JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 03 Issue 01
2022

Research Article

Forensics to Government Agencies Data using Hyper Ledger Fabric (HLF)

Zunair Hussain[1], Muhammad Imran[2*] and Ammbar Nosheen[1]

[1]School of Computing, University Utara Malaysia, Malaysia
[2]Department of Computer Science, Bahauddin Zakariya University, Multan, 60000, Pakistan
*Corresponding Author: Muhammad Imran, Email: m.imran@bzu.edu.pk

Received: October 26, 2021 **Accepted:** December 30, 2021 **Published:** March 15, 2022

Abstract: Security issues are increasing day by day all over the world. Cyber issues are one of the major issues that cause cyber-attacks involving Malware, Phishing, and Ransomware attack. Pakistan is also one of the major countries that are facing cybercrime issues. The most important firms are government agencies like NADRA, Law Firm, and Police Firm. Pakistan has still not made a refined structure to ensure its security from advanced risks. By, and by it has transformed into a national security hazard for Pakistan because the individual data of the government is not secured. Multiple attacks on the NADRA server have occurred in the past. The reason is the centralization server, and security flaws. With the coming of Technology in the 21st century, and security worries that happens due to cybercrimes. Individuals are currently pushing toward new advances, the main thing that comes in the mind to keep away from security hazards, is to circulate the information among various individuals, so the idea of decentralization comes in. A technology that recently has gathered a lot of attention is Blockchain technology. Its decentralized nature gives secure, secret, and basic intends to keep up the records without alteration. Blockchain provides immutability, Integrity, helps enhanced security, distributed ledger, and also provides consensuses. So for government organizations like NADRA data is the most important thing, if this data is compromised due to security flaws then it's happened a national security hazard that causes leakages of the nation's personal information. So this thesis purpose how to secure data using Blockchain technology a private Blockchain technology. An architectural view is presented with the help of use cases for government organizations NADRA, Police Firm, and Law Firm using HLF Blockchain technology. This thesis also presents the design, and architecture of how organizations work, and interact with one another. Using this design, and architecture we will be able to provide forensic to government organization data which makes it more secure from cyber threats.

Keywords: Cyber threads, Blockchain, Private Blockchain, Government cybercrimes

1. Introduction

Advanced security peril is growing well ordered, computerized security chance in Pakistan is a rising issue, Because of opposite computerized security parameterized. Computerized Security threats have been spreading into the associations of banking, preparing similarly as, military, and government parts like NADRA, Police Firms, and LAW Firms. Nevertheless, Pakistan falls behind in confirming its specific parameters. The critical portions of Pakistan are going up against advanced illegal access issues. Pakistan has still not made a refined structure to ensure its security from advanced risks. By, and by it has transformed into a national security hazard for Pakistan because the individual data of government or individual isn't confirmed. For open, and private security particular laws have quite recently been passed anyway they are

not preposterously incredible. They are not penetrated in Pakistan. This all occurs in perspective on the issue that data is supervised in a brought-together domain (SadiaRasool 2015).

Due to the colossal market limit of electronic identity stages, which concurs with the whole state masses, governments are partaking in making electronic identity structures, and attracting a base extent of customers, and pro systems. Possible challenges in the advancement of such systems are related to affirmation concerns, nonattendance of intergovernmental coordination, nonappearance of private-open section joint effort, and strains, for instance, the tradeoff between convenience, and security. Among those issues, security expects a fundamental occupation by attracting the advancement of trusted in electronic affiliation basic structures. Security is a multidimensional property of structures, data, and information. When recommended an IT structure in a business setting, information security is commonly sorted out as the distinctive leveled target of helping operational risks by protecting information from dangers to security, legitimacy, openness, and commitment. In any case, the present unavoidability of robotized movements in both work practices, and occupants' private life, extends the dimension of danger to security, and other human rights. Undesired electronic partition trades, data breaks of human associations, and cash-related information, the insidiousness of pivotal establishments, and unapproved access to electronic hurling check structures are a couple of occasions of veritable encroachment of rights, for instance, ownership, security, flourishing, and opportunity. Since electronic identity establishments fill in as a way to a huge degree of affiliations, their vulnerabilities can significantly affect affiliations, and society. Believe it or not, systems joining, and interoperability of affiliations attract the causing of security scenes well past the points of confinement of a singular relationship with potential ramifications for the execution of an entire ordinary structure. If we think about online FIR affiliation, and Lawsuit against an individual is so far recorded in a centralized database which is appeared to be securities shot or pushed strike (Axelsson, Söderström, and Melin 2016).

With the coming of Technology in the 21st century, and security worries previously. Individuals are currently pushing toward new advances, the main thing that comes in the psyche to keep away from security hazards is to circulate the information among various individuals, so the idea of decentralization comes in. So the first question that comes at the top of the priority list is what is decentralization? Decentralization is a trademark illustrative of intensity, control, access, or possession, as they are spread over different on-screen characters, focuses, or hubs involving a system. It is reflected, and shown in different designs, assemblages, and systems. As we proceed with our walk forward into the 21st century, one thing has turned out to be evident: advance is constant. People, substances, and whole businesses not fit for advancement are immediately usurped, and supplanted by those that are changing the essence of numerous enterprises.

Not having one single purpose of control will constantly display a dilemma. From one viewpoint, all individuals ought to be permitted to be in charge of their riches. They ought to reserve the privilege to work without the interruption of governments or concentrated specialists. To put it plainly, they merit the capacity to keep up their protection. Then again, well, it's additionally unconditional power for culprits to finance psychological warfare, do cybercrime, launder cash, and avoid charges. Decentralized trades take into account every one of these things to occur. They are without reconnaissance, and restriction safe with no capacity for any single substance or individual to take control. So the technology that one should pay attention to is Blockchain technology. The Blockchain is for the most part known as the innovation hidden the virtual cryptographic money bitcoin, however, this postulation analyzes to what else it tends to be used to. Since practically the majority of the information in the present Blockchains are bitcoins, this postulation will quickly dissect what precisely bitcoin is, and why it is equipped for filling in as elective cash. Indeed, even the first thing to stress is that the innovation isn't confined to this utilization as it were. Truth be told, bitcoin has been remarkably condemned, and is professed to be a somewhat constrained use of this innovation. So first we have to comprehend what is Blockchain?

1.1 Back Ground

Blockchain is a conveyed record innovation that goes about as a mutual information base, keeping the majority of its duplicates synchronized, and confirmed. The Blockchain development is still in its beginning stage, however, among its qualities is the possibility to dispose of the requirement for outsiders to go about as a dimension of trust in return of information - alluded to as exchanges. This is one of the

underlying foundations of the numerous signs that the innovation could affect plans of action crosswise over businesses generously(Sepp n.d.).

These days, for all intents, and purposes each industry is trying different things with joining Blockchain into its workflows ranging from agribusiness, style, coordination, and with the majority of the world's best ten organizations presently investigating its potential. Blockchain (a computerized record) work as a link list, including Block, associated and verified utilizing cryptography where each Block contains a cryptographic hash of the earlier block in the chain, a period stamp, and the exchange information which powers these blocks to keep up uprightness of existing information(Halpin, and Piekarska 2017). The decentralized nature of this chain gives secure, secret, and basic intends to keep up the records without alteration. Blockchain provides immutability, Integrity, helps enhanced security, distributed ledger, and also provides consensuses. Blockchain has two types:

- Public Blockchain is also known as permissionless Blockchain.
- Private Blockchain is also known as permissioned Blockchain.

1.1.1 Public Blockchain

Public Blockchain in which anybody can join the Blockchain organize, implying that they can peruse, compose, or take part with a public Blockchain. Public Blockchains are decentralized, nobody has command over the system, and they are secure in that the information can't be changed once approved on the Blockchain. Such a system relies on the number of members for its prosperity and henceforth energizes increasingly more public investment through a boost instrument(Khatwani 2018).

1.1.2 Private Blockchain

When we talk about private Blockchain or when we hear individuals discussing private Blockchain arrangements, they will in general be discussing things on the private, and shut end of the range. We need to control who can compose information to this Blockchain, and we need to control who can peruse information from this Blockchain(Khatwani 2018). Furthermore, to do that, the initial step is character. We have to realize who is a piece of the Blockchain organization. On the off chance that we don't have the foggiest idea who a client is, it winds up troublesome, if certainly feasible, to characterize administers about what information they can focus on the record, and what information they can devour from the record.

So we will utilize Private Blockchain for our structure. HLF is a Blockchain that assists us in such a manner. So what is hyper ledger fabric? As communicated in their site, "Hyper ledger is an open-source communitarian effort made to push cross-industry Blockchain progresses. It is overall participation, encouraged by The Linux Foundation, consolidating pioneers in the record, banking, The internet of Things, supply chains, collecting, and Technology. (Piekarska 2019)"

The fabric was normal for making courses of action with a disconnected plan. Hyper ledger empowers the fragments to be plug-n-play. It is a private, and permissioned Blockchain structure that suggests not in any manner like, in Permissionless (or open framework) systems that empower darken characters to share in the framework, the people select through Membership Service Provider (MSP).

1.1.3 Hyper ledger Fabric Model

Following are the key features of hyper ledger Fabric that fulfill its assurance of versatile undertaking Blockchain.

1.1.3.1 Assets

Enable the exchanging of monetary impetus over the framework.

1.1.3.2 Chain code

Partitioned from trade mentioning, compelling the required components of trust, and check transversely over-center point types, and streamlining framework versatility, and execution

1.1.3.3 Ledger Features

Encodes the entire trade history for each channel.

1.1.3.4 Channels

Enable multi-level trades with high degrees of insurance, and mystery.

1.1.3.5 Security, and Membership Services

In Permissioned interest, individuals understand that all trades can be perceived, and pursued by endorsed controllers, and evaluators.

1.1.3.6 Consensus

Allow orchestrate starters to pick an understanding instrument that best addresses the associations that exist between individuals.

1.2 Problem Statement

One issue is that each individual in the nation is validated utilizing their Identities allocation number stuff that is also known as NID. What's more, every administration action is additionally done based on that number, which is remarkable for every individual doled out by the legislature. Since starting now all of the all-inclusive community data is staying in a united (Centralized DB) region. If some attack on the united machine (Centralized DB) occurs. All individual data is spilled, and criminals can do anything by utilizing this information.

The second issue is on the off chance that someone does any crime still in our nation Fir is done physically, and in some city or town Support online Fir. In any case, they likewise have to possess brought together database. Some programmer or aggressor or even criminal can pay for assault, and change Fir or Fir individual name.

The third issue is on judiciary frameworks that still do not keep up any computerized record. As indicated by Richter(Richter, Kuntze, and Rudolph 2010) impelled proof is viewed as agreeable in the official court on the off chance that it meets the following criteria, by strategies for authentic, complete, solid, and substantial. With the speedy extension in cybercrimes, the advanced proof is developing consistently more criticalness, since it is used to indicate substances or to convict work propel related with cybercrimes. In any case, because of centralization, every town or city has its record-keeping frameworks. It's still a Cause issue for the state.

So the serious issue or motivation behind this exploration is to conquer this issue, which is that there is no association between the Identities allocation System (NID) of the state, Fir System, and judiciary structures everywhere throughout the country. Every industry record is live in an alternate Database., and there is no connection between these separated databases. So publically available firms can also seek the person's information easily and are not able to alter the data by causing any cyber-attack.

On the other way, if some framework is built up that has some association between Identities distributions System, Fir System, and judiciary framework then their record still kept in brought together territory. For the situation or occasion that some developer or attacker strikes on everything confirmation should be changed or tempered. So forensic data is likewise a major issue in that situation.

1.3 Research Objective

The examination expects to accomplish the following targets:

1. To understand Blockchain technology, and determined how its works.
2. To analyze the loopholes of existing centralized systems.
3. To find a new technology to provide a secure network to existing centralization systems.
4. To analyze the way new technology provides forensic to data.
5. To find a way to securely interact between different organizations at the state level without security concerns.

1.4 Research Questions

Q1. What is Blockchain technology, and how does it work?
Q2. What are the loopholes in the centralized systems?
Q3. Which Blockchain technology to use to secure the existing centralization network?
Q4. How does Blockchain provide forensic to data?

Q5. How to interact with a different organization using Blockchain technology so that information is also accessible to the public or Organization without any security issues?

1.5 Research Methodology

The researcher gives an architecture overview to analyze their findings. So for this purpose research first find the problem by extensive literature review, find the root cause, and then provide a solution. The solution is centered around how Blockchain innovation is utilized to commit to the upper hand to government organizations, so research provides an architecture design with the help of Blockchain technology. More will be discussed in the Research Methodology section.

2. LITERATURE REVIEW

The first Chapter provides the introduction and research problem. This chapter discusses the literature study describing Blockchain technology, and grounding Blockchain technology to give solution to the state-of-the-art problem, so to start by answering the first question:
"What is Blockchain technology, and how its work?"

2.1 Blockchain

Blockchain is another innovation, in light of distributed databases, and hashing strategies, which is turned into the establishment of the stages for exchanging digital currencies and executing smart contracts(Pierro 2017). The boom of Blockchain technology started with the introduction of bitcoin as a digital currency(Kikitamara n.d.). Bitcoin is a digital currency, and the underlying technology is the Blockchain. Satoshi Nakamoto first introduced the bitcoin mechanism using Blockchain technology. In his, paper Satoshi describes how to send electronic cash from one party to another party securely, and without the involvement of any third party using a cryptographic algorithm, hashes, etc(Nakamoto 2008). The technology that is working behind this is the Blockchain.

Blockchain is similar to the database but of distributed nature means that it is distributed in a peer-to-peer network. Peer-to-peer work in a way that there is no central resource who serve all the participant, records are distributed between all the participants involved in the network(Crosby et al. 2016). Blockchain (a computerized record) works as a link list, included Block associated, and is verified utilizing cryptography where each Block contains a cryptographic hash of the earlier block in the chain, a period stamp, and the exchange information which powers these blocks to keep up uprightness of existing information. The decentralized nature of this chain gives secure, secret, and basic intends to keep up the records without alteration. Blockchain provides immutability, Integrity, helps enhanced security, distributed ledger, and also provides consensuses.

Blockchain is a distributed record innovation in which every exchange is carefully marked to guarantee its genuineness, and trustworthiness(Hassell n.d.). Blockchain is a collection of blocks that are added by connecting one block to another in a particular order, creating a chain known as Blockchain, the starter block of the Blockchain is the genesis block(Siddiqui 2018). Figure 2.1 will explain how blocks are attached.

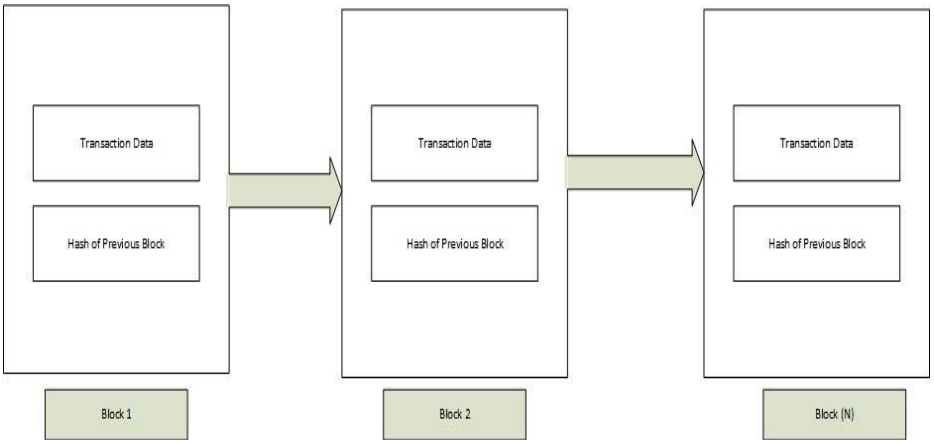


Figure 2.1: Linking Blocks

These blocks are cryptographically secure, and a hash of the previous block is passed to the new block, hence a chain of a block is made like a link list, but it is secured cryptographically. Hash is defined as it can take a variable amount of input but generating a fixed amount of output, and it is a one-way function and a small change in input result change in the hash. To understand Blockchain properly, some key attributes of a Blockchain are mentioned below(Siddiqui 2018).

- **Peer-to-peer Network:** The participants work in a group, with no central authority form where they get services. They work with each other without the involvement of any third party.
- **Distributed Network:** The ledger is distributed in a peer-to-peer network, all peer have complete information of the ledger which make tampering difficult.
- **Secured Cryptographically:** Cryptographic algorithms are used to provide security to the data which makes it difficult for the attacker to attack the ledger.

2.1.1 Consensus Algorithms

This is the most important part of the Blockchain. Without this Blockchain will be nothing as this part help in updating the ledger or adding block via consensus. No central authority is responsible for updating the ledger. Instead, the ledger is updated cryptographically via consensus algorithms. If some peer wants to add a new block, all remaining peers will validate the block, and the block is added only after the consensus has been reached among the peers or participants of the network that this is a valid block. This provides huge security to the network that if someone wants to attack this type of network, then they have to attack 51% of the nodes so that 51% of nodes behave maliciously to change the block which is practically impossible (Baliga 2017).

2.1.2 Immutable

The data in the Blockchain once enter it is almost impossible to change the data.

2.2 Working of Blockchain

1. A person starts the exchange by marking the exchange information with its private key. Figure 2.2 shown below tell us that each person has the public and private key. Through they made a digital signature cryptographically that is shown in figure 2.3 (Siddiqui 2018) (FORTNEY 2019).

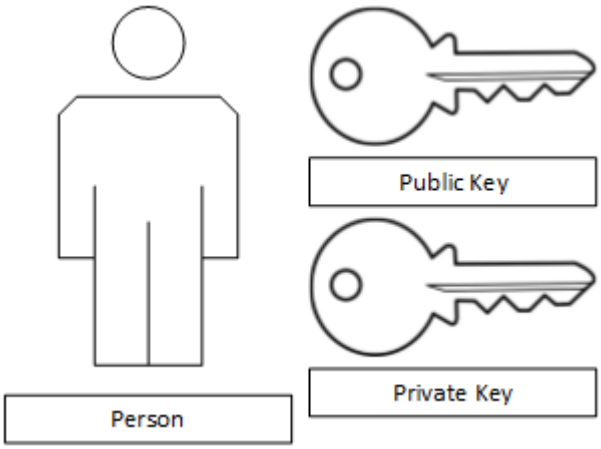


Figure 2.2: Public, and Private Key

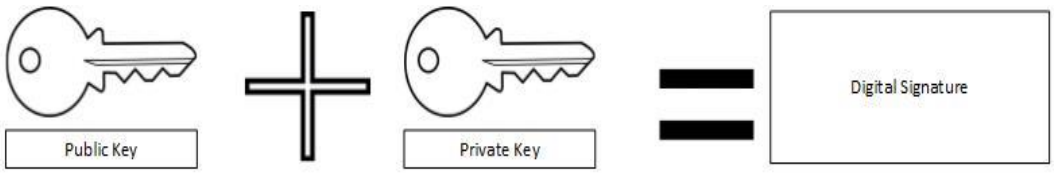


Figure 2.3: Digital Signature

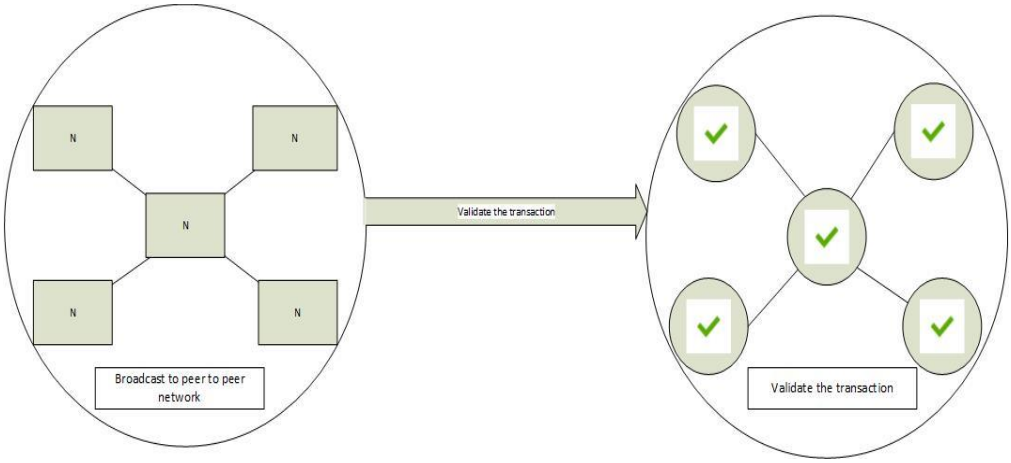


Figure 2.4: Consensus work

2. The exchange information is broadcast to thousands or millions of nodes attached to the network via some protocol that protocol is called the "Gossip Protocol". So that one of the peers should be able to create a block, once the other peers can validate the transaction shown in figure 2.4. This is done in light of preset criteria (Siddiqui 2018).
3. Once the validation is done, the block is added to the Blockchain. The block is now the part of the ledger Shown in figure 2.5, and the newly created block is containing the hash of the previous block and exchange information. Exchanges are then reconfirmed each time another block is attached (Siddiqui 2018).

The complete diagram is shown in the below figure 2.6

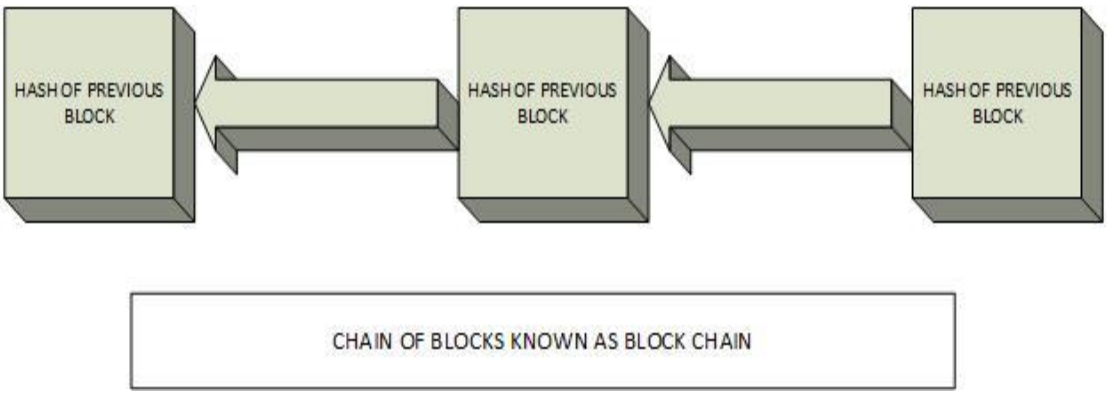


Figure 2.5: Hash of Blocks

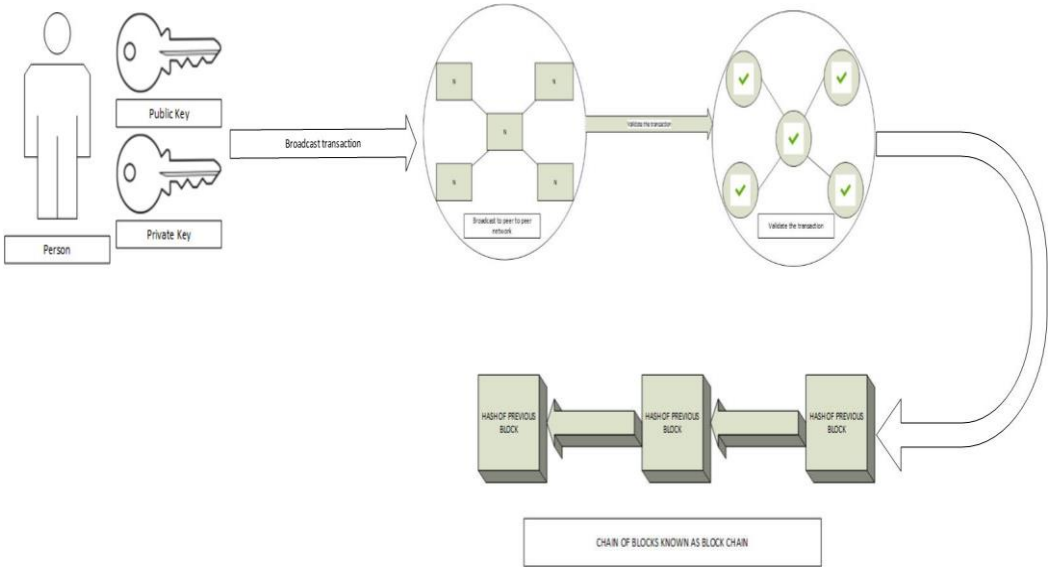


Figure 2.6: Complete diagram of block creation

So the purpose of our research is to provide a secure decentralized environment to currently centralized government agencies like NADRA, law firm agencies, and courts. So our second research question is: *"What are the loopholes in the centralized systems?"* This section gives an overview of centralization issues, and currently what strategies are adopted to overcome these issues or in simple words which techniques are currently used in the market to overcome issues, and what is the drawback of these techniques. By answering these questions, we understand the issues of the centralization technique currently used in NADRA, Law firms, and courts, and in the next section, the researcher will provide a technique to prevent centralization issues.

If we consider the major firm NADRA, we come to the point that Pakistan's first national registration office that registered people of the nation was built up by Zulfikar Ali Bhutto, The dad of the Benazir's Bhutto, in 1973, the explanation for that is to distinguish, and keep up the database about who is the native of Pakistan. The National Database and Registration Authority (NADRA) of Pakistan have turned into a focal player in various program regions like for financial balance opening, Visa Making, Law firms, Court, in the season of elections, and a lot more in all cases individuals are recognized utilizing their enlisted National Identity Number (NID).In expansion to its novel applications, it likewise demonstrates some of the limitations to effectively deploy the technology, the major limitation is the security concern of the data of the people or nation(Tariq Malik, former chairman, National Database, and Registration Authority 2014).

According to (Memon 2016) this paper report researcher describes that NADRA is a centralized database for identity management of the population of Pakistan citizens. The researcher further mentioned, and give a reason, and explanation of his point of view by saying that due to their centralization repository or database NADRA is the current organization that attackers want to attack, and want to steal confidential information of humans, and use it for wrong or illegal purposes.

If we consider E-Government types applications, there are various types of E-Government applications Government to Government, Government to Business, and Government to Public(Alshehri, and Drew 2010). If I mapped it with my research, they mapped in the following way First is Government to Government also known as (G to G) where different government organization applications interact with each other

for example (Law firms interact with NADRA, and Police Cases management Applications). The second type is Government to Business also known as (G to B) where different businesses interact with government applications for example mobile SIM companies application interact with NADRA application as they have to give SIM on the basic of NADRA record to a person etc., and the last type is Government to Public (G to P) where the public can see all information based on NADRA record about cases, about law, acts, and about SIM registration information, etc. But these government applications still is in the centralized repository so if these repositories get hacked all data will be loosed.

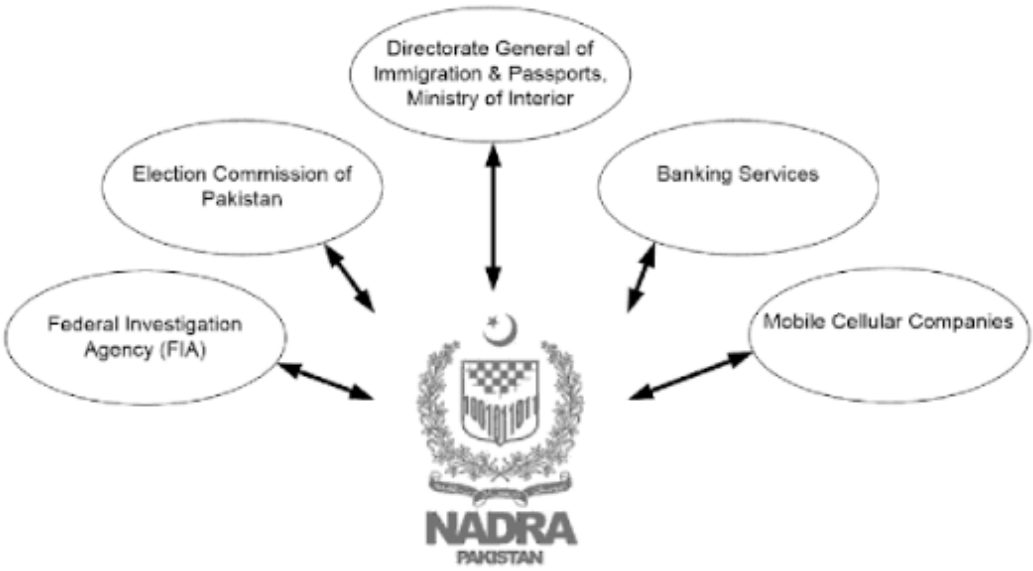


Figure 2.7 Source:(Memon 2016)

With the rapid increase in the usage of the the internet E-government services on the the internet are also prone to a thread(Zhao, and Zhao 2010). According to Report (Milkovich 2018), 95% of the attack/breaches is due to the government sector, retail sector, and technology sector because these sectors are less tireless in their assurance of their client records due to centralization. In 2018 "rewterz" referenced in his report that a huge information break has happened ever of. In the report it is said that "Punjab Information, and Technology Board (PITB)" is in charge of the production of the "NADRA" applications, he further said that "PITB" made use of cell phone that is defenseless against assault since this application interfaces with the API of NADRA that can demand subtleties of any Pakistani native by simply utilizing some various methods. He further referenced his perspective by saying that According to "WikiLeaks, and Julian Assange", these are the American, and British knowledge offices that are endeavoring to gain access to the NADRA database, and need to get hold of the distinguishing proof records of Pakistanis.

As per an Information Security master "Faiz Ahmed", the information was spilled because of unregulated or wrong e-administration applications, for example, the application that are made to sold online tickets of cricket matches dependent on the record that are in the database of NADRA in Pakistan. Individuals give their CNIC, and get the ticket these can cause tremendous abuse of the application(Faiz Ahmad 2018). By the time the internet has been built up, a reality that the internet is progressively going toward centralization design that may unequivocally impede the privileges of end-clients, and jeopardize the protection, and privacy of data(De Filippi, and McCarthy 2012). If we see deeply that Cyber security has become a crucial issue for the legislature of Pakistan, security strategy creators in the present situation of getting serious Cyber dangers to the Critical Infrastructure of the nation. The Critical Infrastructure includes the following sectors, for example, health department, E-Government, military, NADRA, and election commission of Pakistan. These sectors contain sensitive, and critical information of nation as well as the population of the Pakistan. It is likewise said that Pakistan is one of the third nations that are consistently being screened by the outside people for exploitation of cyber issues that exist in Pakistan. Pakistan is continuously in the state of attack if we are talking about the Independence Day abuses of Pakistan's ministries websites or if we are talking about the compromise of the NADRA servers in 2012 by Turkish hackers, and

one big thing that consists of the crash of the database server of the NADRA website in 2013 by the Afghan Cyber Army (ACA). Pakistan is always facing cyber issues in its country(Iqbal 2018). This is just because of the reason that record is kept in the centralization repository or database if attackers misuse that database they can steal all the information of the Pakistani citizen. Various kinds of attack can be possible like a worm, DOS, Virus, exploitation of some black holes, attacks on firewalls, etc.

However in the meantime, if we consider Pakistani Law. There is still no law in Pakistan against those people who break the security rules, security firewalls due to centralization issues there struggle are just to take the important data that cause danger to the whole firm or institution or government sectors, etc. It is a kind of theft, and its starter needs significantly propelled evidence fusing try to enter in the database. Now it becomes a need for the time that Parliament takes its initiative, and should have to bring a new law just on Cyber security for the protection of national / Public, and private data(Tank 2018).

If I consider police firms I found, the vast majority of individuals are currently included in crimes so these individuals would have some criminal record, so they have some FIR bodies of evidence enrolled against them in at least one police headquarters of Punjab or another region. In any case, these cases are enrolled physically in a specific region. In Pakistan be that as it may, rather than what the name derives, the FIR truly banner the start of formal criminal systems which is filed in various registers, and structures at the police base camp with copies of the report flowed too many police, and lawful working environments(Malik 2018). Open diagrams, and reports of government duty, and change establishments exhibit that the police are a champion among the most by, and large feared, whimpered against, and least trusted in government associations in Pakistan, missing the mark on a sensible game plan of obligation, and tormented by pollution at the biggest sums. Zone level police are oftentimes under the control of historic officials, rich landowners, and other enticing people from society. There are different uncovered occurrences of police extrajudicial killings of criminal suspects, the torment of detainees to get affirmations, incitement, and extortion of individuals who hope to record criminal cases, especially against people from the security powers. This report archives genuine human rights infringement by the police in Pakistan. It subtleties the challenges that casualties of wrongdoing, and police misuse face in getting equity, including the refusal by police to enlist protests (known as First Information Reports or FIRs), their requests for fixes, and one-sided examinations. Poor people and other defenseless or minimized gatherings constantly face the best hindrances to acquiring equity in a framework that is fixed against them. It additionally inspects impediments, including money-related, and human asset imperatives, which police say sway their capacity to work appropriately, and takes a gander at instances of some great police rehearses that can fill in as potential models for what's to come. This report additionally recorded hierarchical weaknesses, deficient preparation, and assets, absence of essential assets, poor working conditions, and absence of coordination with other law requirement organizations as obstructions to straightforwardness, and responsibility inside the police power(Daraz 2016).

It is the need vital, that the police system should be fixed up, and displaced with a productive legal, and institutional setup. It is currently significant that police instrument ought to be sufficiently developed that straightforwardness, responsibility, proficiency, merit-based arrangements, mandatory legitimate instruction, proof-based policing ought to be empowered in Pakistan, and one noteworthy thing that it ought to be bound with data innovation, so data against a criminal is kept in an increasingly secure zone, and it ought to be safely disseminated among different association or law offices (Shabbir 2014). So the reason for my examination is to give a secure environment to police associations in Pakistan. At present there is no law for this, if a few uses online FIR instrument, that system isn't verified, and secure enough, and also the system is centralized, and working in a specific area that is also venerable to attack, and not sufficiently grown enough, that criminal information is kept in a protected territory, so there is a colossal need of component that is decentralized so that criminal information is safely kept up transparently. If I see in the report that is mentioned above the report says that hierarchical weaknesses, deficient preparation, and assets, absence of essential assets, poor working conditions, and absence of coordination with other law requirement organizations as obstructions to straightforwardness, and responsibility inside the police power(Shabbir 2014), so from the report I reach to the state that the goal is that, individuals of Pakistan likewise get equity in his nation's police, an officer also work in a fair environment that should be free of corruption, and under the control of historic officials, rich landowners, and other enticing people from

society., and also that it should be available, and accessible to other organization like Law firms, so that every activity happen in full justice, and secure way. So how we can accomplish it will be discus in while.

If I consider the Court Firm or Law Firms the first issue that I found is on judiciary frameworks that it still not keep up any computerized record. Or if in some area or city, keeps a computerized record. It is kept in a centralized database, the record is evidence against criminal activity or criminal Person. As indicated by Richter(Richter, Kuntze, and Rudolph 2010) in his paper impelled proof is viewed as agreeable in the official court on the off chance that it meets the following criteria, by strategies for authentic, complete, solid, and substantial. With the speedy extension in cybercrimes, the advanced proof is developing consistently more criticalness, since it is used to indicate substances or to convict work propel related with cybercrimes.

Browse(Brotsis et al. 2019) present a framework in which he explains how digital evidence is secured so that it can be presentable in the court law. The system utilizes a private database (private database is a Blockchain-based database that is permissioned Blockchain) for storing data that need protection, data is digital evidence, the evidence that is presentable in the court, so the author defined the evidence is stored/captured, along with a permission Blockchain with the goal that it permits giving security administrations like honesty, verification, and non-revocation, so the proof can be utilized in a courtroom.

In any case, because of centralization, and every town or city has its record-keeping frameworks or system there is no relationship exist between a different organization or even within the same organization. This is a real big problem that still Causes issues for the state. So we required a system where data against a criminal is kept in an increasingly secure zone, and it ought to be safely disseminated among different associations or law offices. If I consider the advantages of centralization as mentioned by the author(Sarah C. Michalak, Julio C. Facelli 1999) in his article that: United information development implies the centralization of Major information advancement decisions at one spot. Centralization is generally a pro association between those in all-around control of the affiliation, and the rest of the staff. The more firmly the control connected within, the more conspicuous the dimension of centralization. The upside of the centralization is that top heads remain aware of the operational similarly as fundamental issues, and concerns.

But still there exist a limitation in the current system, when we consider the limitation of the current system we come into the state that huge changes should be required in the architecture of currently implemented systems. The issues that we face in the current systems are cyber security threats like a DDOS attack, Viruses attack, Worms attack, ransomware attack, data theft, and loss of effective information. Since I am considering the major government agencies where all nation data are kept if the attack is successful on these types of systems then a huge information are loosed, and it causes the thread to country repetition as well, so we required systems in which resources are shared among various entities or it is not in control of a single entity or person. *"So what type of systems is required to protect this kind of system?"* The answer is the system that is decentralized in which information is distributed among various entities, and systems that use a mutual consensus mechanism to protect the information, the systems that consist of this kind of facility is the only well-known system the Blockchain. But Blockchain has many different types. *"So which type of Blockchain is required?"* The type of Blockchain is required depending on the requirement of the application. In public Blockchain, Ledger information is publically available in his explorer. If I consider a financial application like bitcoin, Ethereum, etc. this Blockchain has a shared public ledger in which information of transaction till start, from coin creation to coin transaction, and so on is reside, Every single affirmed exchange are incorporated into the Blockchain. This type of finical application required a public Blockchain so that the history of transactions is still shown in a protected way. But for applications like government agencies where data is shown in a protected way and shown only to the authorized person we required another type of block so the question comes to mind. *"What is the name of that Blockchain?"* The name of that Blockchain is private Blockchain.

3. Research Methodology

The researcher gives an architectural overview to analyze their findings by conducting an extensive literature review, identifies the problem that the Pakistan Government faces in terms of IT solutions, and finds the solution on the behalf of problem that how this problem could be solved by providing an architecture design. So for this purpose research first find the problem by extensive literature review, find the root cause, and then provide a solution. The solution is centered around how Blockchain innovation is

utilized to commit to the upper hand to government organizations. So I am going to provide discuss in Phases how I start my work.

3.1 Phase 1

I followed a systematic literature review-based approach by first finding the problem by conducting extensive research in different computer science databases. The problem revolves around e-government issues, Cyber security issues related to government databases which involve NADRA, Police Firms, and Law firms. The query strings that are used to search the paper is given below:
"(Cyber security issues to e-government), and (Cyber security issues to government databases), and (Security issues to NADRA), and (Security issues to Law Firms), and (Security issues, and issues that police faces in terms of IT), and (Cyber Security issues faced by the government of Pakistan)". The systematic review included the following databases that are mentioned in table 3.1 below

Table 13.1: Scholar Repositories

Sr.	IEEE
1	Springer
2	Google Scholar
3	Elsevier Science Direct
4	ACM Digital Library

Phase 1 has divided into two sections: In the first section, I find the papers using mentioned above queries in the mentioned above databases, analyze the issues, and find the problem statement.
In the second phase, I analyze the root cause of the problem. The major issue identified is the centralized access to a data source in simple terms centralization is the big issue. According to Report (Milkovich 2018), 95% of the attack/breaches is due to the government sector, retail sector, and technology sector because these sectors are less tireless in their assurance of their client records due to centralization. Many applications like financial, bank sectors, police firms, voting systems, and public sectors organizations used NADRA provided information of a person, As reported by (Faiz Ahmad 2018) that huge information is leaked when Online booking of a ticket for match is given based on NADRA records. Pakistan is continuously in the state of attack if we are talking about the Independence Day abuses of Pakistan's ministries websites or if we are talking about the compromise of the NADRA servers in 2012 by Turkish hackers, and one big thing that consists of the crash of the database server of the NADRA website in 2013 by the Afghan Cyber Army (ACA). Pakistan is always facing cyber issues in its country (Iqbal 2018). According to "WikiLeaks, and Julian Assange", these are the American, and British knowledge offices that are endeavoring to gain access to the NADRA database, and need to get hold of the distinguishing proof records of Pakistanis. Service availability is also a big limitation of centralized architecture. A high percentage of availability requires a complex architecture that is not cost effective, and required high cost.

3.2 Phase 2

In this phase, I search how to resolve the centralization issues by doing research in different databases that I already mentioned in Table#1. So this phase also consists of two questions first identify the solution: For this, I come into the state that distributed systems will help us in this regard so I start analyzing how distributed systems help resolve the centralization issues. So for this first, I identify what are the distributed systems. A distributed system is the network of autonomous computers systems that Communicate with one another in the way that the computers are independent of one, and another because they communicate using a protocol, and they don't physically share a memory and other resources. By further investigating the solution I come into the state of using Blockchain technology, so for this purpose, I included the research studies that held from the years 2008 to 2019. Satoshi Nakamoto first introduced the bitcoin mechanism using Blockchain technology. In his, paper Satoshi describes how to send electronic cash from one party

to another party securely, and without the involvement of any third party using a cryptographic algorithm, hashes, etc (Nakamoto 2008). So that is why I choose my study from the year 2008 to 2019.

The second phase is how solution help resolve the issues that I face in the centralized architecture so for this purpose An exploratory examination was coordinated to depict the Blockchain's history determined how its work, and how it helps us in resolving centralization issues. For this purpose, I study Blockchain, and its types, and determined that Blockchain has two types: Public, and Private. So I further investigate what is the purpose, and difference of both types, and how Blockchain provides a solution to us or in simple words understands the applications of Blockchain. So I determine public has its limitation the first is that it required transactions, and the second limitation is that information is available to a public ledger that public can also see every information so it contradicts our requirements so I search about private Blockchain so I come into state hyper ledger Fabric will help us in this regard, So I start seeing Blockchain-based application I saw now people are moving their application to Blockchain because it provides high security and availability. Blockchain uses smart contracts to write an application in Blockchain that is cryptographically secure. So the exploratory approach was found relevant for this study as it enables to conduct a research of technology implementation into government management software like NADRA, Police Firms, and Law Firms. Analyses of the most relevant, and valid source by examining the limitation as discus above

3.3 Phase 3

In this phase, I will provide the architecture design of how to use hyper ledger fabric technology to secure NADRA, Police Firms, and Law Firm's data, which means how this technology provides forensic data. So for this purpose, I will understand the technology of hyper ledger fabric, and provide our design that would be helpful for government firms in securing their data in Blockchain, and also provide interaction to different public sector organizations without any security concern this can be described in chapter 4 that is of purposed solution. The pictorial representation of each phase is given below in figure 3.1.

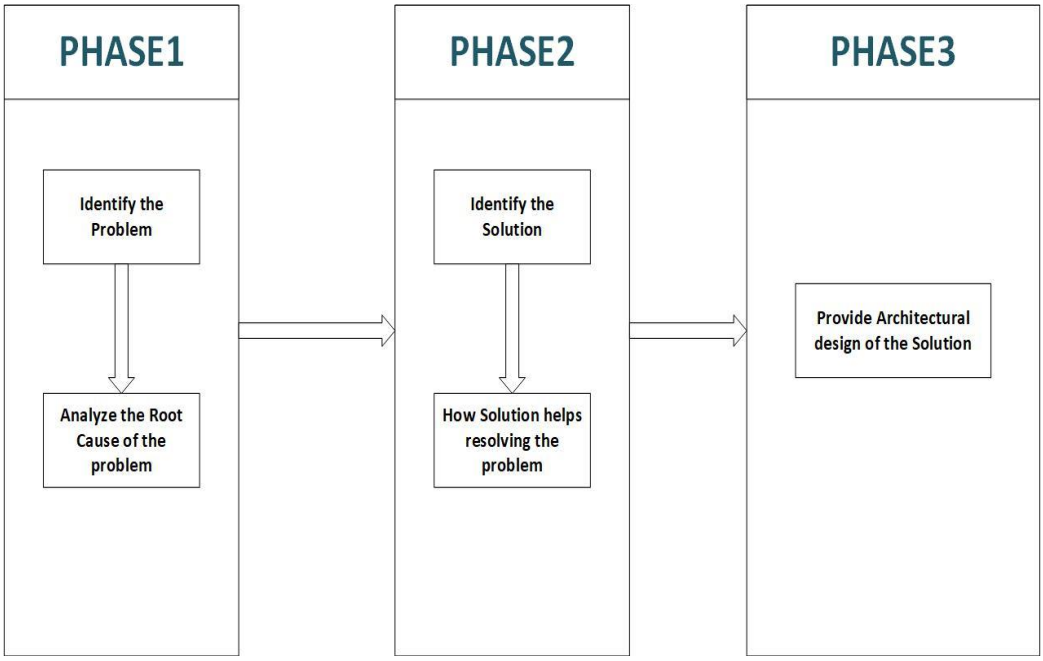


Figure 3.1: Phases of Methodology

So this study aims to see the limitation of government issues that they face. So research is conducted by analyzing the problem and providing a solution to solve this problem. The solution is Blockchain technology, so this thesis will provide the architecture of the design that is described in the next section.

4. Forensics to Government Agencies Data using Hyper Ledger Fabric (HLF)

HLF is an open-source Blockchain that has dispersed record that records every one of the exchanges that happen on the system. It is a permissioned Blockchain that gives high security, changelessness,

protection, and scalability. When we talk about permissioned Blockchain it means its established decentralized relation of the known participant in the network, rather than other Blockchain that provide the public network with no identity. It also supports smart contracts, the name of the smart contract is chain code where the actual business logic resides. It also provides the facility to design your network according to your choice.

The network consists of various participants which are divided into two parts:

1. Physical Participant
2. Logical Participant

4.1 Physical participant

Physical participants include peers, a Membership service provider which is abbreviated as MSP or CA which is known as a Certificate authority, and Orderer.

4.1.1 Peers

The peer is the most important part of hyper ledger fabric, a network is established according to a set of peer nodes, these peer nodes contain the ledger according to their channel, and organization. In its simple terms a Blockchain network is comprised of peer nodes, each of which can hold copies of ledgers, and copies of chain code. All the peers maintain their one ledger per channel. Peer is also of two types' general peer / endorsing peer, Anchor peer (Hyperledger 2019b).

4.1.1.1 General peer / endorsing peer

The peer can be endorsing peer the purpose of endorsing peer is to provide load balancing it also helps to Validate the incoming transaction, check the roles, and certificate of the requester to validate it is the accurate requestor or not. It is also able to execute the chain code but it is not able to update the ledger, endorser peer can approve or disapprove the transaction (Mamun 2018).

4.1.1.2 Anchor peer

Anchor peer is the most important part of the peer, anchor peer is responsible for updating the ledger anchor peer is configured during channel configuration. We can arrange channels among the peers, and exchanges among the peers of that channel are visible just to them. Anchor peer gets updates and communicates the updates to different peers in the organization. Anchor peers are discoverable. So any peer set apart as an Anchor peer can be found by the Orderer peer or some other peer (Mamun 2018).

4.1.1.3 Membership Service provider (MSP) or Certificate Authority (CA)

MSP work to figure out which Certificate Authority are substantial for the association by distinguishing which CAs are approved to issue legitimate personalities for their individuals. An MSP can recognize explicit jobs a client play inside the extent of the association like its function as an administrator or has the benefit to peruse or compose. Certificate authority in hyper ledger fabric work in a similar way that it gives digital identity to all participant involved in the network. The identity is represented by an X.509 digital certificate. (Hyperledger 2019a)

4.1.1.4 Orderer

Orderer is the most important communication channel in the hyper ledger fabric. It contains all organization anchor peer, and channel configuration it makes a block of the transaction proposal, and distribute that block to all participant for validation. Orderer plays a central role in the hyper ledger fabric (Mamun 2018).

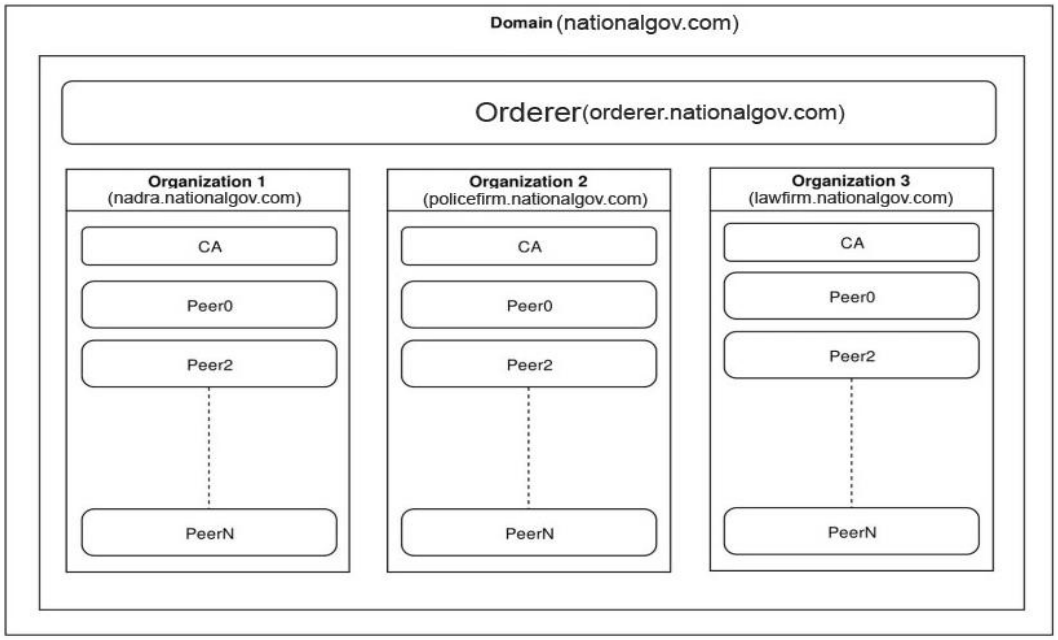
4.2 Logical Participant

The logical participants include organization, channels, and the last one, and the most important part is chain code which is also known as CC.

4.2.1 Organization

Organizations are the holders for the peers, and particular authentication experts (CA). Every organization has its very own CA, and a list of peers. As a rule, organizations are utilized for physical detachment

of the Blockchain arrange where every organization who uses your item can set up their physical machines, and join your system(Varun Raj 2018). In our case below mentioned is the diagram (diagram 4.1) that explains the working of the organization.



4.1: Organization

4.2.2 Channels

Channel is used to create logic a network that has a number of peers so that one ledger is maintained per channel between those peers.

4.2.3 Chain Code

Chain Code is similar to a smart contract in chain code we write our business logic the purpose for which software is going to be created, it is responsible for creating, updating, or invoking the transaction it must run on the peers, and creates transactions. It enables users to create transactions in the Hyperledger Fabric network's shared ledger. In our scenario, we are required to design a system for the government that provides data protection to nation data which has the feature that it must be secured, scalable, and also include known participants in the network so HLF provides all these facilities this is the main reason we choose HLF. The second reason to choose HLF is that if we consider Ethereum that also able to create a permission Blockchain is that Ethereum required mining of coin, and for each transaction since it's a business logic we need to spend a coin for which purpose we have to pay money for each transaction, for HLF this is not required (Varun Raj 2018).

4.3 Organizations Architecture

Below present the diagrams of our architecture, how this architecture work is explained with the help of use cases.

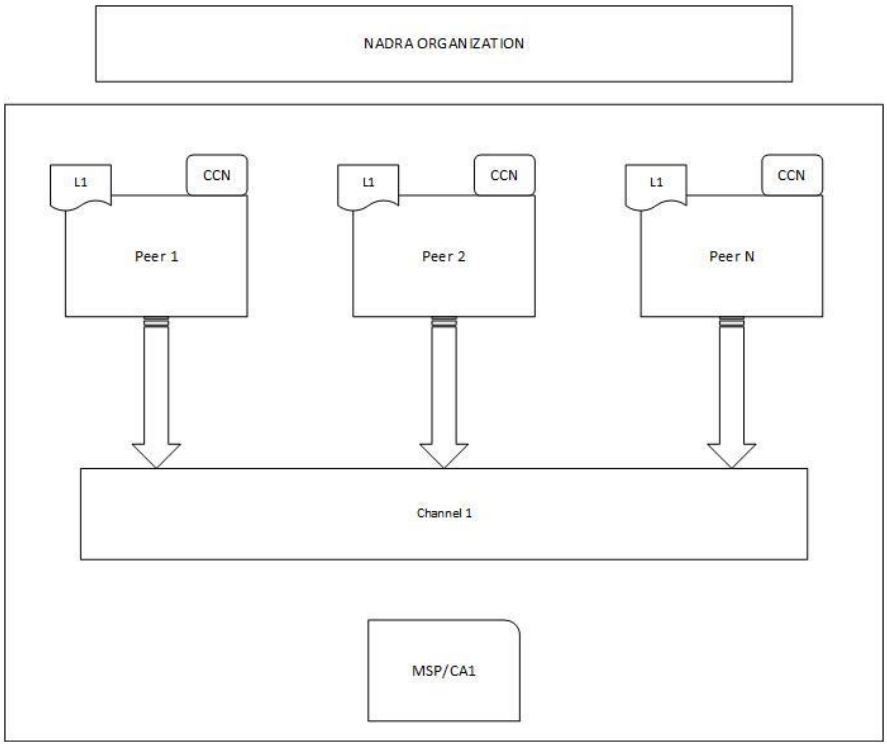


Figure 4.2: NADRA Organization Architecture

The diagram above (diagram 4.2) represents the NADRA Organization architecture, CA represents Certificate authority, L1 represents ledger for channel 1. CCN represents the chain Code for NADRA. CA gives a certificate to each participant of the organization, and there exist multiple peers that maintain the copy of a ledger. There exist an anchor peer that is responsible for querying, and updating the ledger. Installation of Multiple peers also helps us in load balancing. Chain code where the actual logic is written for creating a record, updating a record, and deleting a record. These functions will be able to update or create of a new records in the ledger. The ledger is updated with the help of consensus. There also exists a channel that shows one ledger is maintained per channel.

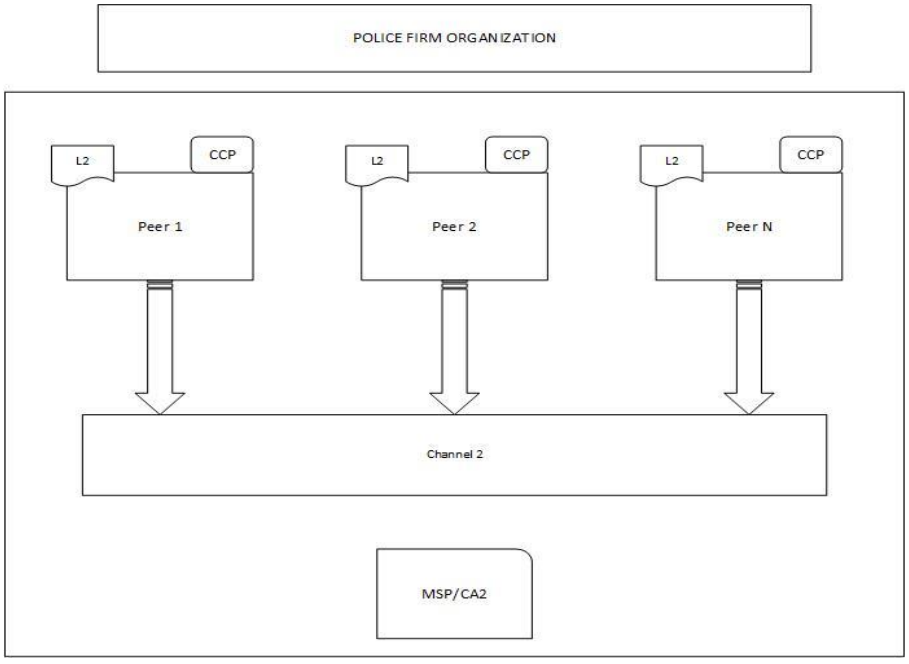


Figure 4.3: Police Firm Organization architecture

The diagram above (diagram 4.3) represents the Police Firm Organization architecture, CA represents Certificate authority, L2 represents ledger for channel 2. CCN represents the chain Code for Police Firm. CA gives a certificate to each participant of the organization, and there exist multiple peers that maintain the copy of a ledger.

There exist an anchor peer that is responsible for querying, and updating the ledger. Installation of Multiple peers also helps us in load balancing. Chain code where the actual logic is written for creating FIR, updating FIR, and deleting an FIR. These functions will be able to update or creating of a new record in the ledger. The ledger is updated with the help of consensus. There also exists a channel that shows one ledger is maintained per channel.

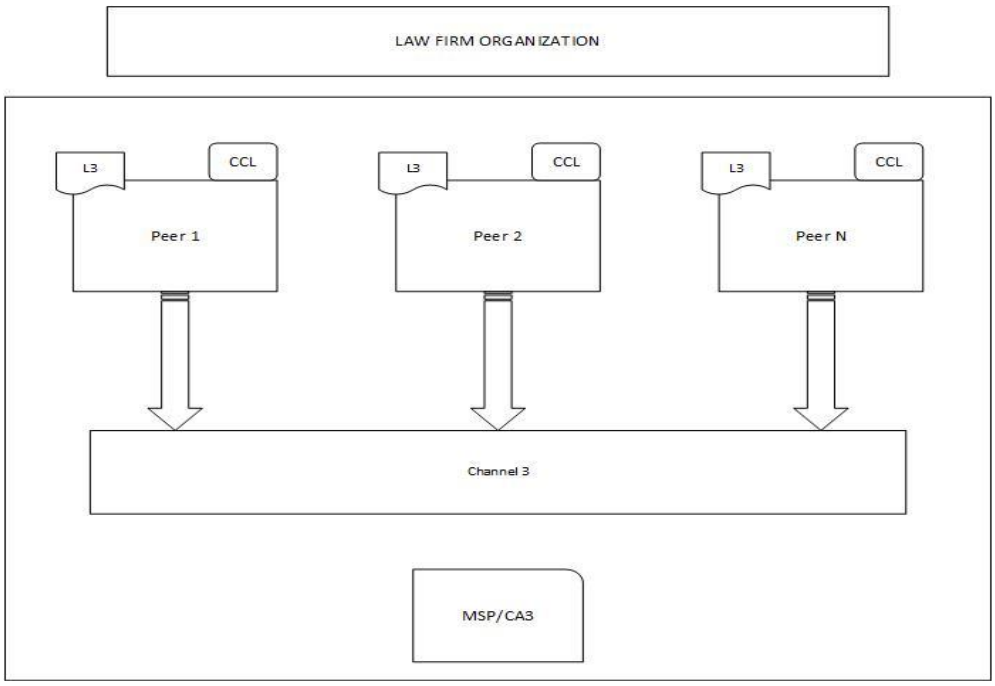


Figure 4.4: Law Firm Organization architecture

The diagram above (diagram 4.4) represents the Law Firm Organization architecture, CA represents Certificate authority, L3 represents ledger for channel 3. CCN represents the chain Code for Law Firm. CA gives a certificate to each participant of the organization, and there exist multiple peers that maintain the copy of a ledger. There exist an anchor peer that is responsible for querying, and updating the ledger. Installation of Multiple peers also helps us in load balancing. Chain code where the actual logic is written for creating FIR, updating FIR, and deleting an FIR. These functions will be able to update or create a new record in the ledger. The ledger is updated with the help of consensus. Note that Anchor peer is also installed based on per province.

4.3.1 Working on the architecture

A user of the application can interact with HLF using an API that is created by the developer. There exist a fabric client that contains API which interacts with the HLF for updating or querying or inserting a record in HLF. Application enrolls with CA of each organization. The user of the application interacts with the fabric client API which internally calls the Chain Code function to update the HLF ledger. Each participant of the network either peer, fabric client, or user must enroll themself in CA to access the network. CA give authority to read, write or update the ledger. Using fabric client, SDK (JAVA OR NODE JS) endpoints are created.

The question of who is responsible to read or write or search the data is handled on the client-side in this architecture. In the presented architecture currently, there is only one ordering server, we can attach more ordering servers for load balancing. The ordering server helps batch the transaction. A detailed diagram of the architecture is given below.

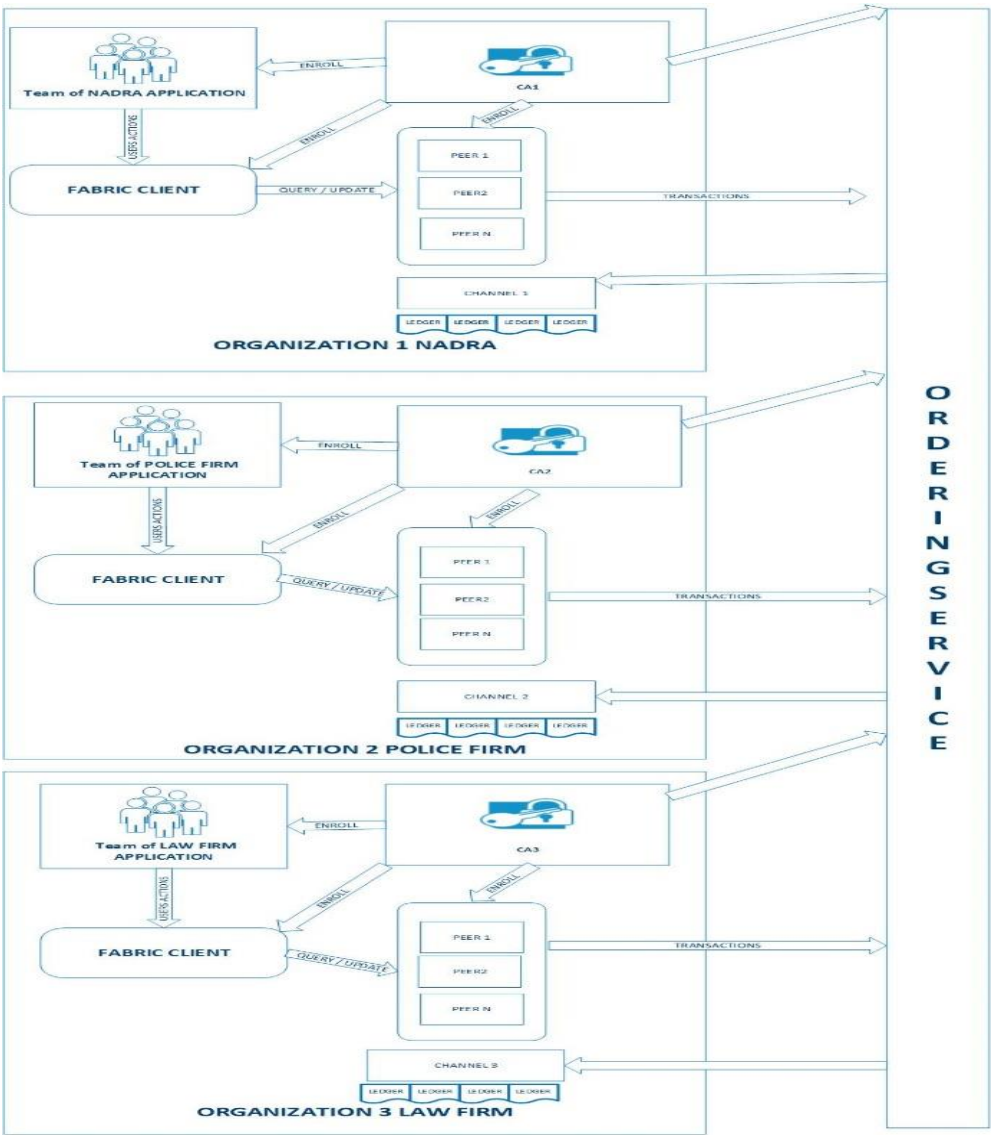


Figure 4.5: Detail Overall Architecture

4.3.2 Working of ordering server

The ordering server contains Channels, anchor peers of each organization. The user of the application via fabric client sends a proposal to the peer. Anchor Peer will validate its accuracy, and send a response to the application. Anchor peer sends this proposal to orderer peer. Orderer peers create a batch of that proposal and send this to all peers of the channel, all peers will validate the batch to achieve consensus, and determined it is according to rules defined by the network. Once consensus is achieved the block will be added to the ledger.

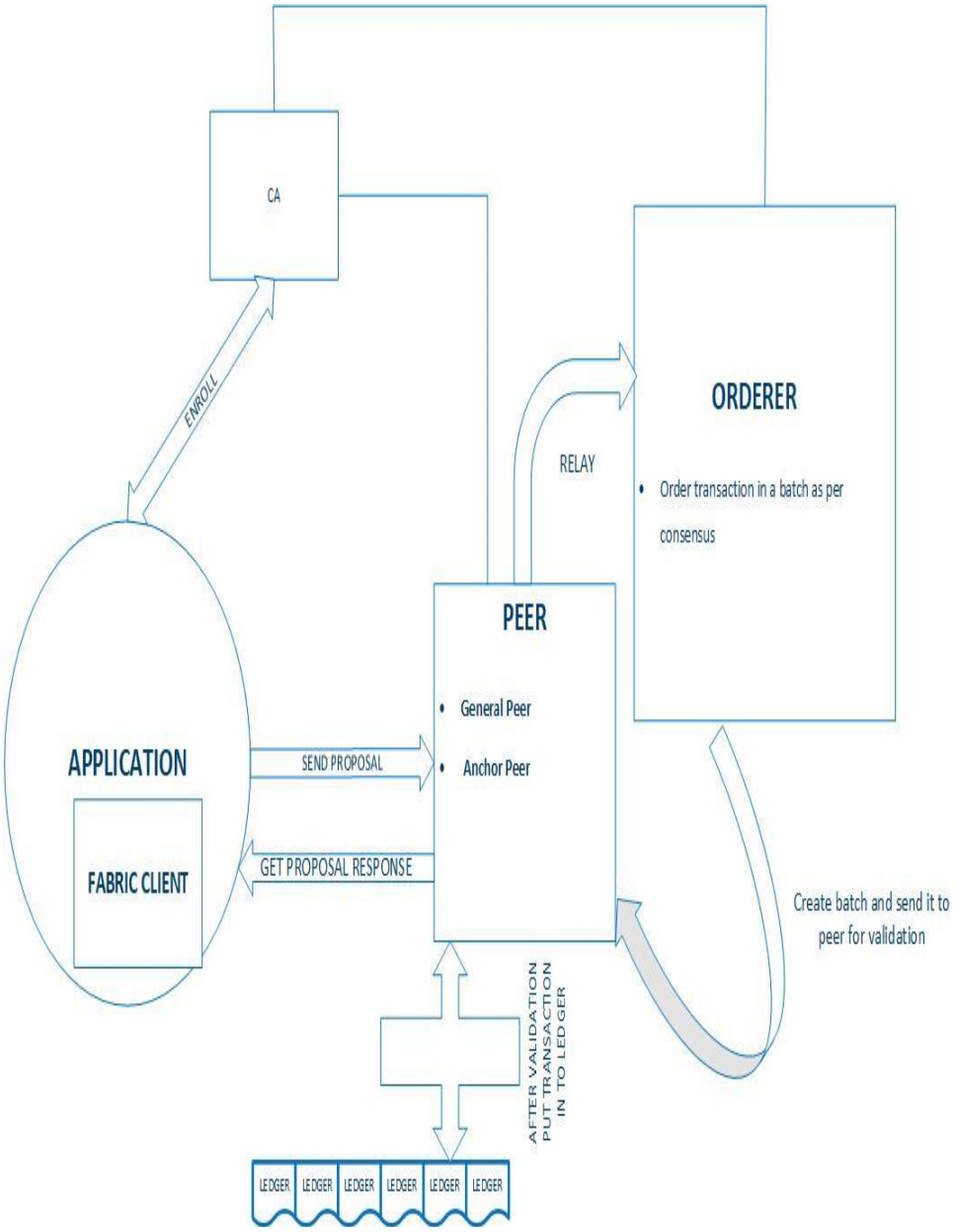


Figure 4.6: Ordering service working

4.3.3 Organization Interaction

Organization interaction is done on the client-side, using mentioned above architecture, endpoints are created for creation, deletion, updating, and searching the data. The user of the application uses that API to do their work. So if a public user wants to search some person's CNIC, the application provides an interface where the public use only enters the CNIC, and at the back end, it will call the search function using fabric client, and retrieve data from NADRA HLF, Police Firm HLF, and Law Firm HLF. All user read, write functionality is handled using the front end by seeing user rights and being being given access to that API. The Overall architecture of interaction is mentioned in the below figure 4.1.

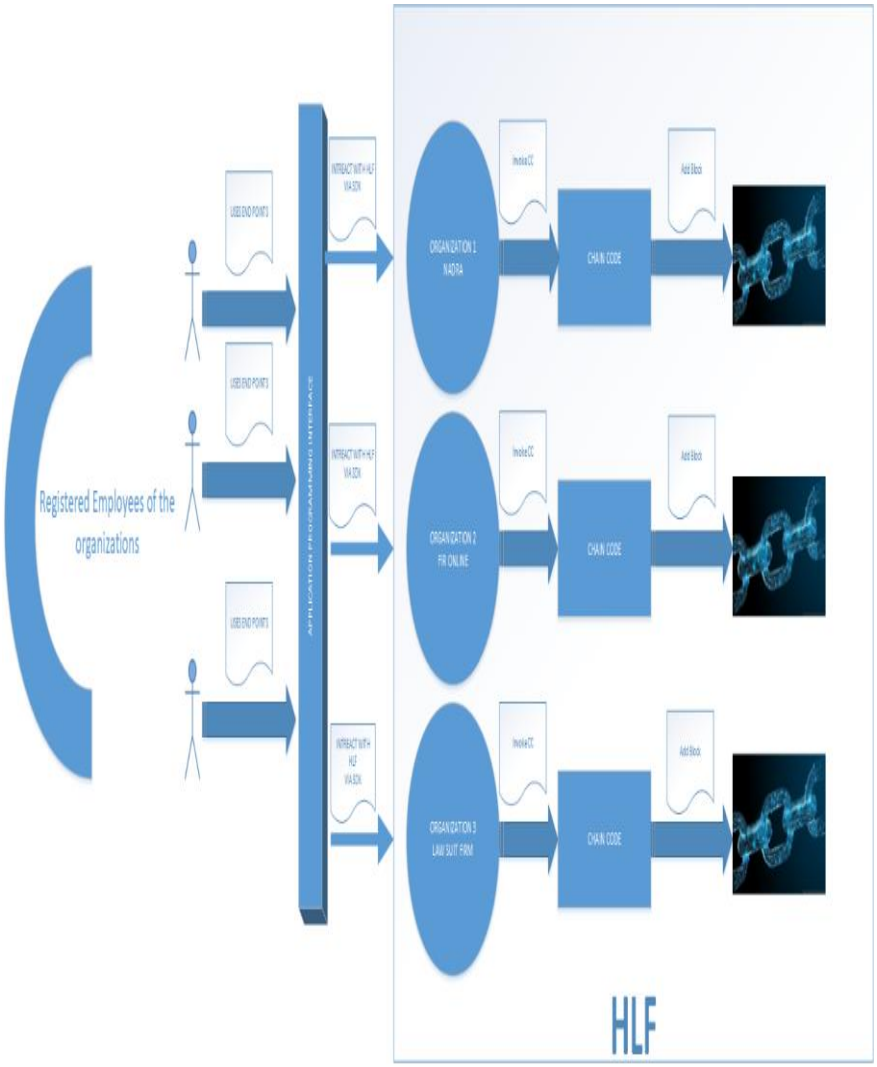


Figure 4.1: Overall proposed architecture

5. Conclusion

The study examined how Blockchain technology helps us provide forensic to government data from security threats, and issues, so for this purpose an architectural view is presented using HLF Blockchain, and map government organization NADRA, Police firm, and Law firm to architecture that is discus with help of use cases, and identified that using Blockchain technology we were able to achieve immutability, security, and also load balancing.

In past, Blockchain technology is mostly associated with cryptocurrencies but with the invention of HLF Blockchain technology, and smart contracts now it can be used with any application that required security and decentralization. Blockchain helps us reduce cyber-attacks because it's built upon a consensus model that all nodes need to agree that this transaction is valid than the true version of the ledger is maintained, and also if someone wants to attack the Blockchain they need 51% participation of nodes to behave incorrectly that in reality is not possible. Every Blockchain has different benefits and limitations. We select HLF because it is a private Blockchain. The main strength of Blockchain technology is that it is immutable.

This architecture is also helpful for the public if the public wants to search some person's CNIC, the application provides an interface where the public use only enters the CNIC, and at the back end, it will call search function using fabric client, and retrieve data from NADRA HLF, Police Firm HLF, and Law Firm HLF. All user read, write functionality is handled using the front end by seeing user rights and being given access to that API.

The architecture that is present in this thesis is also expandable in terms of that it helps government organizations in terms of not only security but also helpful for interacting with different provinces by just adding nodes for that province. Peers are also attached to help in load balancing. So Blockchain is a currently trending topic in the IT world, and it is not only technically interesting but is also attractive from a business perspective.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE..
2. Alketbi, A., Nasir, Q., & Talib, M. A. (2018, February). Blockchain for government services—Use cases, security benefits and challenges. In *2018 15th Learning and Technology Conference (L&T)* (pp. 112-119). IEEE..
3. Alshehri, M., & Drew, S. (2010). E-government fundamentals. In *IADIS international conference ICT, society and human beings*,.
4. Melin, U., Axelsson, K., & Söderström, F. (2016). Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective. *Transforming Government: People, Process and Policy*..
5. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *9*(3), 01-09..
6. Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, *4*, 1-14.."
7. Bergquist, J. (2017). Blockchain Technology and Smart Contracts: Privacy-Preserving Tools.."
8. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavué, C. (2019, June). Blockchain solutions for forensic evidence preservation in IoT environments. In *2019 IEEE Conference on Network Softwarization (NetSoft)* (pp. 110-114). IEEE..
9. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71..
10. Ata-Ullah, N., & Ijaz, S. (2016). This crooked system: police abuse and reform in Pakistan. Human Rights Watch [online]. Available from: https://www. hrw. org/report/2016/09/26/crooked-system/police-abuse-and-reform-pakistan [Accessed 21 Jul 2017]..
11. Rewterz. THE WORST DATA BREACHES OF 2018. Rewterz Pakistan, October 24, 2018 http://www.rewterz.com/articles/the-worst-data-breaches-of-2018.
12. De Filippi, P., & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, *3*(2).
13. FORTNEY, LUKE. 2019. "Blockchain, Explained." https://www.investopedia.com/terms/b/blockchain.asp.
14. Halpin, H., & Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 1-3). IEEE..
15. Vergel Vergel, R. A. (2019). Blockchain: auditoría, contabilidad y normativa..
16. Hegadekatti, K. (2017). Legal Systems and Blockchain Interactions. *Available at SSRN 2893128*."
17. Hyperledger. 2019a. "Membership." https://hyperledger-fabric.readthedocs.io/en/release-1.4/membership/membership.html. 2019b. "Peers." https://hyperledger-fabric.readthedocs.io/en/release-1.4/peers/peers.html.
18. Iqbal, Zaheema. 2018. Cyber Security In Pakistan: Myth Or Reality – OpEd. https://www.eurasiareview.com/12012018-cyber-security-in-pakistan-myth-or-reality-oped.
19. Jun, M. (2018). Blockchain government-a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity*, *4*(1), 7..
20. Khatwani, S. (2018). What Are Private Blockchains & How Are They Different From Public Blockchains. *Recuperado de: https://coinsutra. com/private-blockchainpublic-blockchain*..
21. Kikitamara, S., van Eekelen, M. C. J. D., & Doomernik, D. I. J. P. (2017). Digital identity management on blockchain for open model energy system. *Unpublished Masters thesis–Information Science*.."
22. King, Ray. 2019. "What Is a Smart Contract and How Does It Work?" https://www.bitdegree.org/tutorials/what-is-a-smart-contract/.
23. Law, A. (2017). *Smart contracts and their application in supply chain management* (Doctoral dissertation, Massachusetts Institute of Technology).."
24. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-5). IEEE..
25. Malik, Tariq. 2018. "Reforming the FIR System: Part-I." https://www.thenews.com.pk/print/384673-reforming-the-fir-system.
26. Mamun, M. (2018). How does Hyperledger Fabric works. URL https://medium. com/coinmonks/how-does-hyperledger-fabric-works-cdb68e6066f5..
27. Awan, J., & Memon, S. (2016). Threats of cyber security and challenges for Pakistan. In *International Conference on Cyber Warfare and Security* (p. 425). Academic Conferences International Limited..
28. Milkovich, D. (15). Alarming Cyber Security Facts and Stats. *Cybint Solutions*. /.
29. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.'"

30. Ølnes, S. (2016, September). Beyond bitcoin enabling smart government using blockchain technology. In *International conference on electronic government* (pp. 253-264). Springer, Cham..
31. Ølnes, S., & Jansen, A. (2017, September). Blockchain technology as s support infrastructure in e-government. In *International conference on electronic government* (pp. 215-227). Springer, Cham..
32. Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355-364.."
33. Piekarska, Marta. 2019. "Hyperledger: BlockChain Technology for Business." https://wiki.hyperledger.org/.
34. Di Pierro, M. (2017). What is the blockchain?. *Computing in Science & Engineering*, *19*(5), 92-95..
35. Raskin, M. (2017). The law and legality of smart contracts. 1 Georgetown Law Technology Review 304. *Consultado el*, *13*(06), 2019.."
36. Richter, J., Kuntze, N., & Rudolph, C. (2010). Securing digital evidence. In B. Endicott-Popovsky, & W. Lee (Eds.), *Proceedings of the 5th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2010)* (Vol. 2010, pp. 119 - 130). IEEE, Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/SADFE.2010.31.
37. Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal*, *12*, 21-34.."
38. Michalak, S. C., Facelli, J. C., & Drew, C. J. (1999). Decentralized Information Technology Requires Central Coordination!. *CAUSE EFFECT*, *22*(4), 42-50.
39. Seppälä, J. (2016). The role of trust in understanding the effects of blockchain on business models (Master's thesis)..
40. Shabbir, S. S. (2014). The failure of the police system in Pakistan. In *The Express*. /.
41. Siddiqui, I. (2018). What The Hell Is Blockchain And How Does It Works?. *Simplified). accessed on August*, *27*, 2019."
42. Pakistan's cyber security. Retrieved March 17, 2022, from https://www.thenews.com.pk/print/395751-pakistan-s-cyber-security.
43. Malik, T. (2014). Technology in the service of development: The NADRA story. *Center for Global Development*..
44. Tasnim, M. A., Omar, A. A., Rahman, M. S., Bhuiyan, M., & Alam, Z. (2018, December). Crab: Blockchain based criminal record management system. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 294-303). Springer, Cham..
45. Raj, V. (2018). Hyperledger fabric architecture: Explained in detail.
46. Weiss, M., & Corsi, E. (2017). Bitfury: Blockchain for government. *HBS Case Study*, *12*, 818-031.
47. Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. *Technology Innovation Management Review*, *7*(10)..
48. Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), 49-56..