been filed.

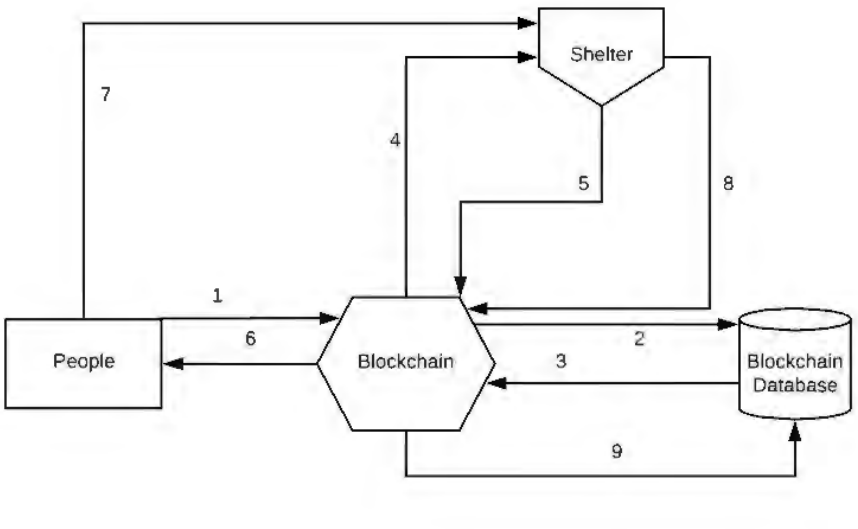

Figure 4.4 Shelter providers joining the blockchain network

Where,

1. People search for shelters by providing information regarding their location and preferences
2. The blockchain network looks in the database for nearby shelter providers
3. Information is provided to the blockchain network
4. The nearby shelter providers are informed about the request raised
5. The shelter provider who believe that they are able to provide the requested services accept the request
6. Information is directly provided to the people through blockchain network regarding the shelter provider
7. People gets in touch with the shelter
8. Information regarding the arrival and the individuals are provided to the blockchain network
9. All this information and data is further stored in the blockchain database for future consideration

Food service providers

Anyone, either an individual, a group of individuals or an organization who is willing to provide their services to the affected community can register themselves on the application and provide proper information to the network regarding which area are they situated in and what kind of food supplies do they have in inventory. The application will further help the food supplies seeking people or shelter to connect directly with the providers via the help of the blockchain network as the request published in the network is visible to all the members in the network and

anyone who has the inventory to provide the requested good can directly be in contact with the people in need. The blockchain network helps to provide direct communication between both the parties. The food service providers can also request for food and ingredients from the government in order to have a stocked inventory and can provide services in case of emergency.

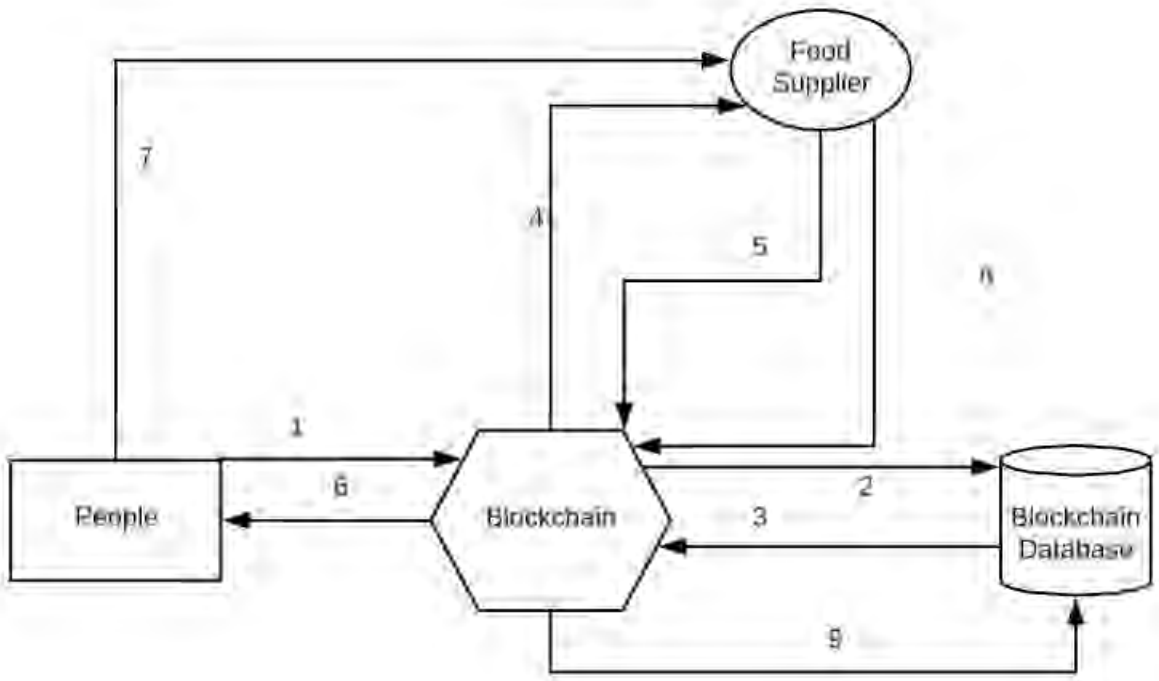

Figure 4.5 Food suppliers joining the blockchain network

Where,

1. Request for food supplies from people with specific requirements
2. Blockchain network provides ability to the app to look for nearby food suppliers in the data base
3. Information regarding these suppliers are provided to the blockchain network
4. The request is being published in the network and all the nearby food suppliers are notified
5. The food suppliers accept the request
6. People are notified about the food suppliers
7. Food services are provided to people
8. All the information and data is published in blockchain network
9. Everything gets stored in the blockchain database for future consideration

Medical service providers

Medical service providers can also register themselves in the application for free and Blockchain developers can add them to the network. There is no need for a third party for communication. If residents want to communicate directly with the medical service provider, they can connect with them over the application without relying on the first responders. In that case, no misuse of the patent information can take place and confidential information can remain confidential. Medical service providers can update the information regarding medicines and can send medical practitioners to the requested area. The medical service providers can work closely with the telecom company to work on the basis of electronic priority.

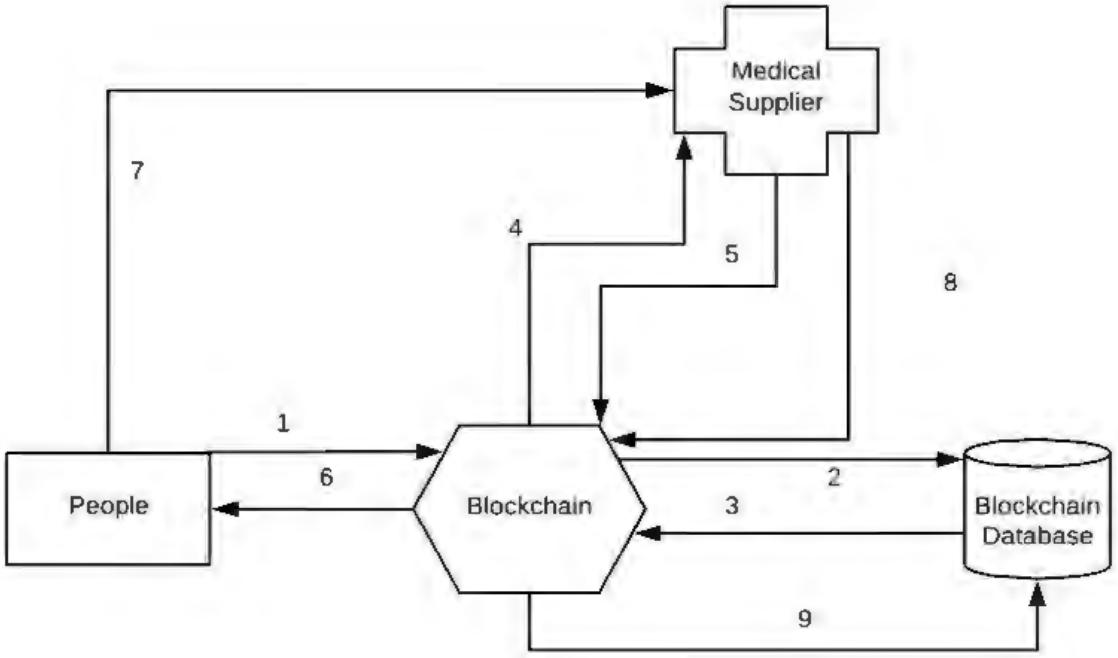

Figure 4.6 Medical service providers joining the blockchain network

Where,

1. Request for medical supplies from people with specific requirements
2. Blockchain network provides ability to the app to look for nearby medical service providers in the data base
3. Information regarding these suppliers are provided to the blockchain network
4. The request is being published in the network and all the nearby medical service providers are notified
5. The medical service providers accept the request
6. People are notified about them
7. Medical services are provided to people
8. All the information and data is published in blockchain network
9. Everything gets stored in the blockchain database for future consideration

Transportation

The transportation organizations can also register on the application for free and then can be added to the Blockchain network. These service providers can offer information regarding the area and the location supported. They can also update the information regarding the type of transportation they can provide and can publish data on the application regarding all the people they have helped to move from the disaster site to a shelter. The shelter can contact these organizations directly through the Blockchain network and request for the necessary transportation facilities.

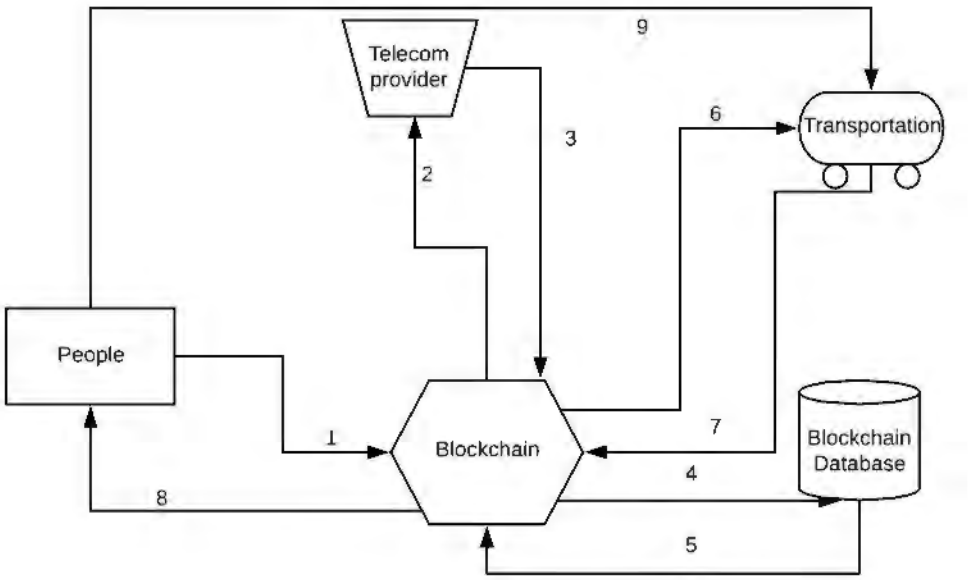

Figure 4.7 Transportation service providers joining the blockchain network

Where,

1. The person in need raises a request in the blockchain network for transportation
2. The blockchain network requests for GPS location of the person who requested services
3. Telecom service provider provides the GPS location
4. Nearby service providers are selected from the database
5. The information regarding the nearby providers are provided to the blockchain network
6. The request is published in the network for the nearby service providers
7. The one willing to help responds to the network so that everyone can keep a track of it
8. Information regarding the service provider is provided to the people in need
9. People and service provider communicate directly

Fund allocation

There are times when an affected person or family runs out of money and are in need of some funds and as per the current way of fund allocation the money will get transferred from government to different departments in a chained format which eventually delays the fund transfer process and increase the chances of corruption and manipulation of the allocated money. If the victim requests for funds through a blockchain network the request will get published in the network and all the members can check and verify the transaction while the anonymity of the requester is intact. The government official may verify the authenticity of the request by asking for the GPS location of the requester from the telecom department and tallying it with the condition of the area so that no fraud can be committed (Mohan, 2017).

The whole process is quick, safe and reliable and the funds are updated in the mobile wallet of the requestor which can be cashed out at certain government verified offices.

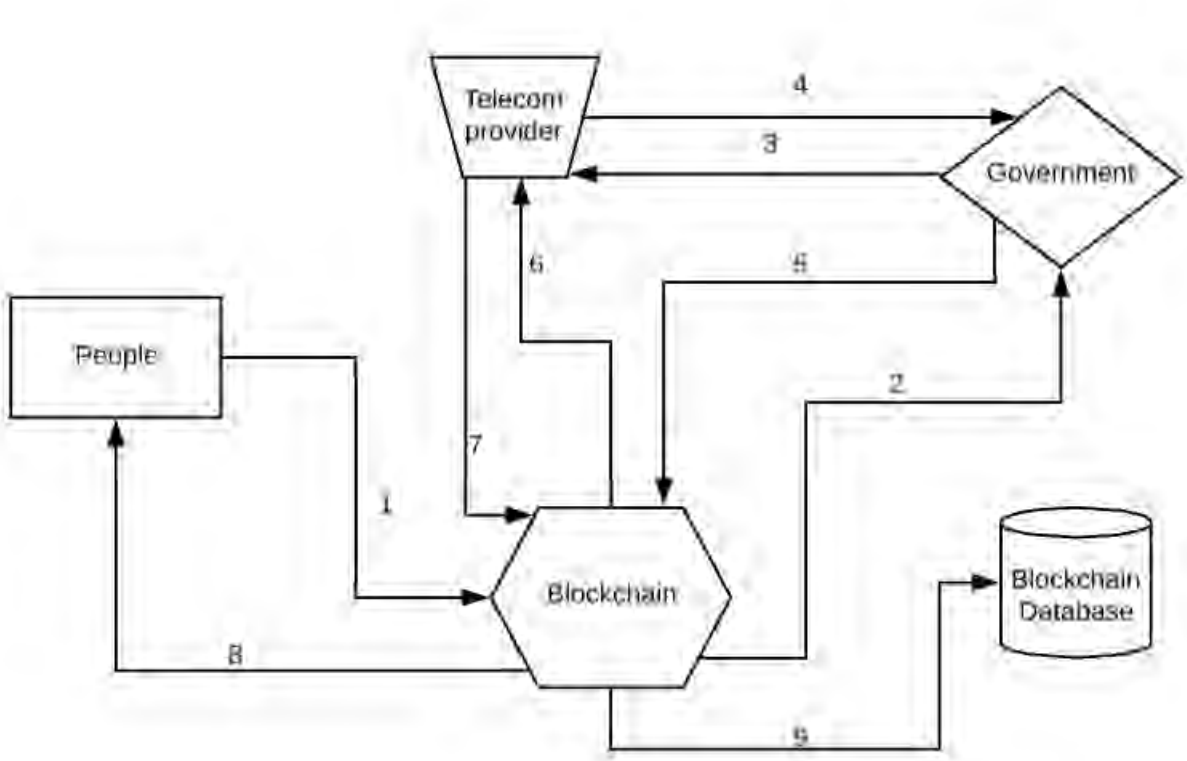

Figure 4.8 Fund allocations from government to the person in need with the help of blockchain network

Where,

1. Request for funds are initiated by the victim and is published in the network
2. Government officials dealing with fund allocation is notified
3. Government official asks for GPS location for the verification of the losses and request
4. GPS location is provided and condition is confirmed
5. Access of funds

6. Request for updating funds in mobile wallet
7. Request is accepted by the telecom service provider and money is transferred through blockchain network
8. Money reaches the victim directly without the transfer of funds from one department to another
9. All the information gets stored from the network to the blockchain database

Combination model

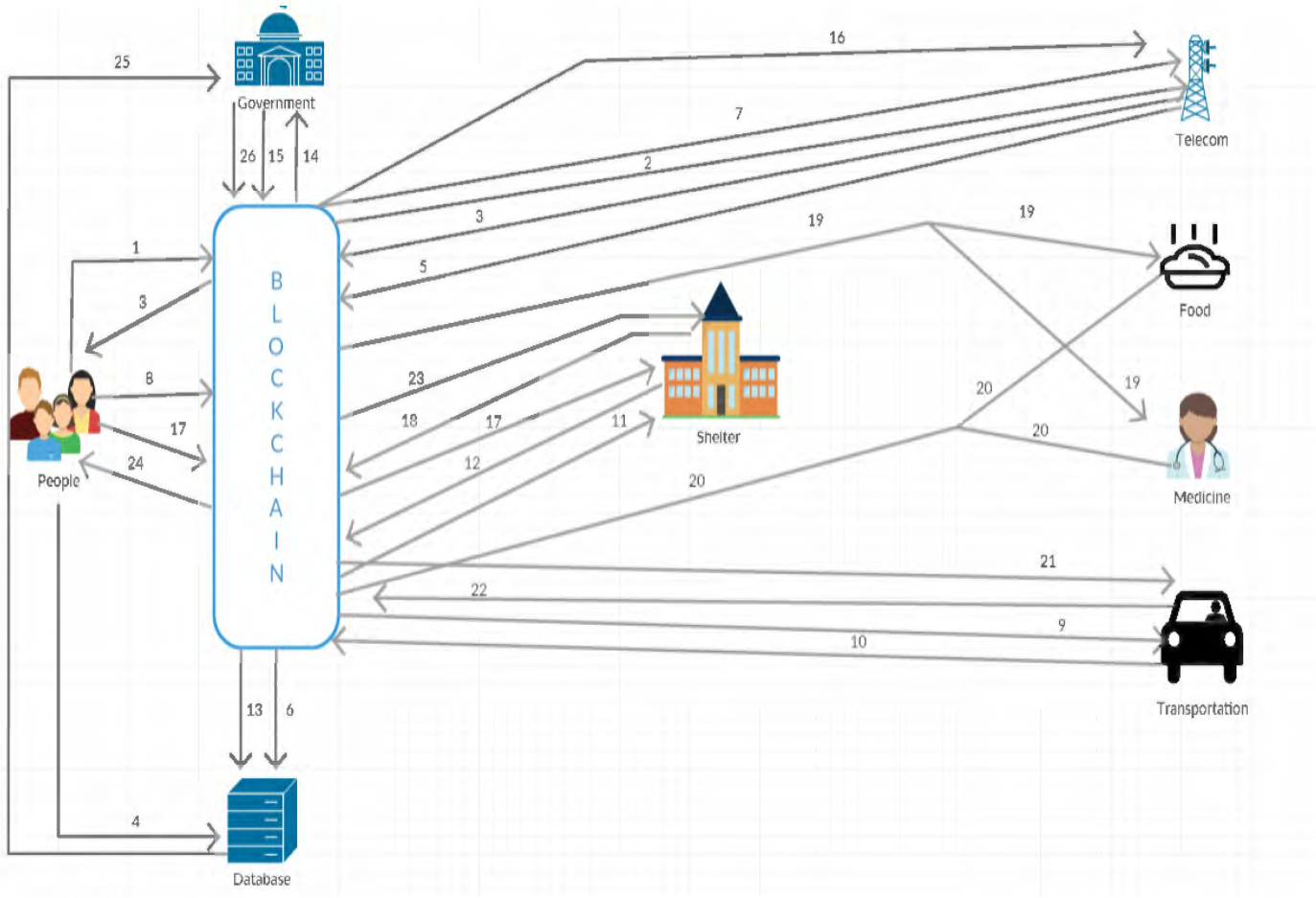

Figure 4.9: A combined model containing all the components working together in a blockchain network

Where,

1. The people register on the application with their mobile number (Name, address, profession, etc.)
2. The telecom provider verifies the user request that is sent to them based on the basis of the user's mobile number
3. After the verification the user profile is created on the application
4. All the information is stored in the Blockchain database
5. The telecom network providers request to join the network
6. The identity of the service provider is verified and they are enrolled as a member of the network
7. Through Blockchain, service providers receive requests for supplies and services
8. People who are stuck in the hazardous areas can request for transportation
9. The request is further sent to all relevant transporters via Blockchain
10. The transporters accept the request and Blockchain helps to link the respective parties on the basis of their response to request. (First come first serve basis)
11. The shelter is informed of the new booking by Blockchain regarding the people who requested for transportation from an unsafe place to the shelter.
12. The shelter then update the vacancy and the individual's detail in the network
13. All this information is stored in the database which can be used for future study
14. The government analyses the data and study the conditions of the effected people
15. If there is a missing person request, the government requests for GPS coordinate of missing residents from the telecom service provider via Blockchain

16. The telecom service provider gives the information to the government in a fast and secure way
17. People request shelter for necessities like food, water, medicines and medical help
18. Shelter requests the network to provide the necessary supplies
19. The Blockchain network directly connects the shelter to the food and medical suppliers
20. The service providers request for transportation of supplies and medical practitioners
21. They are connected to the respective transporters and communication is fast and effective
22. The information regarding the respective shelter is provided to the transporter
23. Supplies are provided to the shelter and the data base is updated about the resources
24. The supplies thus reach the respective resident who requested for it
25. All the information stored in the database can be analyzed by the government and studied to provide better relief in future
26. The government keeps all the information in the Blockchain network, so that no one change, manipulate, tamper or delete it

All these models can work together in order to provide efficient disaster management, reducing the delay in provision of funds, help or services to the affected individual or a group of individuals.

During the whole process, the identity of the individual is safe in the Blockchain network and all the personal information is kept confidential. The whole purpose of the proposed model is to reduce the delay in time and provision of faster, safer, secure and effective disaster management and rescue operation.

Consider a specific area under the effects of the hazard. Without the application, there would be no direct communication between the medical supplier, food supplier, water supplier, transportation supplier etc. This may result in uneven distribution of resources or allocation of resources without the actual need at a specific region. With the help of the application, all the providers can be in contact with each other and the residents who are looking for resources. It will reduce the time of delivery, the waste of resources and all members of the network will get what they need. On the other hand, all the information would be updated on the application as it works on the Blockchain principle, the government can directly analyze the situation and needs of the residents and provide more funds in order to rescue people.

4.2 Reducing the frequency of identity theft using blockchain

In today's world, the area with the biggest and the fastest growth that we can notice is in the technology. The technological advances have eventually played a huge role in the sudden increase in the cases of identity theft. The personal and confidential information is required for most of the important transactions, loans, and purchasing of expensive items. As the sources of these services are different all the personal information is stored at various databases at various organizations which make it vulnerable. It is comparatively easy for someone to steal all these information. In 2017, 16.7 million people have affected by identity theft and around $17 billion dollars were stolen.

There are some signs of identity theft, which include: receiving bills for items that we didn't buy, accounts that we don't recognize, medical services that we didn't use, unexplained withdrawals from bank accounts, notification regarding more than one tax return filed.

Few people refer identity theft as the new millennium's crime. This crime can be accomplished anonymously, by different means, and leaving a devastating impact on the victims life. Any activity in which identity and personal information are shared creates an easy opportunity for the thief to steal someone's identity (Hoar, 2001). As majority of the people use their Social Security number and other private information at various places in order to confirm identity, it is comparatively difficult to keep it same from someone accessing all private information. Even though consumers can take precautionary measures to secure their identity but there is nothing they can do to guarantee that it would not happen (Hornung, 2002).

Blockchain technology can help to reduce the frequency of identity theft by acting as a secure network to store personal information. The consumers and all the participating party can come to an agreement of being part of the blockchain network in order to perform all sort of transaction. The possibility of providing control to the consumers over what kind of information and how much of it they want to share with the other party makes it easier for the consumer to have better control over their private details and can reduce the risk of their identity getting stolen.

Part 1

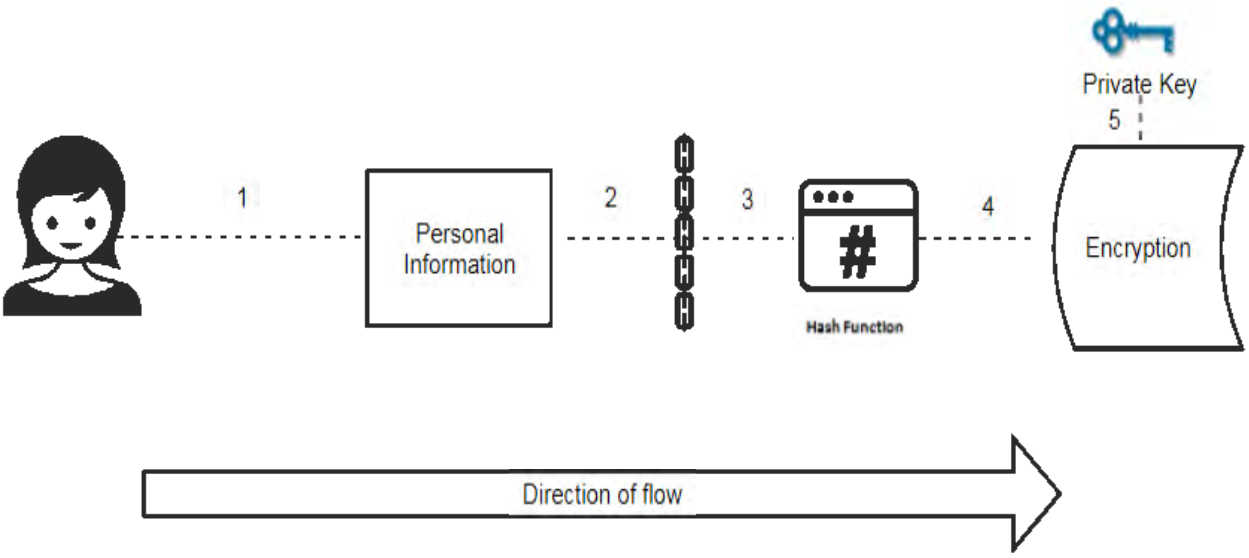

Figure 4.10: Conversion of information to encrypted document using blockchain

Where,

1. The personal information is collected at a portal
2. This information is further converted in to 256 byte hash function using blockchain network
3. The combination of hash function are combined together
4. All the information is stored as an encrypted document with a private key only available to the owner

This encrypted information can be provided to the respective party for further transaction and a public key can be provided to them in order to verify the information. This will work as follow:

Part 2

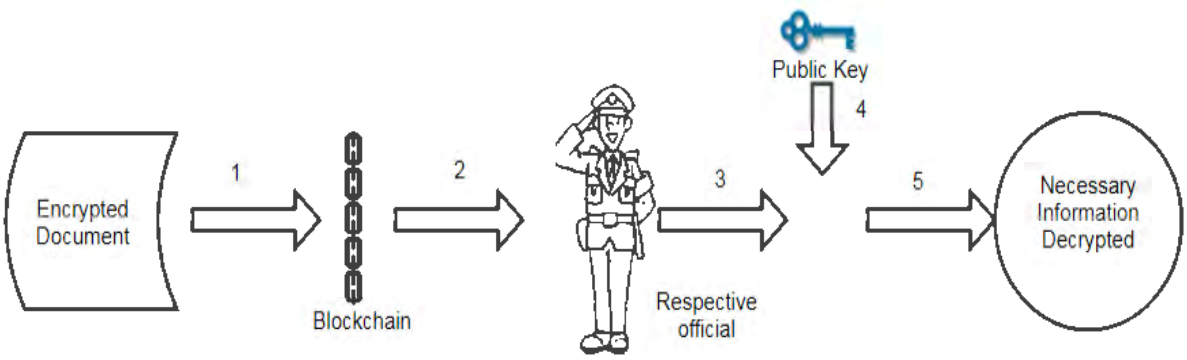

Figure 4.11: Conversion of encrypted information to decrypted document using public key

Where,

1. The encrypted document generated from part 1 is published in the blockchain network
2. The information is then accepted by the respective official who need to verify the details
3. With the help of the public key provided the information can be decrypted
4. Public key matches the details with the private key and decrypt the information
5. Necessary information is gained

The public key will only work and provide the decrypted information if the information is encrypted using the appropriate private key. And the owner has the ability to provide the public key to the respective official or the other party. The information would not be stored at a specific database which is vulnerable and available to be stolen at any time. The information is going to be in the blockchain network making it difficult for anyone to steal it. In order to do so, the thief has to use all the super computers present in the world all together but still the possibility of the thief being able to steal the information is next to impossible.

As the private key is only available to the respective owner and no one in the world has an idea about what combination it is, it makes it extremely difficult for someone to steal the information and use it for their personal benefit.

4.3 Blockchain and border security

The population of the world keeps on increasing and so does the globalization. These two aspects are the most important reason for people, or a group of people migrating from one country to another in order to seek better education, employment opportunity or medical services. In this period when nations and populations are progressively presented to the openings and dangers related to the consistently growing worldwide movement of individuals, there ought to be appropriate border control, administration, and security. The United State of America has been facing this problem of illegal immigrants moving in the country without a proper channel. A lot of people commit fraud by generating false paperwork including fake passports, making it difficult for the security officials to keep a track and control over these people getting in the country claiming to be someone else. On the other hand, there are cases where illegal and harmful substances or goods are smuggled into the country through various ways especially via road transportation.

Blockchain technologies can be used to keep a track of all the verified transportation organizations whose vehicles pass through the border and all the individuals who are willing to enter the country. Blockchain network being immutable, safe and fast reduces the risk of illegal transportation of goods or individuals in the specific country.

Step 1: Registering on the government portal

Government should come up with a portal where it is mandatory for all the citizens of the country to register themselves. The portal is based on the blockchain network and a technology, making it secures and safe for everyone to provide information regarding themselves.

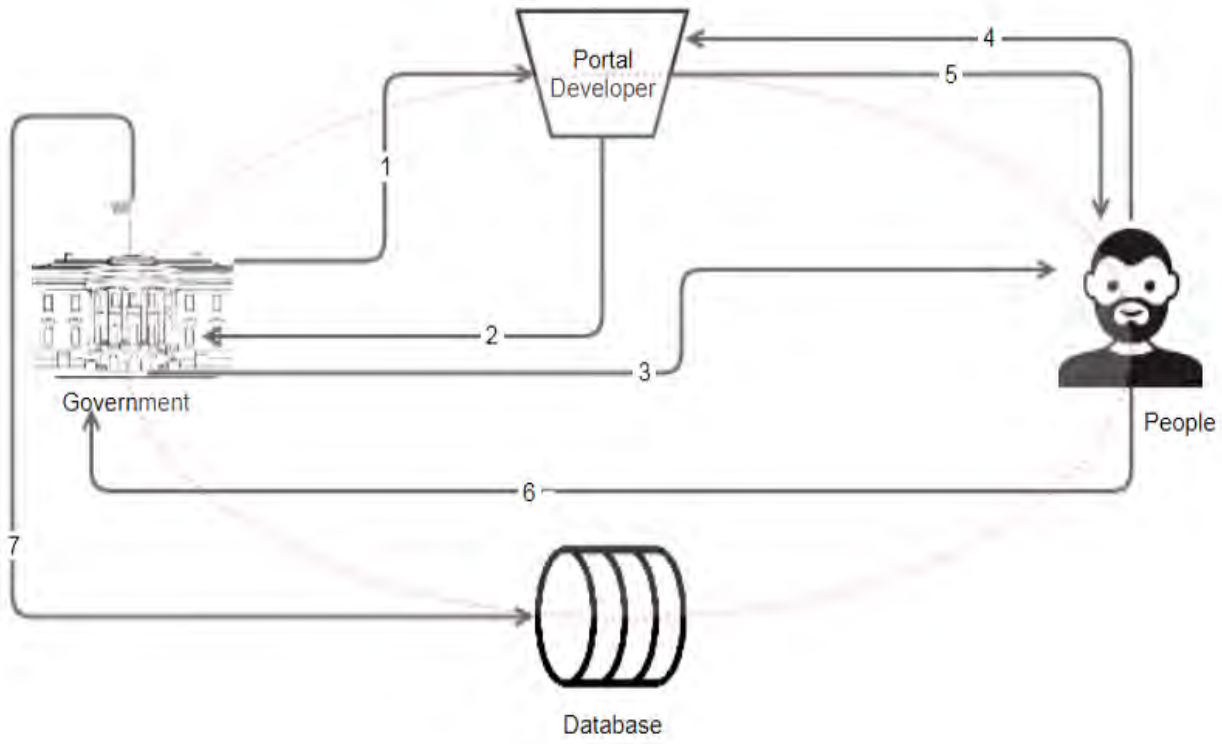

Figure 4.12: People registering on the blockchain portal using their personal information

Where,

1. Government requests the developer team to develop a portal which works on basis of blockchain technology
2. The team provides confirmation to the government regarding the development of the portal
3. Government makes it mandatory for every citizen to register on the portal using their personal information and biometrics
4. People register over the portal
5. Unique identification code is generated and provided to the people
6. People provide confirmation to the government agencies dealing with this whole process
7. All the information is saved in a blockchain based data base

Step 2: Use of the identification code generated

The identification code generated can be used to verify the identity of an individual before they enter a specific country. As the identification code generated is based on the unique biometric of an individual as well as all the information which is only known to the respective individual. This makes it comparatively difficult for someone to enter a country with false documentation or it would be impossible for someone to adapt identity of someone else.

Now, when a person registers him over the portal all his information is encrypted and a unique hash function is developed. The owner of the information has the ability to set private and public key as well. Private key is only known to the respective individual and public key can be provided to the other person with whom s/he plans to share all the information. The public key will only function properly and allow access to the information only if the combination of private key and the hash matches with combination for public key. Therefore if someone has no knowledge regarding the private key and the personal information, it is impossible to generate the same hash function over the portal, which makes it next to impossible to commit fraud or to pretend to be someone else in order to enter a specific country.

4.4 Blockchain and resilient communication

Blockchain can play an efficient role when it comes to communicating highly confidential information from one department or one person to another. There are times when such highly confidential information gets leaked and causes a lot of trouble as it might compromise the safety of the people of a nation. On, the other hand from years various countries have been using code languages to communicate with their army or other governmental authorities in order to strategize their next move. With the help of blockchain, the information could be transferred from point A to point B without any chance or risk of misuse or leaking. It could reach the receiver in the exact same way as it was sent by the sender. There would be less loss of time and information can be conveyed in a faster, secure and immutable manner.

4.5 Blockchain and Weapon of Mass Destruction (WMD)

The current system of handling of deadly weapon and viruses which might cause deaths and harm to a huge amount of people is not very transparent. Whether it is related to manipulation of genes, radioactive materials or the transportation of such harmful substances, the system works in a closed manner with little to no availability of real-time status of their location and condition.

The radioactive material, when used for harmful reasons, may cause a lot of harm to a huge number of people. Radioactive materials are used for medical purposes by a lot of medical organizations in small amounts. This is further stored in the organization and is transported from one place to another making it vulnerable to theft and manipulation.

Blockchain technologies can be used to keep a track of all the organizations which deals with radioactive materials and their vehicles which pass through the international border. Blockchain network being immutable, safe and fast reduces the risk of theft or improper use of these materials. Blockchain technology can also be used to monitor the harmful viruses and their research procedure.

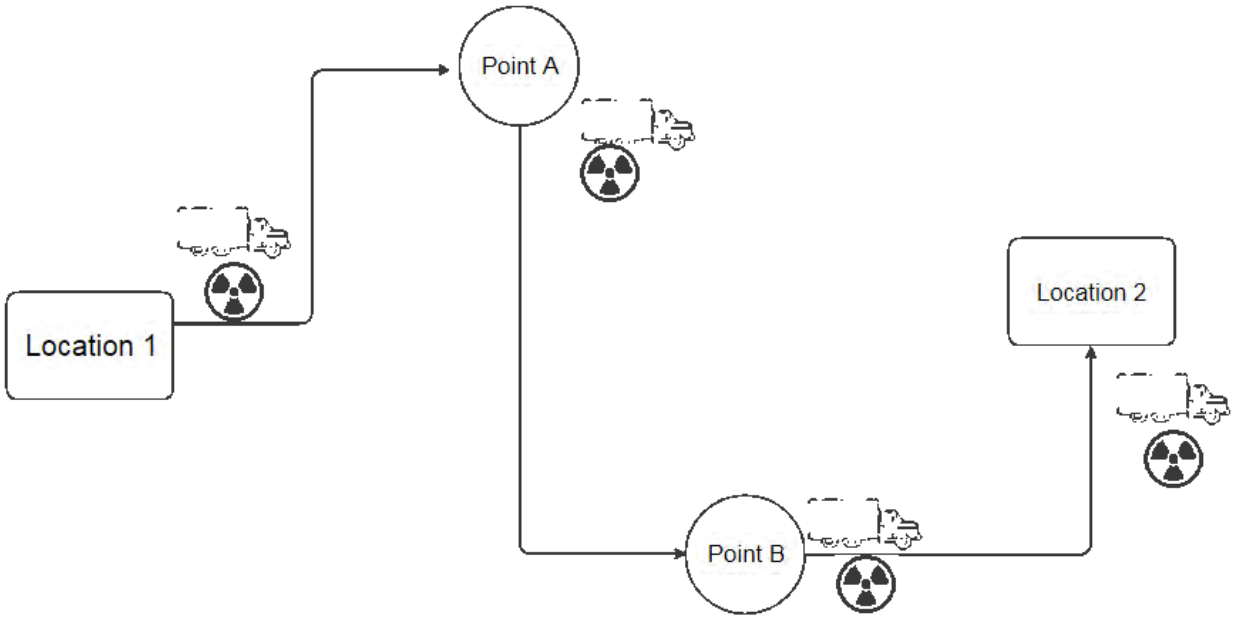

Figure 4.13: Transportation of radioactive material from location 1 to location 2

In figure 4.11, the transportation of radioactive material from location 1 to location 2 is shown. But the points A and B are the places where the vehicles stop and the driver takes a break. These points are vulnerable to risk of attack. Thieves try to steal small amount of radioactive materials from these vehicles so that the robbery remains unnoticed. If anything happens during the transportation of such elements and the robbery remains unnoticed, then it would be easier for the thieves to use it for wrong purposes.

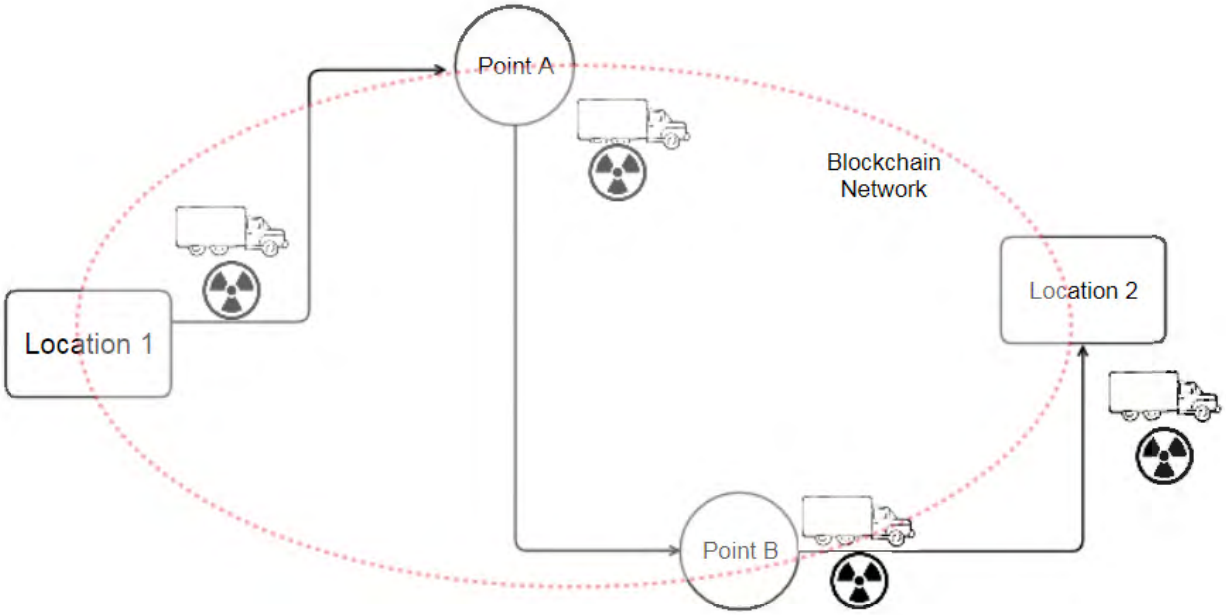

Figure 4.14: Transportation of radioactive material from location 1 to location 2 using blockchain network

With the use of blockchain technology and its traceability and immutability feature, it is comparatively difficult for the thieves to steal the elements. Suppose a situation where the supply chain system is based on the blockchain technology and the radioactive materials are being transported. The specific quantity of the material will generate a specific unique code and even if there is a loss of very little amount of material, every member in the system would be notified about it. With the implementation of smart contracts and blockchain together, the nearest police force would be informed about the theft and the search for the thieves can be restricted to a specific area. Thus even a slight change can be identified and thus the harmful effects can be reduced.

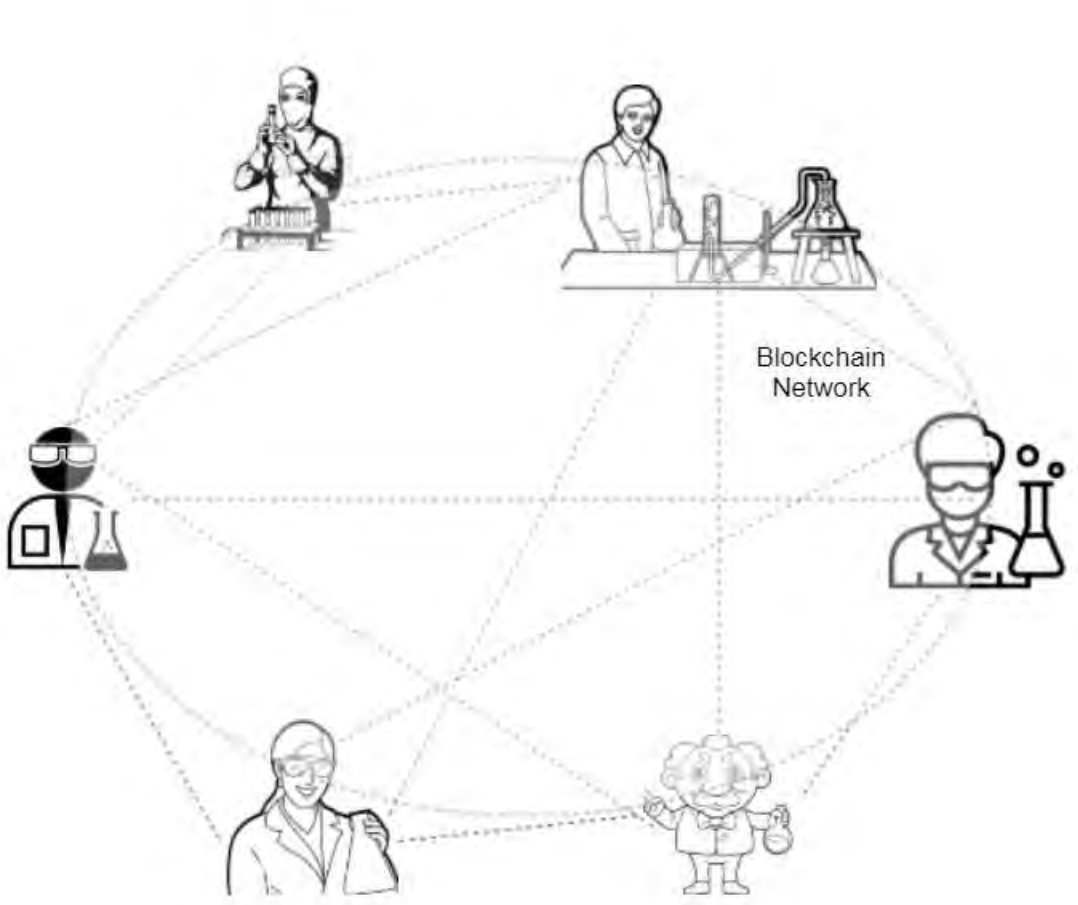

Figure 4.15: Research work on the genes and harmful viruses using a blockchain network

As mentioned above that since 2016, genetic editing is considered as a weapon of mass destruction. But still this process takes place under strict supervision and isolated research labs in order to treat various diseases. If the whole lab and its functioning is not a decentralized system it would be difficult for the central authority to keep a track of all the scientists working in different streams with different genes.

Blockchain network and technology can be used to supervise the research work and if anyone in the research group tries to use the technology for bad purposes, the network has to verify it before the information can be sent to the different place or authority. Similarly, working on the harmful viruses can also be monitored. The place of storage and quantity of the virus can be stored on the network and authorized access should be provided to the area. Thus, if anyone tries to work with it the information would be transmitted throughout the network and the lab access report would also be shared on the network. If some tries to steal the viruses or manipulate with them the entire network would be informed. Thus, restricting the spread of such deadly and lethal viruses in the world.

Blockchain technology can be used to keep a track op each and every small move and process at such places and because of its immutable capability; no one can actually hack it and change the records according to their will.

CHAPTER 5

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

5.1 Conclusion

Blockchain allows organizations to facilitate a service and publish on the network using their existing ecosystem. All the transactions taking place are stored in the network. It provides an immutability feature by offering a secure network where a record once created can't be tampered or deleted. Since it works on a shared distributed ledger system, it ensures that the data and transactions reach the respective parties as soon as they are created. This leads to early settlements.

This study stated solutions for 4 major questions which are:

- What is blockchain and how does it work?
- Can a blockchain network provide better disaster management?
- Can a blockchain network be used for safer storage of private information and reduce the possibilities of identity theft?
- Can blockchain network and technology be used to provide better national security in terms of border security and the weapon of mass destruction?

The study was focused on how blockchain technology and the network can be used to provide relief and better disaster management along with how the frequency of identity theft and people entering a country illegally or by committing fraud can be reduced. Throughout the study, various models are introduced with the implementation of which all these problems can be reduced to a certain extent. The traceability functionality of blockchain is one of the most important tools when it comes to keeping the track of shipment or transportation of radioactive goods from one place to another.

And it is hard to say whether using Blockchain in the disaster management and rescue operations techniques will completely eradicate the loss of life and property, but it should help to reduce the intensity of the losses.

The measurable gains in efficiency, transparency, and immutability obtained by using blockchain in relief and disaster management will save lives which will save more than time and money.

With the help of blockchain network concerning parties can communicate with each other while keeping all the information confidential and secure. Blockchain would make it really hard for anyone to steal funds or information as in order to do so, the person or group of people will have to overcome not only the specific block but the entire chain linked to it. As blockchain works on these 3 ‘Ds’, Decentralized network, Distributed ledger, and Data Structure which help to keep the network as a community where there is no single party which owns it and all the parties have the power to execute the transactions in real time. Validation of a transaction is done by all the members of the network. As the blocks keep on piling over each other with validation to the preceding block it is hard to delete or alter anything. Although all the members will have the visibility on all the transactions, they will not know about who owns the transaction unless you are part of the transacting parties.

This helps to keep the identity of a person safe, reduces the chances of misuse and theft. During the use of personal information, the hash encrypted documents would be transferred using the blockchain network and no one can see the decrypted version except the concerned parties with private and public keys. Blockchain techniques and technology can be used to develop a better performing system for better disaster management, reducing the frequency of identity theft, and provision of better national security if implemented properly

5.2 Future research direction

The blockchain is a rapidly growing technology around the globe. It represents an exciting new technological resource that has a huge potential in international development. Let it be disaster management, national security, economic growth, digital currency, supply chain and many other areas. There are new applications of blockchain being adapted by various organizations every day. One of the researchers (Kshetri, 2017) asked the question whether blockchain will aid in getting rid of the world's poverty. Another researcher coined that various disputes can be solved with the help of blockchain as it will reduce the government corruption and unnecessary bureaucracy (Murray, 2015).

Various national and international organizations are looking forward to incorporating blockchain technology in their disaster management policies and finding ways in how blockchain can provide efficient national security and reduce the amount of illegal immigration. There are a lot of aspects related to blockchain which has to be understood and a lot of implementation in various areas to be done. Researchers and scientists are working in this field to optimize the use of blockchain and help reduce the crime rate in the world and provide better and faster services.

The implementation of smart contracts along with blockchain has the ability to change how the countries around the globe function and how they frame their policies. Various studies are taking place in this direction in order to provide better supply chain, healthcare, national security, third-party risk management etc. Blockchain can save time, money, assets, and more importantly, lives.

5.3 Challenges of implementation

It is often assumed that that if Blockchain technology has significant benefits, then it will be adapted inevitably. However, there are many challenges to the adaption of blockchain. The blockchain technology is relatively new, it still need a lot of research in order to implement the technology to the above mentioned models and use cases. If proof of work is used as the consensus, then there would be a lot of energy consumption (electricity) and more powerful computers would have to be installed. The overall cost of implementation would be really high in order to regulate the models throughout the United States. On, the other hand the number of people working in this field are also less. There are very few people at this point in time, who know how to work on and implement blockchain technology. Which leads to a vague path in order to adapt the technology. The way to the adaptation of this innovation isn't clear, particularly where a considerable lot of the advantages are huge just with expansive scale adaptation in view of network impacts. Government will have to put a lot of efforts and resources in order to implement this technology and change the whole system.

REFERENCES

1. An Emerging Threat of Bioterrorism - Volume 5, Number 4-August 1999 - Emerging Infectious Disease Journal - CDC. Center for Disease Control, Aug. 1999. Web. 06 Apr. 2014. 3f16-4f29-b3ac-0607f1ecefa7

2. A thorough overview and chronology of key developments on WMD, as well as a listing of educational resources, is available from the Center for Nonproliferation Studies, part of the Monterey Institute for International Studies. http://cnsdl.miis.edu/cnserd/Affairs

3. Acting Commissioner Kevin K. McAleenan, 2017. U.S Customs and Border Protection; Honor First: U.S. Border Patrol's 93 years of services

   https://www.cbp.gov/newsroom/blogs/honor-first-us-border-patrol-s-93-years-service

4. Alden,(2012) "Immigration and Border Control," Cato Journal, 32(1):107–124.Bach, (2005) "Transforming Border Security: Prevention First," Homeland SecurityAffairs, 1(1):1–14.

5. Alexis, (2017). 10 Things A General Counsel Needs to Know About Blockchain.

6. Antonopoulos (2013), Mastering Bitcoin: Chapter 7. The Blokchain. Bach "Transforming Border Security: Prevention First," Homeland Security behind-bitcoin-is-shaking-up-much-more-than-money/

7. Assessing the U.S. Climate in March 2018 (National Centers of Environmental Information)
   https://www.ncei.noaa.gov/news/national-climate-201803

8. Bennett, 2016; Prevent and avoid Identity theft (https://www.consumerprotect.com/how-to-prevent-avoid-identity-theft/)

9. Blockgeeks; https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

10. BNET Business Directory
http://dictionary.bnet.com/definition/Disaster+Management.html

11. Business Insider: http://www.businessinsider.com/ibmceo-ginni-rometty-blockchain-transactions-internet-communications-2017-6

12. Carnegie Endowment for International peace; Nuclear policy http://www.carnegieendowment.org/npp/

13. Castro, Miguel, Liskov, Barbara, et al. "Practical Byzantine fault tolerance". OSDI ch07.html#merkle_trees. Changes in Immigration from 1986 to the Present and Their Implications for American

14. Correia et al., "Byzantine Consensus in Asynchronous Message-Passing Systems: A Survey.," International Journal of Critical Computer-Based Systems 2, no. 2 (2011)

15. Cutter (2005). Pragmatism and Relevance: a Response to Wolf R. Dombrowski. In E.L. Quarantelli & R.W

16. Data and analysis of trends and developments in military expenditures and arms production worldwide can be found at the website of the Stockholm International Peace Research Institute: http://www.sipri.org/contents/milap/

17. Data Breach: https://www.trendmicro.com/vinfo/us/security/definition/data-breach

18. Disaster Management within the Framework of a Changing Disaster Landscape. https://www.researchgate.net/publication/323189405_Disaster_Management_within_the_Framework_of_a_Changing_Disaster_Landscape [accessed Apr 05 2018].

19. Drabek, & Hoetmer (1991). Introduction. In T.E. Drabek & G.J. Hoetmer (Eds.), Emergency management:ENVT 6132 Climate Change Vulnerability and Capacity

20. Extensive resources and a chronology of the nuclear age are available at the website of the Nuclear Age Peace Foundation, http://www.nuclearfiles.org

21. Facts + Statistics: Identity theft and cybercrime: Insurance Information Institute https://www.iii.org/article/identity-theft-insurance

22. Federal Trade Commission; https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security

23. Geek4geek, https://steemkr.com/blockchain/@geek4geek/do-you-know-there-are-different-types-of-blockchain

24. Hans De Smet (2017) Disaster Management within the Framework of a Changing Disaster Landscape

25. Hornung, 2002, METHOD FOR IDENTITY THEFT PROTECTION

26. Identity theft: White and Lifelock; https://www.lifelock.com/education/dumpster-diving/

27. Identity Theft: The Crime of the New Millennium Sean B. Hoar USA Bulletin (March 2001)

28. Insurance Information Institute, 2010 Identity theft on the rise during holiday season; whether shopping online or at the mall, be vigilant

29. International Federation of Red Cross and Red Crescent Societies http://www.ifrc.org/en/what-we-do/disaster-management/

30. Irshad and Soomro , IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.1, January 2018 Identity theft and social media

31. Javelin: Identity fraud hits record high with 15.4 million U.S. victim in 2016 https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

32. Johnson, 2018. Blockchain Technology Implications for Development

33. Jones, Michael and Els De Graauwe (2013) "Looking Back to See Ahead: Unanticipated

34. Kaplan (1997). The Words of Risk Analysis. Risk Analysis, 17, 407-417

35. Katz, 2018 Congress, FBI Already Investigating Potential Abuse of Federal Funds in Puerto Rico's Disaster Response https://www.govexec.com/management/2017/10/congress-fbi-already-investigating-federal-spending-fraud-puerto-ricos-disaster-response/141876/

36. Keane, Odysseas Papadimitriou: Identity Theft: What It Is, How It Happens & the Best Protection https://wallethub.com/edu/identity-theft/17120/

37. Kikitamara, Digital Identity Management on Blockchain for Open Model Energy System

38. Knight, 2017 The Technology Behind Bitcoin Is Shaking Up Much More Than Money Retrieved from MIT Technology
Review: https://www.technologyreview.com/s/604148/thetechnology

39. Kshetri, 2017 Will blockchain emerge as a tool to break poverty chain in Global South?

40. Laura Reed *S*ecurity Studies Program, MIT, Cambridge, MA, USA Article on weapon of mass destruction (https://www.hampshire.edu/pawss/weapons-of-mass-destruction)

41. Lexology.com: https://www.lexology.com/library/detail.aspx?g=a2504096

42. Majumdar. 2017 Article on weapon of mass destruction

43. Media, Inc, 2013. url: http://chimera.labs.oreilly.com/books/1234000001802/

44. Merriam-Webster, Incorporated, "Definition of identity theft," 2017. [Online]. Available: https://www.merriam-webster.com/dictionary/identity%20theft. [Accessed 3 May 2017].

45. Milyo & Cordis, 2013, Don't Blame the Weather: Federal Natural Disaster Aid and Public Corruption

46. Mohan, 2017: IBM Disaster Management Solution – Part 1and 2: Cloud, IoT, Blockchain

47. Murray, 2015 World's poor: " We want Capitalism" the freeman Perry (Eds.), What is a disaster? New Answers to Old Questions. (pp. 104-106). Philadelphia: Xlibris Corporation.

48. Nakamoto, Bitcoin: A peer to peer electronic cash system

49. National Science Foundation. http://www.atomicarchive.com/Glossary/Glossary1.shtml

50. Newman and McNally, Identity Theft Literature Review, final report to the National Institute of Justice, July 2005, NCJ 210459, referred to throughout this publication as "the full report." Access the report online at http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=210459.

51. Perry, (1989). Taxonomy, classification and theories of disaster phenomena. In G.A. Kreps (Ed.), Social Peter Keane, dean emeritus and professor at the Golden Gate University College of Law.

52. Politics Today," Annual Review of Political Science, 16:209–230.

53. Principles and practice for local government. (pp. xvii-xxxiv). Washington, DC: International City

54. Pulwarty Notes, 2007-2008- UWI Cave Hill, CERMES

55. Quarantelli, (1985). What is a Disaster? The Need for Clarification in Definition and Conceptualization

56. Rapier, (2017, June 21). From Yelp reviews to mango shipments: IBM's CEO on how Blockchain research. In B.J. Snowder (Ed.), Disasters and Mental Health: Selected Contemporary Perspectives.

57. Rockville: National Institute of Mental Health-Center for Mental Health Studies of Emergencies.99 (1999), pp. 173–186.

58. Rohr, 2017: SAP Article Blockchain for Disaster Relief: Creating Trust Where It Matters Most

59. Sharrieff, 2018 https://sciencing.com/impact-natural-disasters-5502440.html

60. Signoli, "Reflections On Crisis Burials Related To Past Plague Epidemics." Clinical Microbiology & Infection 18.3 (2012): 218-223. Academic Search Premier. Web. 5 Apr. 2014.

61. Spamlaws.com, "The History of Identity Theft," 2017. [Online]. Available: http://www.spamlaws.com/id-theft-history.html.

62. Strengthening the Global Partnership, through the Center for Strategic and International Studies. www.sgpproject.org

63. Structure and disaster (pp. 351-359). Newark, DE: University of Delaware Press.

64. Suk, "Dual-Use Research And Technological Diffusion: Reconsidering The Bioterrorism Threat Spectrum." Plos Pathogens 7.1 (2011): 1-3. Academic Search Premier. Web. 3 Apr. 2014.

65. Swanson, “Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems” (Working paper, April 6, 2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers.pdf.

66. Tan, "Surveillance For Anthrax Cases Associated With Contaminated Letters, New Jersey, Delaware, And Pennsylvania, 2001." Emerging Infectious Diseases 8.10 (2002): 1073. Academic Search Premier. Web. 3 Apr. 2014.

67. The Arms Control Association offers excellent resources on a wide variety of issues pertaining to WMD, including an overview of key arms control agreements and analyses of timely issues. http://armscontrol.org

68. The Carnegie Endowment for International Peace provides a comprehensive website that includes an assessment of weapons, updates on proliferation concerns, and useful links

69. The Nuclear Threat Initiative offers a comprehensive overview and primer on WMD, including analyses, news updates, and country profiles. http://www.nti.org/f_wmd411/f1a.html

70. Vasin, “Blackcoin’s proof-of-stake protocol v2. 2014” URL:http://blackcoin.co/blackcoinpos-protocol-v2-whitepaper.pdf (2015).

71. Velasco, January 2016. [Online]. Available: http://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft

72. WHO: Disasters and Emergencies (http://apps.who.int/disasters/repo/7656.pdf)

73. Zheng, “Blockchain Challenges and Opportunities: A Survey” (2016)