Blockchain Based Business Digital Identity for Protection of Patents and Intellectual Property

Author

Sheeza Jamil

00000329041

Supervisor

Assoc. Prof. Dr. Fahim Arif

A thesis submitted to the faculty of Department of Computer Software Engineering, Military College of Signals, National University of Sciences and Technology (NUST), Rawalpindi, in the partial fulfillment of the requirement for the degree of MS in Software Engineering.

(August 2023)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Miss Sheeza Jamil**, Registration No. **00000329041**, of **Military College of Signs** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor **Assoc. Prof. Dr. Fahim Arif**

Date: _____

Brig
Head of Dept of CSE
Mil College of Sigs (NUST)

Signature (HOD): _____

Date: 23/11/23

Signature (Dean/Principal) _____

Date: 23/11/23

for

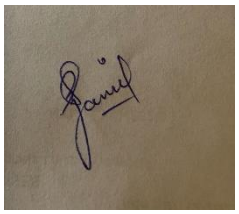
Brig
Dean, MCS (NUST)
(Asif Masood, Phd)

Declaration

I, ***Sheeza Jamil*** declare that this thesis "**Blockchain Based Business Digital Identity for Protection of Patents and Intellectual property**" and the work presented in it are my own and have been generated by me as a result of my original research.

I confirm that:

1) This work was done wholly or mainly while in candidature for a Master of Science degree at NUST.
2) Where any part of this thesis has previously been submitted for a degree or any other qualification at NUST or any other institution, this has been clearly stated.
3) Where I have consulted the published work of others, this is always clearly attributed.
4) Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my work.
5) I have acknowledged all main sources of help.
6) Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.



Sheeza Jamil,
00000329041 MSSE27

Dedication

“In the name of Allah, the most Beneficent, the most Merciful"

Glory be to Allah (S.W.A), the Creator, the Sustainer of the Universe. Who only has the power to honor whom He please, and to abase whom He please. Verily no one can do anything without His will. From the day, I came to NUST till the day of my departure, He was the only one Who blessed me and opened ways for me and showed me the path of success. There is nothing which can payback for His bounties throughout my research period to complete it successfully. I dedicate this thesis to myself, my family and my friends who supported me in achieving my goals.

Abstract

Using cutting edge technology solutions is crucial in the quickly changing corporate management and intellectual property protection market. Businesses have flourished by adopting the applications of technology but securing the business and its ownership of intellectual property (IP) is still one of the major concerns these days. Businesses in Pakistan are facing challenges due to economic, financial, political and social factors. There are many fraudulent businesses which are not registered by the government. Fraudsters impersonate the business or create fake profiles to defraud customers. Business suffers lack of credibility, limited access to digital marketplaces and difficulty in complying with regulations. Moreover, business may have difficulty protecting their patents or trade secrets from infringement. Competitors may misappropriate the business's inventions, ideas, or proprietary information without authorization. All these challenges not only affect the business but also has an adverse effect on the economy of Pakistan.

This research offers a thorough foundation for a blockchain-based digital identity system for businesses that is adapted to Pakistan's particular requirements. The architecture is made up of several different parts, such as tax administration, intellectual property matching, and user registration and authentication by applying software engineering practices. By utilizing the capabilities of Hyperledger Fabric blockchain technology, the suggested decentralized model guarantees safe and effective communication between companies, authorities, and individuals. In order to improve security, cooperation, and transparency within the business ecosystem, the system integrates elements of identity verification, access control, and patent registration. The architecture's ability to simplify business registration, promote innovation, safeguard intellectual property rights, and improve tax collection procedures highlights how pertinent it is to national regulations.

We have conducted a case study of Pakistan to identify potential challenges and threats in business registration, taxation and IP protection. To validate our proposed framework we adopted grounded theory for qualitative analysis via questionnaire. A total of 98 responses from IT professionals, business owners and researchers were gathered to conclude our research. The study reveals a viable way for Pakistan to use blockchain technology together with deep learning and software engineering practices to modernize corporate processes and manage intellectual property in a way that is consistent with its distinct socioeconomic environment.

Acknowledgments

All praises to Allah for the strengths and His blessing in completing this thesis. I would like to convey my gratitude to my supervisor, Assoc. Prof. Dr. Fahim Arif, for his supervision and constant support. His priceless help of constructive comments and suggestions throughout the experimental and thesis works are major contributions to the success of this research. Also, I would like to thank all my friends for their helping hand and moral support. Lastly, I am highly thankful to my parents for their constant support and prayers. I would like to thank them for their patience, cooperation and motivation in times of stress and hard work.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IP	*Intellectual Property*
IPO	*Intellectual Property Organization of Pakistan*
SECP	*Securities & Exchange Commission of Pakistan*
FBR	*Federal Board of Revenue*
NTN	*National Tax Number*
AES	*Advanced Encryption Standard*
CNN	*Convolutional Neural Network.*
LSTM	*Long Short Term Memory.*
GAN	*Generative adversarial network.*
NLP	*Natural language processing.*

1. Introduction

1.1 Introduction and Motivation

Within the domain of contemporary business and technology, the progression of digital systems has presented a range of prospects and difficulties for global economies. In nations such as Pakistan, it is crucial to cultivate a climate that promotes corporate expansion and innovation. Consequently, the adoption of state-of-the-art solutions becomes a strategic requirement. This research presents a forward-thinking conceptual framework and architectural design aimed at effectively addressing the unique requirements of Pakistan's commercial environment. This framework seeks to transform the processes of company registration, intellectual property protection, and taxes management via the use of blockchain technology. The integration of these essential elements within a holistic framework not only optimizes procedures but also establishes the groundwork for a corporate environment that is characterized by enhanced transparency, security, and efficiency.

The rationale for the development of this suggested framework arises from the intricate and diverse array of obstacles encountered by firms operating in Pakistan. The conventional approaches to company registration, intellectual property protection, and tax administration have often been characterized by inefficiencies, delays, and a lack of transparency. In addition, the increasing need to promote innovation and safeguard intellectual property rights necessitates the adoption of a transformational methodology. This purpose is consistent with the overarching national objective of fostering economic development, facilitating company operations, and establishing a favorable climate for technical progress.

A lot of reach has already been carried out in context of Digital identities. Many countries like Estonia, UAE, Switzerland, Luxemburg has implemented digital identity system for its residents. As a successful pilot project, the City of Switzerland Zug [12] is utilizing the Ethereum blockchain to provide its inhabitants e-ID. The author [9] provides information about a 2018 conference with the subject "Government Services and Digital Identity." This lists the e-identity initiatives of Estonia [11] and the IDs of Zug citizens in Switzerland [10] as significant use cases for Europe in the eID environment. It describes real-world blockchain implementations from many nations in the area of public

administration. This applicability gives up an idea of transforming business identity management where their end-to-end systems are taken into a digital platform. This requires sound research on the considering all the aspects of a country regulations and standards as well as efficient software designing and development for its implementation. Daniela proposes a reference architecture in for the digital identity management, but the layered approach is time taking and the updates from blockchain networks can cause delays [13].

The core of this invention is centered upon Hyperledger Fabric, a blockchain technology that is well recognized for its adaptability, robust security measures, and capacity to handle large-scale operations. The architecture of Hyperledger Fabric, characterized by its permissioned network and modular design, is well-suited to meet the specific needs of Pakistan's business environment. Hyperledger Fabric facilitates the involvement of authorized stakeholders and preserves data integrity by enabling semi-decentralization and implementing customized access restrictions. The inherent compatibility of the platform with smart contracts and its ability to seamlessly integrate with other systems make it an ideal solution for the automation of intricate operations and interactions within the envisioned framework. Together with Hyperledger we incorporate Event Driven architectural style, assumes a critical role in achieving the objectives of this architecture by prioritizing security, privacy, and interoperability.

1.2 Background

The need for new solutions to solve the particular issues encountered by nations such as Pakistan is becoming more important in the fast-expanding world of technology and business. The suggested framework and architecture reflect a ground-breaking effort to use blockchain technology to build a commercial digital identification system that is uniquely customized to Pakistan's national needs. This project aims to address the complex challenges of company registration, intellectual property protection [16], and effective tax administration within the context of the country's economic situation. The architecture aims to not only streamline administrative processes but also foster an environment of trust and transparency that fosters innovation and growth by seamlessly integrating various government bodies such as the Securities and Exchange Commission of Pakistan (SECP), the Federal Board of Revenue (FBR), and the Intellectual Property Organization (IPO). The system displays a forward-thinking approach to fulfilling the digital and regulatory demands of Pakistan's contemporary business environment, with machine learning approaches increasing intellectual property matching and secure event-driven

communication enabling real-time coordination. This context sets the setting for an examination of how the proposed framework connects with the nation's aims and ambitions for long-term economic growth and technological innovation.

1.3 Problem Statement

Pakistan is underdeveloped country which is facing serious socio-economical and financial crisis. The corporate landscape and intellectual property protection processes require contemporary and safe solutions. Traditional business registration, authentication, and IP management methods are inefficient, opaque, and vulnerable to fraud [15] that adversely affects the economic growth. Complex tax collection methods can also be error prone. These issues hinder corporate growth, intellectual property rights, and government regulation and revenue collection. There is a need to propose a system that best utilizes software engineering and information security practices to provides secure digital identities, streamlined business registration, reliable intellectual property matching, and efficient tax management to address these issues. This research proposes a comprehensive architecture adapted to Pakistan's economic and regulatory context to bridge the gap between traditional practices and technological breakthroughs.

1.4 Aims and Objective

The research aims to achieve the following goals:

- To Review and analyze challenges and threats to the current regulatory framework for business identity and intellectual property of Pakistan.
- Analyze the benefits of using blockchain for business digital identities and their Intellectual property.
- Propose blockchain based business digital identity framework for Pakistan using software engineering practices that handles business related process and data, protects their intellectual property, and comply with National regulations.
- To validate the proposed framework.

1.5 Relevance to National Needs

Businesses in Pakistan are facing major challenges related to businesses identity theft. Growth of counterfeiting and piracy products in the market, not only adversely affects the

original businesses but also results in the loss of achieving tax target by the state which affects the economy of Pakistan. By proposing the framework for business digital identity using blockchain technology, Pakistan can implement a secure and transparent National business registration and authentication system that protects patents and IP according to the National laws regulations of Pakistan. The enforcement of intellectual property rights by blockchain technology can automatically give rewards and penalties which reduce delaying responses from legal/governing bodies. The blockchain-based mechanism has the potential to provide many more benefits for performing government tasks for service provision, such as requiring fewer work hours and employs, lowering accountability management costs, reducing the likelihood of corruption, storing business data in a secure manner, and increasing trust in government departments many folds.

1.6 Advantages

These benefits show how the suggested structure satisfies the unique requirements of the business digital identification system for safeguarding intellectual property in Pakistan while also boosting productivity, security, and collaboration.

Decentralization and confidence: The adoption of blockchain technology, specifically Hyperledger Fabric, ensures decentralization while promoting participant confidence. Because there are multiple actors with partial control, there is less chance of fraud or manipulation.

Secure Digital Identity: Using cryptographic keys to ensure authenticity, the system provides enterprises with a secure digital identity. This provides security against access fraud and identity theft.

Effective Business Registration: The automated process for registering a business speed up approval and cuts down on administrative delays. Processes for registration and taxation are streamlined by integrated modules with SECP and FBR.

Protection of Intellectual Property: Using machine learning to match intellectual property improves protection against infringement. Patents are transparently validated, protecting innovation.

Private Data Management: To balance data privacy and on-chain validation, sensitive data is stored off-chain with references on-chain. This increases privacy without sacrificing traceability.

Smart contracts automate operations, ensuring accuracy of execution and minimizing human mistakes. Flexible smart contracts. These flexible contracts increase organizational effectiveness.

Business interactions that promote cooperation and innovation include the purchase and sale of patents. Fairness and transparency are guaranteed by secure transactions supported by cryptography.

Real-time tax calculation and collection are provided by the system, which minimizes manual work. Tax-related processes are precisely and securely carried out through smart contracts.

Enhanced Data Security: Cryptographic methods secure data against alteration and unauthorized access. The immutability of the blockchain strengthens data integrity even more.

Transparent Auditing: The transparency of the blockchain creates a trail of all transactions that can be examined, assisting with regulatory compliance and promoting accountability.

Event-driven design accelerates communication between blockchain and backend systems, providing real-time changes and effective coordination. This results in effective event management.

Scalability and Performance: Hyperledger Fabric's modular structure makes it possible to scale. As the network expands, channels enable selective data sharing and retain high performance.

Cybersecurity Measures: To defend against online dangers and attacks, the framework uses encryption, access controls, and continuous monitoring.

1.7 Area of Application

- Digital business identity application at National level.
- Businesses industry
- Intellectual Property Organization of Pakistan
- Securities & Exchange Commission of Pakistan (SECP)
- Law enforcement agencies

1.8 Thesis Organization

The thesis has been organized as follows:

- Chapter 2 review and analyze the related work in context of Business Digital Identity for securing Intellectual Property. Section 2.1 thoroughly discusses the basics of blockchain and Hyper Ledger fabric blockchain. Section 2.2 gives an overview of the use of blockchain for digital identity. Section 2.3 gives an overview of the use of blockchain for Intellectual property management 2.4 provides summary of machine learning and deep learning techniques for Patent matching.
- Chapter 3 Discusses the case study of Pakistan's Traditional Regulatory Frameworks for Business and Intellectual Property. It highlights the challenges and threats to the existing systems.
- Chapter 4 proposes the framework for conducting the analysis. It gives the architecture and streamlines the workflows for Business end to end processes.
- Chapter 5 gives the results and analysis of the proposed framework. It also provides an insight to counter the challenges and threats to the existing system.
- research by summarizing it. It also defines the limitations of the work done and suggests future direction in the corresponding domain.

1.9 Summary of Introduction

In this chapter, the introduction and motivation behind a forward-thinking conceptual framework is offered to solve difficulties in Pakistan's commercial sector using blockchain technology, especially Hyperledger Fabric. The background of research in blockchain based business digital identity signifies the relevance to national needs and highlights the

problems that the inefficiencies and lack of transparency of traditional approaches have made disruptive alternatives necessary which needs be tackled by this research work. The advantages taken out of this research are also discussed and applicability of this work in different sectors. Lastly, this chapter defines the organization of the whole work.

2. Literature Review

2.1 Overview

The literature review has been done in various dimensions to cover the applicability of the proposed research topic. The blockchain basics concepts, key features and types has been studied thoroughly to choose the best suitable blockchain. Moreover, we studied the applicability of blockchain for digital identity management and patent protection. The literature highlights the use of machine learning/deep learning techniques for patent protection along with the blockchain.

2.2 Blockchain

Blockchain is a combination of security and encryption protocols that allows multiple nodes to record and verify transactions. Blockchain technology was introduced by Satoshi Nakamoto in 2008 [21] for the purpose of keeping track of Bitcoin transactions as well as other encrypted digital currencies. It ensures data integrity, immutability, transparency by storing the data in a distributed ledger and decentralized manner. This decentralized architecture system uses a peer-to-peer network to impose reliability as well as transactional integrity [27]. Every block that contains the transactional data is approved by the consensus protocol to make it a part of the blockchain [22]. A growing public ledger is maintained at each node that reflect the most recent state of a blockchain. Data is readily available and cryptographically protected against alteration and modification. Moreover, blockchain performs its functions without any central body and avoids the use of third parties like banks for intervention and mediation.

Blockchain technology has been progressively adopted by all the domains and industries to promote security and transparency among their processes and the way their data has been stored, validated and accessed [30]. Blockchain 1.0 refers the to the use of technology for cryptocurrencies like Bitcoins, Ethereum etc. Later, Blockchain 2.0 was introduced as baseline for contracts for financial application as a self-executing code of terms and agreements known as Smart contracts. Now blockchain 3.0 [31] has expanded its application in multiple domains including transparent supply chain management, secure IOT data sharing, healthcare, real estate transactions, trustworthy voting system, secure identity management systems, protection of intellectual property rights etc.

2.2.1 Working

To provide insights into the significance of blockchain we need to understand the structure of the blockchain. Blockchain is a collection of blocks connected to each other which contains the transactional data. Here's the breakdown of the structure of each block in the blockchain [3].

1. **Block Header:**

   Block header contains all the meta data about the block i.e Version number, Hash of previously mined block, Merkle root that acts as a summary of all the transactions hashes, Timestamp which tells time and date of creation of block, Nonce is a number used only once to find the hash of the block.

2. **Transaction:**

   It contains the transaction data and information about the sender and receiver.

3. **Hash**: A digital fingerprint that uniquely identifies the block containing and encrypts the metadata.

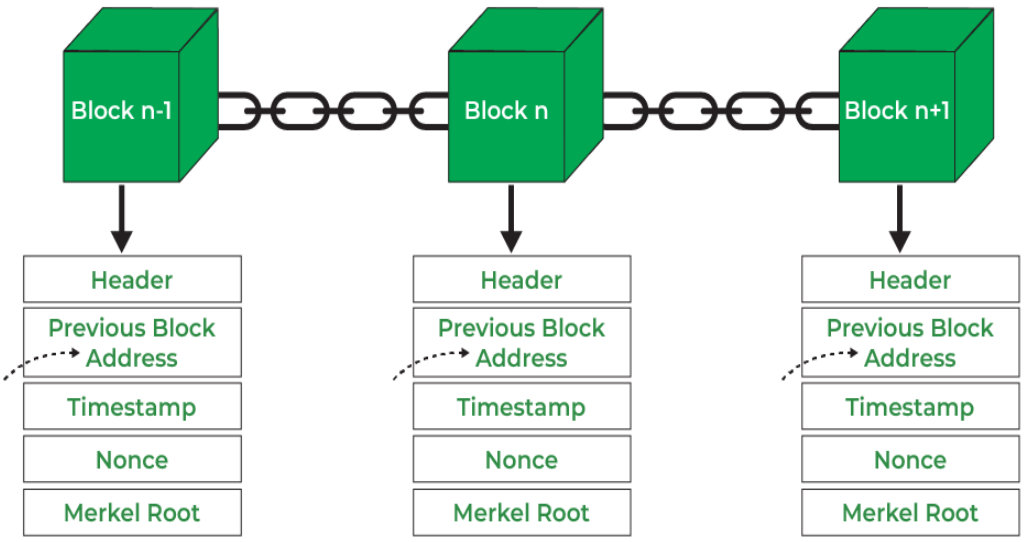


Figure 2. 1 Structure of Blockchain

Whenever a transaction is made, a block is created and some of the nodes in the blockchain known as miners compute the Hash of the newly created block known as consensus mechanism. The first miner who mines the block gets the reward for solving this complex puzzle. The nodes verifies the transaction and a block is appended to the end of the blockchain. The reference to the previous block's hash the new block's header links it to the chain. Hence, all the nodes update their ledger. The data of the blockchain is not saved in a single place. So,

to reflect a new block to the blockchain every single computer system is upgraded. Fig. 1 shows the basic working steps of Blockchain technology [29].

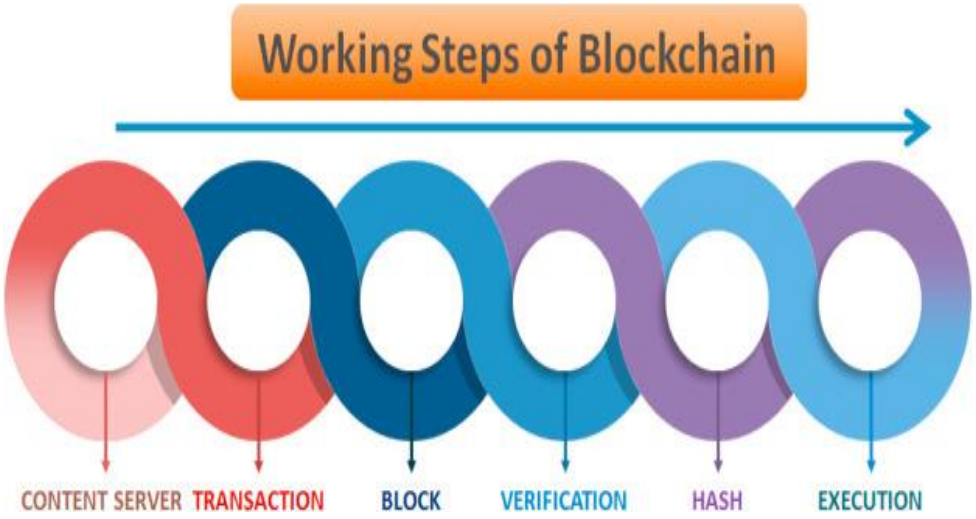


Figure 2. 2 Working of Blockchain

2.2.2 Key Features of Blockchain

Blockchain technology is composed of four key features. The primary feature of blockchain means that blockchain does not have to depend on a centralized branching system anymore therefore the disturbed data can be upgraded as well as data can be stored and recorded by using this system [24]. The four-key element of block chain are given below:

- **Transparent:**

  The blockchain system is reliable and trustworthy because the data recorded by this system in each branch is transparent and even the upgrading and updating of data is transparent as well. The blockchain system is transparent to the public and everyone. Individuals can use these technological systems to build new applications.

- **Autonomy:**

  The main idea is to gain the trust and reliance of an individual and an entire system on the basis of agreement that every branch in the blockchain system will upgrade data or transfer data safely. It is enabled by the decentralized nature of blockchain where control their data n actions.

- **Immutable:**

  Any records or data cannot be changed until or unless someone takes control of more than 51% of the branch at the same time till then the data and records will be saved forever.

- **Anonymity:**

  Blockchain technologies have solved the trust issues between node to node, therefore the transaction and data transfer will be safe, you just need to know the individual address of the block chain.

2.2.3 Types of Blockchain

There are three types of block chain systems: consortium, public and private block chain. Every type of block chain system has its own scheme and scenario. The protocol of agreement will be adopted if they fit in the demand of the application scenario of the system.

In public blockchain, everyone can take part in the agreement process and the recorded data will be transparent to the public. Proof of work, Proof of stake, and Delegated proof of stake can be applied to public blockchain. Consortium blockchain and private block chain belong to the approval of blockchain because only permitted branches or nodes can engage in the agreement process. In Ripple and practical byzantine fault tolerance (PBFT) the identity of each node and branch is known to the public therefore they are suitable for both consortium blockchain and private block chain. Because of the high efficiency and powerful stability of consensus the consortium block chain and private block chain are not decentralized like public block chain, these two applications are worthier and more appropriate for some organizational purpose [22].

1. **Public blockchain:**

   Public can also engage in the process of getting consensus and can also verify, examine, and check the transactions. For example, public blockchains include Ethereum and Bitcoin.

2. **Consortium blockchain:**

   It means the node that has authority can be selected in advance. Normally has partnerships like business-to-business partnership. However, blockchain data can be seen as partly decentralized as well as transparent, open or private. For example, Hyperledger consortium blockchain.

3. **Private blockchain:**

The data access is not easy due to the strict authority management. The nodes in the private block chain will be secure and not every node can cooperate in this blockchain). The table below shows the classification of blockchain with respect to access and validation.

Table 1 Classification of Blockchain with respect to validation and access

Actions	**Public Blockchain**	**Consortium blockchain**	**Permissioned Blockchain**
Managing to add a node in the network	Not contemplated	Depends on the legal contract and requirement.	Depends on the legal contract and requirement.
Validating/ mining a node	Everyone – costly mining procedure	Only if permission granted, depends on smart contract.	if permission granted
Add a node that holds the blockchain	Everyone	Everyone	if permission granted
Deploy a smart contract	Everyone but requires fee/gas	Only if permission granted	Only if permission granted
change the state of blockchain (writing rights) by Sending trans-actions	Everyone but requires fee/gas, smart contracts changes their state if transactions come from authorized node	Everyone. Smart contracts change their state if transactions come from authorized node	Requires correctly logged and authorizations. A check on the nodes might also be performed
Send read only transactions to smart contracts	Everyone	Everyone but request accepted from authorized nodes	Requires correctly logged and authorizations. A check on the nodes might also be performed
Read access on Blockchain	Everyone	Everyone	Requires correctly logged and authorizations

2.2.4 Pros of Blockchain

The positivity and the advantage that has been bought by block chain system and technology are given below [27]:

- **Transparency:**

Distributed ledger or record is used by block chain that is kept by the individual parties and this data can only be upgraded by the consensus process. That means that the file or data can only be upgraded or updated if all legal groups agree to do so. The stored transaction data of block chain technology is transparent, open and visible to all the user parties of that specific chain [27]

- **Enhanced security:**

  Block chain is more safe, stable and strong than other recorded management systems because transactions can only be added after the agreement of all the legal parties. With each block in the system, a save hashing process has been attached, the purpose of this process is to make the block safer and secure which holds the number of transactions. Therefore, this process has made the block strong and secure, so it is impossible to temper a block because modification of other blocks will be required as well.

- **Enhanced traceability:**

  Transactions are transparent and open to all legal parties of that block which has made the traceability of data and process easy. This has also led to the tracking operation convenient for block chain. If the individual party's enterprisers and deal with supply chains this chain will make their tracking easy and convenient.

- **Fast and efficient:**

  This system is faster and highly efficient because it is automatic operation, no paperwork is involved, and it is operated without the involvement of a third party.

- **Cost-effective:**

  This system does not require the involvement and intervention of third parties as well as no intermediary is needed therefore this system is more cost-effective.

2.2.5 Cons of Blockchain

This disadvantage and disbenefits of block chain technology and system are given below:

- **Real World Enforcement:**

  Blockchain system is "ON-CHAIN" though the real world is more into the "OFF-CHAIN" process which is a challenge for this system. Smart contracts are simple software that can impose only that data state which has access on the block chain. In a fully decentralized network, there should be consensus on the state of the ledger among all the nodes at all times. Nodes cannot individually connect to external systems without compromising the consensus and the information (external) should be valid and

authentic. If the third party is added it will affect the benefit of block chain that is a decentralized system for example, Oracles in block chain. Oracle as a third party should strictly follow the rule of block chain and don't give them false information and should be strict [25]. Smart contracts will influence the block chain in terms of immutability. Standard software systems are fixed and enhanced all the time. They are not yet recognized as legal contracts until the legal framework evolves and lawyers become quasi-programmers [25].

- **Performance:**

  In the theoretical process, the Ethereum block chain does twenty-five transactions per second though on the other hand bitcoin does seven transactions per second. These transaction throughputs have still to reach the standards required in industries like Retail and Finance. Complex consensus mechanisms are not needed in a private environment which will improve the performance of throughput, but its implementation is still a challenge.

- **Standardization:**

  As technology grows and develops businesses will need to build sustainable and interoperable solutions based on industry standards for example the objective of private consortiums to boost industry standards. But it will be tough as the block chain system does not fit in the regulatory framework. Regulators and market participants need to work together to ensure the compliance of future standards [25].

- **Governance:**

  The governance of the block chain system is straightforward that one company or consortium block chain who have made it will rule it.

2.2.6 Hyperledger Fabric

Hyper ledger fabric is a blockchain based open-source framework for the development of permissioned and consortium blockchain applications by IBM and Linux Foundation. It is best known for its modular architecture [34], suitability for enterprise level use cases and security features. The self-executing smart contracts are termed as "Chaincodes" which are executed by nodes. While there are multiple types of nodes so they work collectively to form a secure, scalable and private solutions for the business needs by means of Docker container technology.

The specific functionalities of these nodes are as below.

- Peer Nodes: These are required for the ledger to be maintained, smart contracts to be executed, and transaction processes to take place. They are separated into endorsing and committed peers, each with its own set of responsibilities.
- Ordering Nodes (Orderer Nodes): These nodes are in charge of ordering transactions in the proper order and guaranteeing consensus. They organize approved transactions into blocks for approval.
- Certificate Authority (CA) Nodes: These nodes provide digital certificates to participants for secure communication, identity verification, and network security.
- Membership Service Provider (MSP) Nodes: These are responsible for identification and access control, as well as creating trust rules to assure authorized participation.
- Client Nodes: These are the nodes that interact with the network by submitting transactions and accessing the ledger. They depend on peers to carry out blockchain transactions.

Hyper ledger uses the Endorsement policy and Practical Byzantine Fault Tolerance protocol for the consensus mechanism. Whenever a transaction is initiated in the network, the endorsers peer nodes validate the transaction and returns it to the application. Ordering nodes then create the block against that transaction and decide the order of all the transaction and pass it to Anchor peers. Anchor peers then broadcast the transaction to the network so all the nodes can update their ledger [33].

2.3 Blockchain and User Identity Management

Numerous Identity Management (IDM) solutions have been devised in the absence of using Distributed Ledger Technology (DLT). Consequently, a number of issues have arisen with relation to the consolidation of power or influence by external actors, as shown in prior research. On contrary, scholarly endeavors have endeavored to provide remedies based around the utilization of blockchain technology. The use of blockchain technology in the advancement of IDM systems has presented many issues pertaining to centralization, particularly in the context of private blockchains. The intricacies inherent in this particular context are to the establishment of private blockchains, the implementation of a central governing entity, the assurance of data accessibility, and the proficient management of cryptographic keys. The domain of centralized identity management has several challenges in safeguarding user privacy. This involves a basic reliance on external entities for the creation, verification, and

validation of identities and their associated attributes. The reliance on third-party intermediaries for accessing services from suppliers amplifies customers' susceptibility to surveillance. The presence of a Single Point of Failure (SPOF) poses a significant challenge in the realm of centralized identity management.

The potential of integrating blockchain technology with identity management is substantial, since it presents a variety of possibilities that may enhance system efficiency and safeguard user privacy. The degree of ambition enhancement is greatly impacted by prominent characteristics such as decentralization, transparency, and immutability. However, it is important to thoroughly contemplate the associated challenges. The issue of scalability in blockchain systems has substantial significance and necessitates meticulous deliberation as the integration advances [36].

The authors of the cited article [38] provide a detailed account of a new approach to IDM using a private blockchain platform. The primary objective is to develop a streamlined and efficient protocol that caters to the unique requirements of organizations operating in the realm of the Internet of Things (IoT). This study uses the Hyperledger Fabric architecture to provide a theoretical foundation for intelligent dwellings. Additionally, it utilizes the Golang programming language for the development of chain codes. The fundamental components of the IDM system are categorized into three distinct phases: identity registration, identity verification, and identity revocation. These stages provide simultaneous execution. Smart contracts are used throughout these phases to interact with the blockchain. This research investigates the possibility of the aforementioned technique to enhance the intercommunication between entities inside the IoT. The study includes an examination of a consortium membership service and an identity management system. The utilization of a private blockchain is acknowledged for its potential to augment security measures and improve scalability. Nevertheless, it has been observed that several attributes of the paradigm have a similarity to centralization rather than decentralization. Consequently, this phenomenon amplifies the potential risks associated with SPOF and complications associated with centralized authority.

In a particular study outlined in reference [64], researchers have developed a prototype of a decentralized IDM system specifically tailored for the public transit industry. The architectural framework is founded upon the principles of self-sovereign identity and use the Hyperledger Indy blockchain as a proof-of-concept. The main aim of this unique solution is to reduce the

need of having multiple travel cards for those who often use different modes of transportation in diverse jurisdictions. The proposed plan is to provide a standardized platform for transportation services in Europe via the implementation of an IDM system based on blockchain technology. This system empowers users with direct authority over their personal identities. The architectural design enables the generation of many decentralized identification (ID) systems for individual users, followed by secure key pairs to permit safe data transmission.

For the past 20 years, the first nation to deploy digital identification for its inhabitants is Estonia. It allows users to digitally authenticate themselves so they may access services like banking, eVoting, and health care [40]. The authors propose the use of blockchain technology to establish a decentralized IDM system in the public sector of South Korea, as stated in reference [63]. The researchers introduce a mobile application that has been designed to enhance the efficiency of producing electronic identity cards. Subsequently, the distribution and administration of these cards are undertaken by a centralized governing body operating at the national level. The process of validating user IDs is accomplished via the use of a unique QR code that is designed to interface with a certain application. The present application is designed using a client-server architecture that has been implemented using Hyperledger Fabric V1.0. The incorporation of Amazon Web Services (AWS) aims to enhance the operational efficiency of the process. The use of hash map-based key-value pairs and chain code for storing user data in a database displays some characteristics associated with centralization. This gives rise to concerns over the participation of the national central authority and potential limitations in broader implementations.

The proposal of a framework called Blockchain-based Identity Management and Access Control (BIMAC) has been put out as a potential solution to the challenges encountered by traditional banking systems, as cited in reference [65]. The framework has been developed using the Model-View-Controller (MVC) architecture, with the objective of enhancing user experience via facilitating easy access to multiple bank accounts. The use of self-sovereign identity principles within the context of open banking aims to simplify the adoption of efficient authentication mechanisms. A proof-of-concept IoT identity management system has been developed, as described in reference [37], with the aim of preserving the integrity of data provenance records in IoT resources. The Solidity programming language is used in the construction of the blockchain concept, then implemented on the Kaleido platform. The main goal of this system is to preserve the data integrity inside an organization's networked resources, with a particular focus on the Internet of Things (IoT) domain.

Following that, numerous nations adopted blockchain technology to create digital identities and integrate it into their corporate structures for effective business management. In terms of blockchain technology and metaverse, South Korea is considered to be at the forefront. According to a study released in June 2021 by the market research firm Report Linker, the blockchain identification market would increase by an additional $3.58 billion by 2025, representing a compound annual growth rate of 71% [62]. This demonstrates that corporate and government verification of its digital identity are equally crucial to business digital identities as are users' digital identities.

The authors propose the use of a verified anonymous identity management system (VAIM) as a potential method to enhance privacy within the realm of blockchain identity management, as mentioned in reference [39]. The utilization of zero-knowledge proof (ZKP) methodologies augments the system's ability to uphold the property of unlink ability.

The IDM cloud protocol, which is built on the Ethereum platform and described in reference [61], seeks to tackle the problem of reliance on external entities in traditional identity management systems. Smart contracts are used to enhance the level of secrecy in data transmission and to augment the flexibility of the system.

2.4 Blockchain and Intellectual Property Management

The incorporation of "Legal Tech" solutions inside the field of legal professionals has been met with significant hesitation. This reticence is especially noticeable in intellectual property (IP) organizations, where there is legitimate concern about using AI and blockchain technology. The consequences of an incorrect technical choice are recognized as possibly permanent, with major repercussions for their clientele's well-being. Furthermore, established practitioners in the field of IP law frequently lack direct exposure to these domains, have limited time to devote to the investigation of proposed solutions, and see these innovations as potential threats to their traditional business frameworks. To be thorough, the passion around AI and blockchain has spawned reasonable queries, as well as instances of false representation, speculative ideas, and misunderstandings. This means that these technical breakthroughs continue to be a mystery to a vast number of IP experts, remaining essentially unreachable within the operational scope of many IP organizations. This situation persists despite continuous democratization initiatives aimed at increasing access to AI and blockchain technology.

Wei Chen et al. focused on blockchain technology and its application to a basic study of intellectual property protection. It examines the blockchain technology's functioning mechanism, properties, and potential application scenarios. The article also addresses the background development status of blockchain and analyses local and international instances of blockchain technology being used to safeguard intellectual property. The review's goal is to help with the implementation of blockchain technology [68].

Ragot et al. address the applications of artificial intelligence (AI) and blockchain technology in intellectual property (IP). It underlines the significance of IP experts experimenting with AI and blockchain technologies in order to better understand their advantages and disadvantages. The paper also emphasizes the importance of carefully interpreting machine learning results and involving IP professionals in analyzing IP rights and violation. It defines blockchain as a decentralized database and discusses its possible uses in storing evidence of creative works. The article goes on to discuss how cryptographic hash functions and timestamps may be used to secure and validate data on the blockchain [67].

Using blockchain technology, businesses can be verified, and their patents and intellectual property rights can be safeguarded. China has made significant contributions to the use of blockchain technology for managing IP. According to Peng Zhu's analysis, blockchain technology has the ability to completely transform the way that intellectual property rights are managed by introducing a safe and transparent method of registering and confirming ownership. The author developed a blockchain-based approach that significantly improves the capacity to track original achievements and includes an automatic incentive-rewarding system for both the development and preservation of original achievements [66]. Savelyev investigated the legal implications of blockchain applications for copyright management and made the case that these applications could fundamentally transform the copyright management sector [35].

2.4.1 Patent Matching Through ML

To narrow the scope of the research currently we are only considering patents as an intellectual property to that need to be secured while this concept can be applied to Copyrights and trademarks as well. Machine learning fosters in the protection of patents by their infringement detection based on the similarities between the patentability document and already existing documents. The approaches for determining patent similarity and classifying patent documents are the main topics of this section's critical assessment of the body of literature. The review presents ground-breaking research in the fields of measuring patent

textual similarity and using machine learning for patent analysis. It includes discussions of both content and form level similarities.

2.4.2 Patent Similarity

Prior research has roughly divided patent similarities into two main categories with regard to content and form. Moehlre (2010) established a distinction between form-level similarity, which concentrates on textual congruencies and bibliographic parallels, and content-level similarity, which stresses structural factors such as the goal and application of patents [41]. Expanding on the idea of textual similarity in patents, Arts et al. (2018) introduced a keyword-centric approach for determining textual similarity by mining patent abstracts. This method was further strengthened by a Jaccard-based similarity measure that was approved by subject matter experts [42]. Lai and Wu (2005) conceived a patent taxonomy based on bibliometric co-citation analysis using bibliographic data as a metric [43]. A similar strategy was used by Rodriguez et al. (2015) to evaluate pairwise patent similarity via both direct and indirect co-citation connections [44]. The examination of Subject-Action-Object constructions (Wang et al., 2019) [45], a synthesis of semantic and syntactic structures (Yang et al., 2021) [46], and multifaceted word sense interpretations (Ahmad & Faisal, 2022) [47] are just a few examples of more recent contributions that have delved into linguistic analyses.

A considerable body of research has focused on methodological advancements, notably using the paradigms of deep learning, machine learning, and natural language processing (NLP). Cascini and Zini (2008) developed a patent similarity clustering approach that can identify functional and hierarchical interactions across patents [48]. A pioneering automated technique to calculate continuous similarity distances across patent duos was developed by Younge et al. (2016) [49]. Based on this, Feng (2020) promoted a technique that uses Doc2Vec processes to create vector space representations of patent abstracts [50]. The use of NLP in patent research has proved helpful. With an emphasis on keyword extraction and processing, Noh and Lee (2015) carried out text mining operations for patent examination [51]. For strategic technology planning, Joung and Kim (2017) used a keyword-centric modus operandi [52]. Works like Lee & Hsiang (2019) [53] are an example of the current surge in BERT-oriented methodologies in patent analytics.

2.4.3 Document Similarity in Natural Language Processing

This section delves into key literature focusing on the evaluation of pairwise document similarity within the field of natural language processing, considering that patents are

essentially documents in natural language. Kadhim (2019) presented a foundational framework for text classification, incorporating a study on supervised machine learning models, such as the K-nearest neighbors' model [54].

Recent research endeavors have concentrated on refining the efficiency of models. Farouk (2020) proposed a comprehensive methodology to evaluate sentence similarity. This method seamlessly blends structural and lexical similarities, giving special attention to the semantic nuances within sentences and leans heavily on the discourse representation structure (DRS) [55]. In a similar vein, Lan (2022) introduced a composite methodology that marries the idea of a similarity-weighted tree structure with the semiotic tenets postulated by Dong & Dong (2020) [56]. The core aim of this approach was to counteract the reduced accuracy stemming from the TF-IDF technique, whilst simultaneously circumventing the 'curse of dimensionality' [57].

Recent works have also showcased the integration of transformer-based architectures into text classification tasks. González-Carvajal and Garrido-Merchán (2020) exhibited the ascendancy of BERT over traditional TF-IDF embedding methods in machine learning-led text classification [58]. Garg and Ramakrishman (2020) introduced a BERT-centric methodology to craft adversarial examples tailored for text classification, aiming to bolster the resilience of text classification systems [59]. Furthermore, Viji et al. (2022) employed a Bidirectional Long Short-Term Memory (Bi-LSTM) model, augmented with weighted word embeddings via BERT fine-tuning. This hybrid model's efficacy in NLP tasks, such as gauging text similarity in question pairs or document pairs, was empirically verified [60].

2.5 Conclusion to Literature

In Conclusion, to this chapter an extensive literature review has been done regarding the blockchain basic working and concepts of the technology and identifies that how the usage of blockchain technology for identity management and intellectual property protection with machine learning and blockchain can efficiently, accurately, securely protects the business and their intellectual property.

3. Case Study -Traditional Framework for Businesses in Pakistan

3.1 Overview of Case Study

In this chapter, Pakistan's regulatory framework has been studied thoroughly to identify the working of all the interlinked organizations to register, manage, maintain, and secure multiple businesses. SECP, IPO and FRB are the main bodies entitled in business related processes. Multiple challenges and threats have been identified to model the business needs of research.

3.2 Intellectual Property Organization

A government organization called the Intellectual Property Organization of Pakistan (IPO-Pakistan) was created in accordance with the Intellectual Property Organization of Pakistan Act, 2012, and is responsible for managing and defending the nation's different intellectual property rights. It is associated with the World Intellectual Property Organization, a well-known organization that promotes and defends intellectual property (IP) rights on a worldwide level [18]. This involves overseeing the issuance of patents, industrial designs, trademarks, copyrights, and geographic indications, as well as their protection. In order to further preserve intellectual property, IPO-Pakistan protects these rights via legal action against violations, public education initiatives, and participation in international partnerships. By effectively protecting intellectual property rights while balancing artists' rights and social interests, its primary goal is to promote innovation, creativity, and financial stability. Despite being acquainted with the term "intellectual property," most people have no idea what intellectual assets are. People are ignorant of the significance of protecting intellectual property rights and the damaging effects that piracy and illegal trade have on the economy. It is crucial that the general public understands the importance of IP rights [20].

The International Intellectual Property (IIP) study provides light on the persistent challenges faced by publishers in Pakistan in their battle against widespread piracy, which is further compounded by the government's limited capacity to implement rigorous measures. Despite the implementation of recent revisions to intellectual property rights (IPR) laws in order to conform to international norms, the issue of piracy persists and continues to inflict substantial economic harm. The presence of legal loopholes, the slow pace of implementation,

the leniency of punishments, and the protracted nature of the court procedure all contribute to the issue at hand. According to the second source [19], the paper proposes the establishment of collaborative partnerships with international organizations and the use of diplomatic pressure from the United States, primarily via the implementation of agreements, to enhance the efficacy of intellectual property rights (IPR) protection. Nevertheless, given the substantial population, fragile economy, and prevailing issues related to fundamental requirements in Pakistan, it is uncertain whether immediate economic gain can be achieved by the implementation of intellectual property rights (IPR). Enhancing intellectual property rights (IPR) systems has the potential to result in increased prices and diminished employment prospects. Although the current legislative framework demonstrates proficiency, it is essential to prioritize the proper execution and enhancement of the judicial process. The key criteria for development are the implementation of autonomous IP dispute resolution courts, the enhancement of arbitration mechanisms, and the reduction of cost.

3.3 Securities and Exchange Commission of Pakistan

In the academic context, SECP stands for Securities and Exchange Commission of Pakistan. It is the regulatory organization in charge of observing and regulating Pakistan's corporate sector, non-banking financial institutions, and securities market [4]. The main goals of the SECP are to guarantee openness, investor protection, and the stability of the nation's financial system. Systems are in place at the SECP in Pakistan to look for suspected copyright violations or duplication throughout the registration process [5].

Business Registration process by SECP:

The conventional procedure in Pakistan is to complete the following steps [3]:

- Pick a company name and request SECP approval for it.
- Create the necessary paperwork, such as the articles of incorporation and the memorandum.
- Obtain the directors of the company's digital signatures.
- Send the registration application and all required paperwork to the SECP.
- Pay the enrolment fee.
- If your application is accepted, you will be given a Certificate of Incorporation, which will formally establish your company.

Drawbacks of SECP

They have systems in place to confirm the uniqueness of company names, trademarks, and other forms of intellectual property. However, if the copying is subtle or the SECP's resources are constrained, it may be difficult to accurately identify all instances of copying. Businesses must take aggressive steps to safeguard their intellectual property rights and seek legal counsel if they believe there has been any infringement.

1. **Limited resources:** The SECP might not have enough money to thoroughly examine each registration for possible plagiarism or infringement. Because of this, some situations might fall between the cracks.
2. **Subjectivity**: Deciding if something is a straight copy or an infringement can occasionally be a matter of opinion. It might necessitate a thorough analysis of the parallels and divergences, which can be difficult for the SECP.
3. **Time restraints:** The registration procedure itself might be subject to time restraints, and the SECP might not have the time to fully investigate each application.
4. **Legal complexities:** The SECP may find it difficult to keep up with all the nuances and changes in copyright and intellectual property laws given their complexity.
5. **False positives or false negatives:** The automated system may occasionally fail to detect copyright infringement or copying, which can result in either false positives (flagging genuine registrations as violating the law) or false negatives (missing actual cases of infringement).
6. **Limited scope:** If the infringements include complicated or nuanced circumstances, the automated system may not be able to detect them.
7. **Absence of human judgement:** It may be difficult to appropriately assess some cases using automated systems since they lack the same level of discernment and judgement as human experts.
8. **Changing strategies:** Copying and infringing tactics might change over time, and an automated system may find it difficult to keep up with any modifications or new techniques.

Businesses should be aware of these restrictions and take extra precautions to protect their intellectual property rights, including seeking legal counsel and doing exhaustive trademark searches and consulting a lawyer to guarantee that their rights are properly protected.

Internal Threats

Internal threats are security hazards that arise from within an organization while utilizing SECP. These dangers may come from:

1. Insider Attacks: SECP implements stringent access restrictions, monitoring, and auditing to detect and prevent insider attacks. It assists in identifying and mitigating the risk of hostile acts by workers or privileged users.

2. Data Leakage: SECP assesses the safeguards in place to stop insiders from disclosing sensitive information without authorization. It makes sure that encryption is used to prevent data leaking and data loss prevention techniques are put in place.

3. Abuse of Privileges: SECP helps reduce the likelihood that employees will improperly access or alter data. It encourages the idea of least privilege by making sure users only have the access permissions they require.

Organizations can reduce these internal dangers and improve the overall security of their databases by adhering to SECP rules.

Threats to Database Security

The following dangers can arise from using the SECP database security:

1. Unauthorized access: There is a chance that unauthorized people will access the SECP's database, which could result in the misuse or theft of private data.
1. 4. Data loss: The SECP's database may experience data loss due to technical issues, software bugs, or natural disasters, which could result in disruptions and the loss of important information.
2. SQL Injection Attacks: The SECP program assists in locating and minimizing vulnerabilities that can be used in SQL injection attacks. To avoid injection attacks, it encourages parameterized queries and secure coding techniques.
3. Insider Threats: The SECP evaluates the safeguards put in place to identify and stop insider threats. It places a focus on the use of monitoring and role-based access controls.

Overall, SECP offers a thorough framework to counteract these risks and strengthen database security. The SECP should put in place strong security measures, like encryption, firewalls, frequent security audits, and employee training, to reduce these risks. Additionally, to lessen

the effects of data loss or system failures, they should have backup and disaster recovery procedures in place.

3.4 Federal Board of Revenue

In Pakistan, the Federal Board of Revenue (FBR) is the official tax organization in responsibility of collecting federal taxes and levies [6]. The act of dodging taxes and exploiting legal loopholes may be utilized to escape one's rightful tax duties, culminating in the exploitation of the tax system. Prominent individuals and corporations frequently use their considerable resources and influence to avoid tax obligations through methods such as deliberate understatement of income, advocating for favorable tax legislation, using offshore accounts, or employing intricate financial maneuvers such as transfer pricing. The aforementioned activities have a negative influence on the fairness and efficiency of the tax system, necessitating legislative reforms, stronger enforcement measures, international collaboration, and public awareness to successfully address these issues and ensure fair tax collection.

The reduction of tax fraud and exploitation performed by resourceful corrupt individuals within the FBR organization needs the execution of comprehensive reforms aiming at addressing existing legislative loopholes, strengthening enforcement measures, and cultivating an open culture. Multinational cooperation is required to properly handle the problem of cross-border tax evasion. Furthermore, public awareness and pressure may serve as accelerators for establishing fair tax practices and ensuring that notable businesses are held accountable for meeting their tax duties.

On average, the Federal Board of Revenue (FBR) system experiences more than 71,000 cyberattacks per month. According to the FBR's assessment on the Pakistan Raises Revenue Project (PRRP), continuous hacker efforts to initiate cyberattacks have also presented a severe danger of data theft in recent years [7].

3.5 Summary of case Study

The case study examines Pakistan's traditional system, including the IPO, SECP, and FBR. IPO protects intellectual property rights against piracy via international cooperation with WIPO. A major challenge of IPO states that traditional approach for matching IP with existing IP is using keywords and self-examination into database that does not produce proper results. SECP regulates corporate sectors and securities markets, company registration, and internal

dangers via access restrictions and surveillance. Threats to SECP are database breaches and data loss. FBR fights cyberattacks and tax evasion via reforms, enforcement, and international partnership. This report details Pakistan's commercial environment, regulatory complexities, and difficulties and solutions.

4. Methodology and Framework

4.1 Overview of Framework

Currently, businesses and intellectual property have involved blockchain in their design and development process, but the adoption of this technology is greatly influenced by the security, efficiency, scalability, performance and usability. This architecture is proposed for government of Pakistan for business management and protection while Businesses can maintain their portfolio, trade with other business and users, perform analytics on their data and protect their intellectual properties. The Blockchain Business Digital identity is a meticulously planned architectural design that deploys software engineering principles [14] together with deep neural network and blockchain technology. This framework aims to provide a decentralized and secure digital identity to all the business while the governing bodies of Pakistan can effectively play their roles in business registration, taxation, intellectual property rights reservation. Moreover, it defines the workflows of the proposed framework according to the regulatory requirements of Pakistan.

4.2 Proposed Architecture

The model is based on the Hyper Ledger fabric consortium blockchain technology to enable semi decentralization and control over the participant of the network who performs specific roles and responsibilities. In this model IDPC, SECP, IPO, FBR, Businesses and Users are the actors of the network. Let us decompose the high-level architecture into its components for better understanding.

Front-end:

Actors can interact with the system via a front-end browser where they can perform their certain actions and upload their data or documents to make any transaction.

Wallet:

Each actor has a unique identity on the blockchain system which comprises of the public and private keys. The public is the address to receive any transaction while private key is necessarily required to make any transaction in the network. These keys are stored on the wallet and is protected an owned by every member of the network.

Edge Services:

Components that provide services and deliver multiple functionalities to the members of the network by connecting them to the application backend. Edge services provide faster and secure data transmissions between the user interface and the back-end application. Data, information, and documents are being exchanged via HTTP/REST protocols.

Message Bus:

Since we have proposed a service-oriented system, asynchronous communication protocol is used via a message bus that improves efficiency and flexibility. It provides smooth communication between the blockchain layer, backend application logic, and external systems by decoupling components. The message bus publishes events triggered by critical system processes such as identity issuance and patent matching, allowing backend event listeners to reply asynchronously.

Event Listener:

Event listener acts as a cornerstone for effective communication and coordination among the blockchain layer and backend logic. Event listener manages subscriptions so whenever an event occurs in the system the event listener listens to it and broadcasts it to the backend via a message bus and acts according to the predefined actions such as notifying stakeholders, triggering processes and updating data [8]. Event listeners use “polling” to periodically check the updates event occur in the blockchain network and push them to services.

For example, when a business is registered and its identity is created on the blockchain the event listener automatically captures the event and in response to the event it updates the identity verification status on the backend, notifies other member of the network and triggers the machine learning algorithms to match the existing models n intellectual property.

Off-chain Data Storage and Encryption:

To facilitate the efficiency, scalability and privacy of the system sensitive and large data is kept off-chain that holds data related to blockchain. The data is hashed via SHA-256 algorithm which is used as an input to encrypt/decrypt data through AES encryption algorithm. This encrypted data is stored off-chain. The data is updated according to the blockchain events and business logic respectively. The hash of the data is stored on the blockchain to access it for multiple purposes.

Multiple off-chain repositories are created off-chain to store User profiles, business profiles, credentials, accounts, identity verification documents, Patents, transaction history, large media files and external system data from SECP, IPO and FBR.

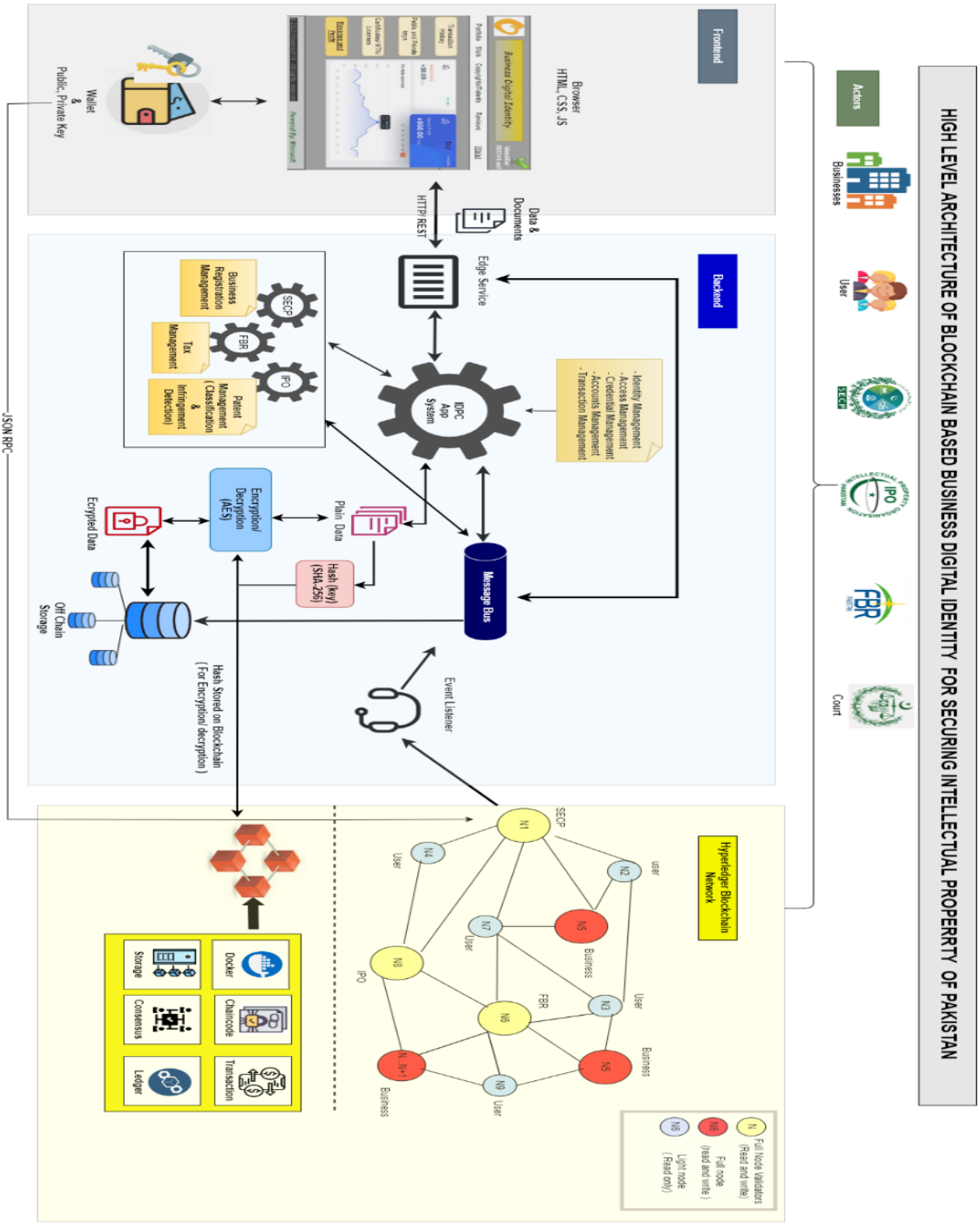


Figure 4. 1 High level Architecture of Blockchain Business Digital Identity System

Backend Application Logic:

The backend application can be termed as the brain of the system to achieve business objectives. Each application logic is based on the functionalities each actor can perform. In the proposed architecture we have one major application system for IDPC and 3 subsystems for SECP, FBR and IPO which are integrated with the main application system of IDPC. Since, the proposed architecture is based on blockchain, so application logic decides which data and computations are kept on-chain or off-chain respectively considering the scalability, traceability, and security of the system.

A. **IDPC Application System logic**: The IDPC holds the logic of the application which is responsible for the following management.
   - **Identity Management**: The data of the User/Business is processed and upon verification by the peer nodes (SECP/FBR/IPO) an identifier is granted to each Business/user. This makes use of public and private key pairs that uniquely identifies them. A profile is created where they can manage and maintain their business. Identity registration, verification, revocation is done here.
   - Access Management: Chaincodes are written against each identity where pre-defined set of rules defines the self-sovereignty of a User/Business over their identity on the network [17]. This restricts and controls users to access only authorized data and functions. Here, Users can only view other Business profiles while businesses can view other business too and manage their profile and portfolio. FBR can view the Business profile and has access to their total revenue and profit to calculate their taxes. SECP can access a business NTN number and check their details while IPO can have access to a Business intellectual Property to protect it from infringement.
   - **Credentials Management**: Credentials are created based on the identities created.
   - **Accounts Management:** All the financial statements of businesses/Users are managed and processed here.
   - **Transactions Management:** All the blockchain transactions which are signed by the public and private keys are managed. This holds the logic of how transactions is made and broadcasted to the network to update.

B. **SECP Application System logic:** The SECP application hold the logic of Business registration management.
C. **FBR Application System logic:** FBR application holds the logic for Tax management of the businesses where the total tax is against each business is calculated and collected.
D. **IPO Application System logic:** IPO application holds the logic of verifying any new business models by matching it with already existing business models and their intellectual property using machine learning and deep learning techniques.

Blockchain Network:

The nodes are connected to each other in a decentralized blockchain network. The nodes in yellow are the government authorized bodies known as full who can validate other nodes. They have read and write access to blockchain. The nodes in red are the business who gets a digital identity on the blockchain they can read and write on blockchain while the nodes in light blue are the read only User known as light nodes.

All the nodes have real-time software running on their devices known as Docker to connect with the blockchain network. Chain codes are written and, in this software, so whenever a node makes a transaction in the network a chain code written against it triggered. A consensus mechanism is done by the nodes so once a transaction is verified, a block is appended to the blockchain, and all the nodes ledger is updated.

4.3 Transaction Mechanism

A transaction occurs when the business request is catered by any entity/organization. For instance, if a business request for business digital identity, then the IDPC after verification sends the Identifier as an output. This transaction is signed by the IDPC private showing that it is made by an authenticated node. The transaction is broadcasted to the blockchain network where it is mined by the peer nodes using endorsement policy in hyper ledger fabric blockchain. It uses BZFT consensus algorithm to approve the transaction. The transactional data is only decrypted by the receiver's public key such that only authorized node can access it. So the receiver's wallet contains the data they requested. This transaction is stored on the blockchain, and ledger is maintained by all the nodes.

Here. It is noted that Business wallet contain all the important transactions and required data and documents in a secure and decentralized manner.

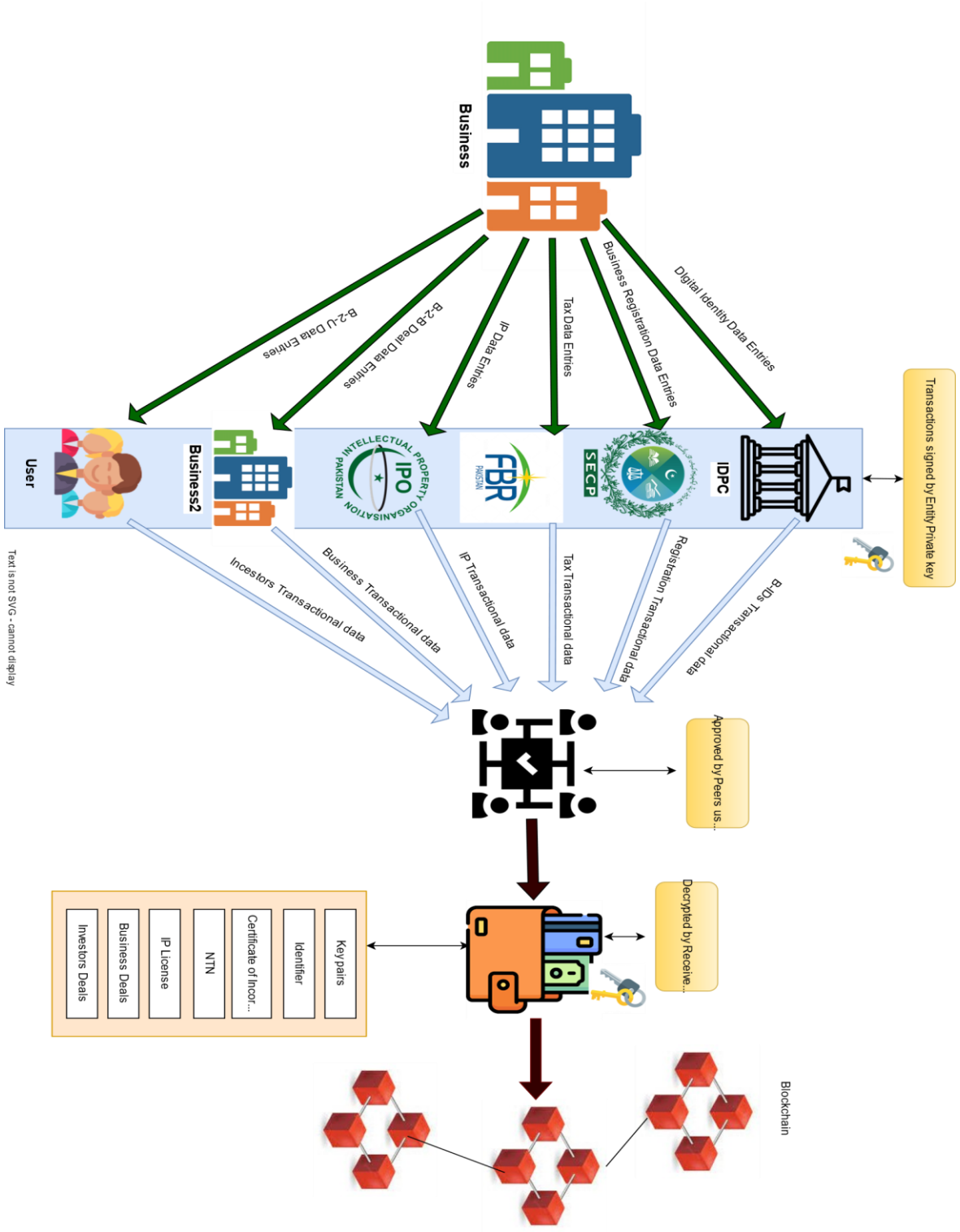


Figure 4. 2 Transaction Mechanism

4.4 Workflows of Proposed Model

The proposed model is split into different modules to cover all the aspects and its applications.

4.4.1 User Registration Module

The users can join the blockchain business identity network by signing up the at the IDPC portal where they can insert their data. IDPC verifies their data and creates a key pair of public and private keys used to make and receive transactions. IDPC creates user profile and wallet. The keys are encrypted in wallet and the user identifier and public address is added to the blockchain network and their data is stored off-chain. IDPC creates user credentials and return user their credentials, public and encrypted private keys and an identifier.

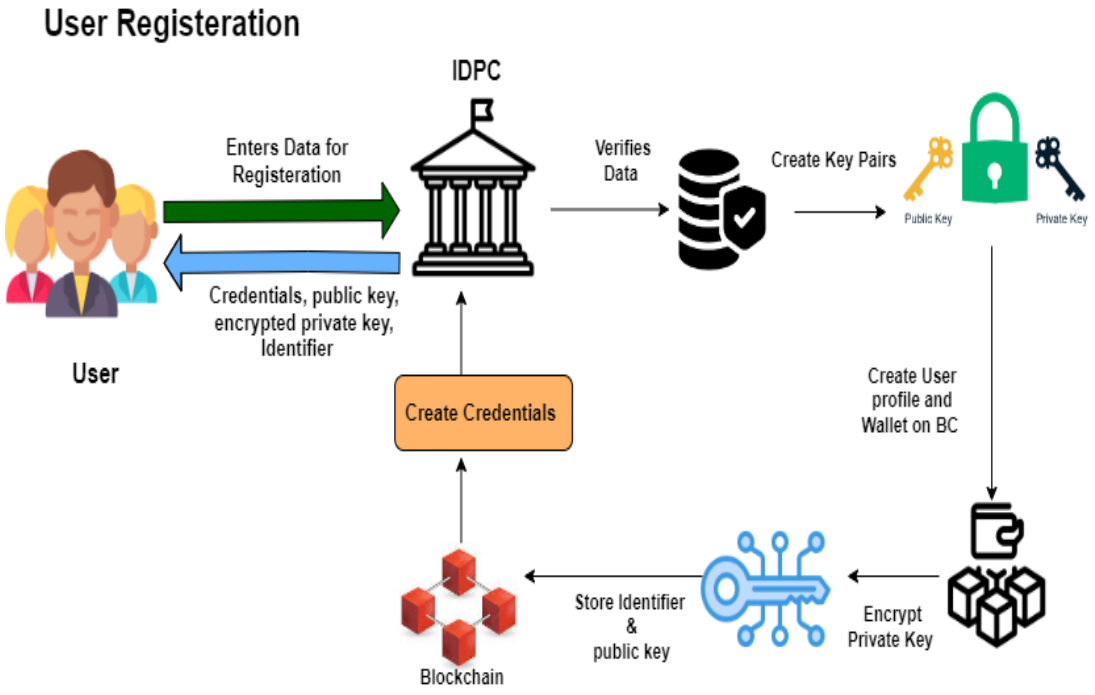


Figure 4. 3 User Registration

4.4.2 Buy Cryptocurrency Module

A user registered on the blockchain business digital identity system can buy digital currency in through IDPC. IDPC authenticate user by checking their credentials and identity in the system. The user makes their PKR payment which is authenticated by the bank. IDPC then make crypto payment and generate a transaction by signing it with their private key and user public address. This transaction creates a block which is mined and validated by the peer using endorsement policy. The block is appended to the blockchain. Even listener listens to this event and the message to is broadcasted to via message bus and the account repository is updated accordingly. Hence, the cryptocurrency is credited to the user's wallet.

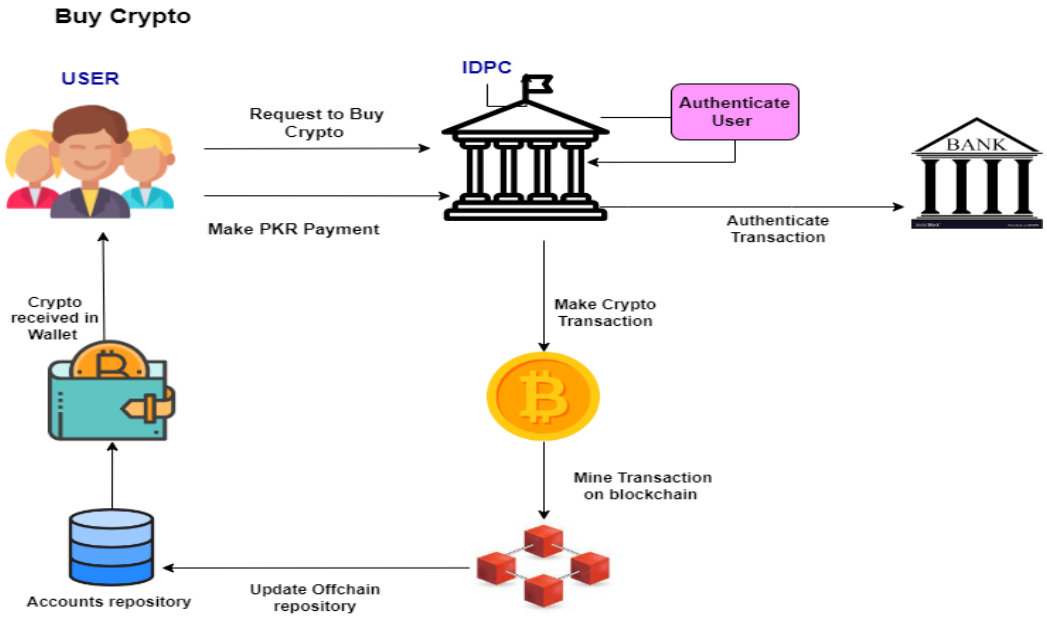


Figure 4. 4 Buy Cryptocurrency

4.4.3 Business Registration Module

A user can register their Business in the Blockchain Business Digital Identity System. The business request for their business registration by inserting their data and uploading their documents on the IDPC portal. The IDPC forwards the request to integrated SECP application logic where SECP checks the validity of the user and matches the business name in with already existing business name in their off-chain repositories. Invalid results request for new business name otherwise the business registration is rejected. Upon valid results SECP requires the

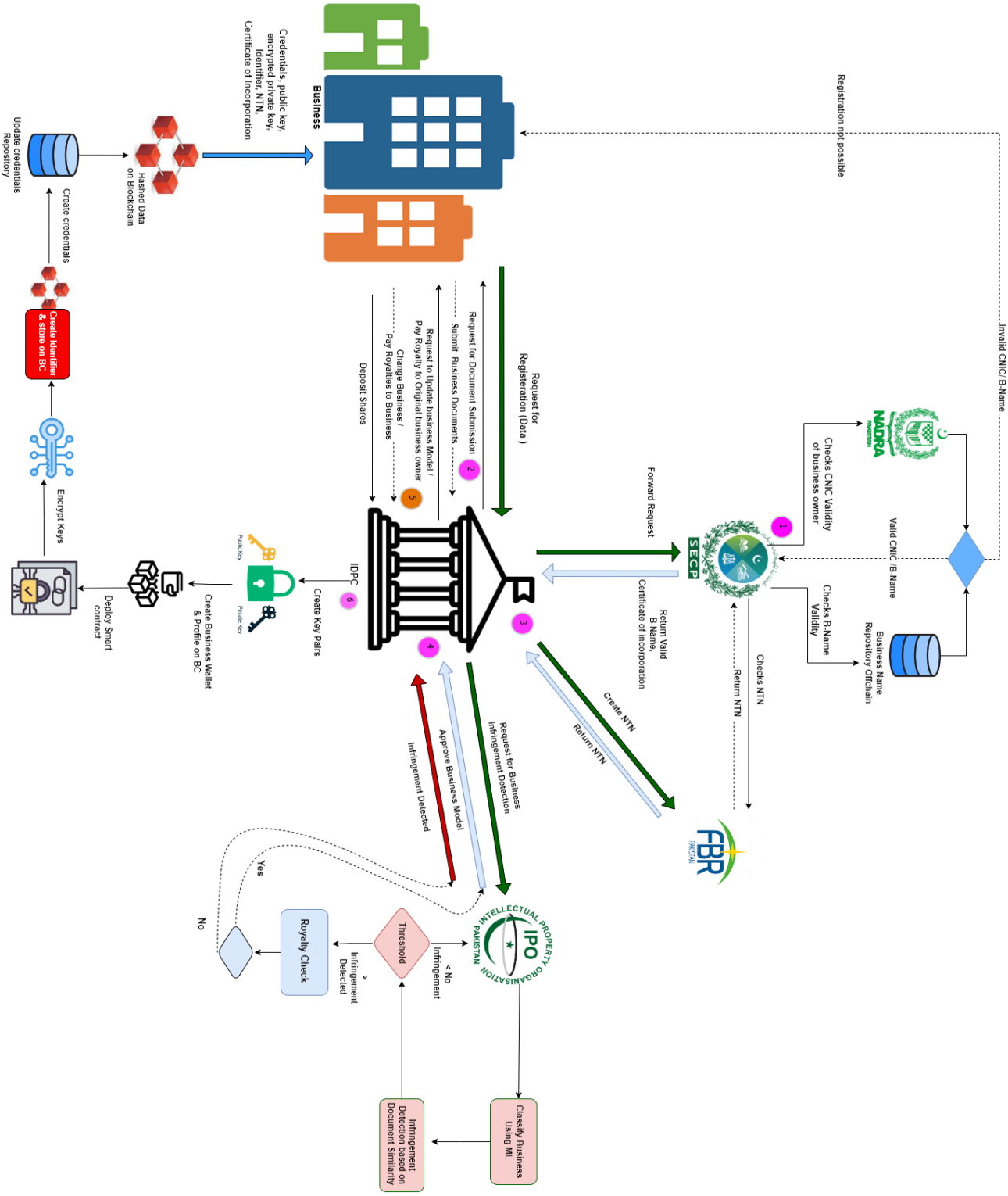


Figure 4. 5 Business Registration

SECP requires the submission of company incorporation documents along with their business model. SECP check with FBR if the NTN number is already generated against that business required to register a business otherwise business can request for the creation of NTN through the IDPC portal and FBR creates the NTN number which is signed by the FBR's private key and Business public key address. This transaction is broadcasted to the blockchain network which is captured by event listener, so the system is updated via message bus. On approval the SECP generates a verified business name and certificate of Incorporation to IDPC against the business registration request.

Now IDPC generates a request to IPO for business infringement detection where a business model and their intellectual property is matched with claims and prior art. IPO uses machine learning for business classification and deep neural network BERT to detect the matching with claims and prior art. If the matching is less than the threshold, then the business model is approved and if it's above the threshold then IPO check if the business has given the Royalty to the intellectual property owner. If royalty credit is given, then the business model is approved by IPO and now IDPC can successfully register a business otherwise IDPC request the business to either change their business model for innovation or pay royalty credit to the original owner of the intellectual property owner. If the business fails to do so, then IDPC rejects their business registration.

Once a business is approved by all the inter-related organizations, now IDPC creates a key pair of public and private keys against the business. An authenticated business profile and its wallet is created on the blockchain. The key pairs are encrypted in the wallet and a Chaincode is deployed against the business profile which defines the access and control of the business identity. A unique business identifier is generated based on the key pairs and its credentials are also created which are used to login to the system. The credentials are stored in the off-chain storage which is hashed, and its link is stored on the blockchain.

4.4.4 Business Authentication Module

A User/ Business can authenticate any business online on the IDPC portal where they can enter a business name. IDPC back-end logic checks the existence against that name using identifier on the blockchain where IDPC gets the public key address of the business and IDPC check the revocation of the business and gets business validity results. Upon successful authentication and verification, the IDPC portal displays authenticated business profile with an identifier. Similarly, the user can also be authenticated.

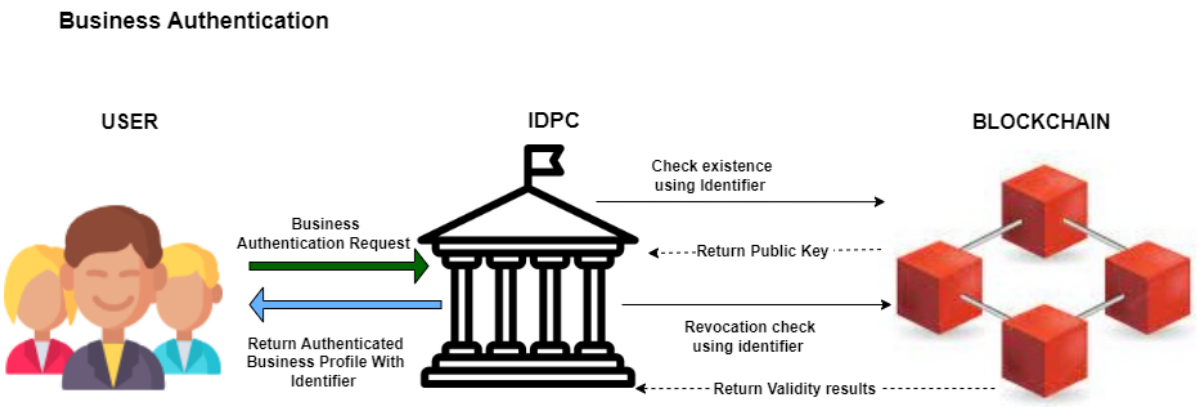


Figure 4. 6 : Business Authentication

4.4.5 Patent Registration Module

A business can register their intellectual property through IDPC portal. IDPC authenticates the business using their identifier. The user fills IPO P-27 form and pay fee in crypto and gets limited access to the off-chain prior art repository. It returns patentability report to the business that allows them to apply for patentability. Business prepare their documents and file their patents by filling P1, P2, P3 and P28 form of IPO. The patentability application is examined by IPO for intellectual property infringement detection where a business model and their intellectual property is matched with claims and prior art. IPO uses machine learning for business classification and deep neural network BERT to detect the matching with claims and prior art. If the matching is less than the threshold, then the patents are approved and if it's above the threshold then IPO checks if the business has given the Royalty to the intellectual property owner. If royalty credit is given, then the patent is approved by IPO. A chaincode is written against the patent that defines the ownership, access control of the patent, charges of patent and the duration of access to the patent if the owner wants to sell their patents. This chaincode is deployed on the blockchain. Patents are granted to the owner and broadcasted to the blockchain signed by the IPO private key and public address of the owner. Otherwise, infringement is detected so the request is generated by IDPC to prove their innovation or pay credits to the original owner else the patentability is rejected.

If the infringement is detected at later stage against any patent then the system automatically updates the IPO application and the chaincode is triggered on the blockchain which define automatic fines and penalties as per Pakistani court and laws.

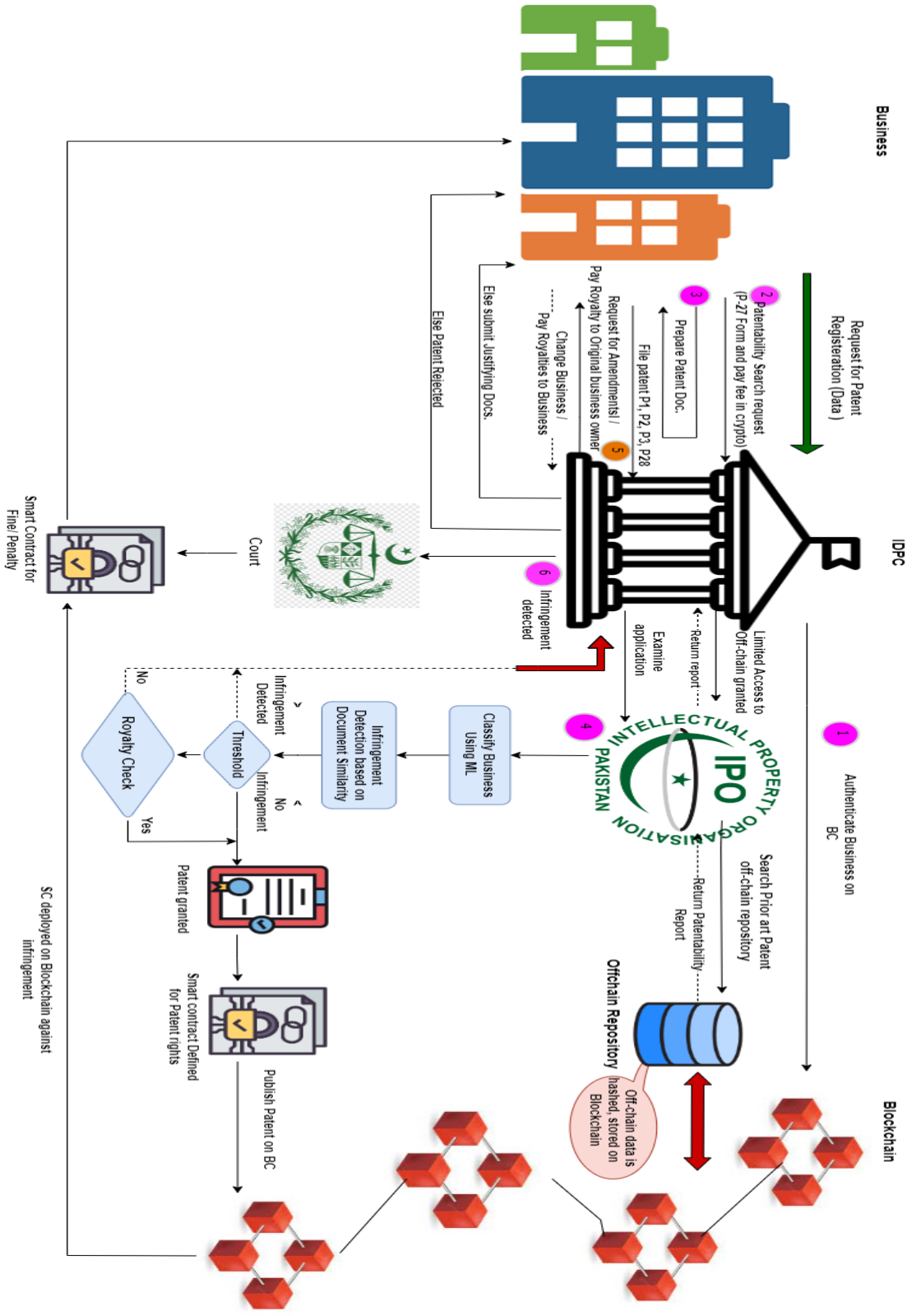


Figure 4. 7 Patent Registration

4.4.6 Buy Patent Module

Businesses can collaborate with other businesses to buy their patents rights to flourish their business through IDPC portal. IDPC authenticates a business and forwards buying requests to business2. If Business2 denies selling their patents, then rejection is sent to business1 otherwise on acceptance the chaincode is triggered on the blockchain. Business1 makes the cryptocurrency payment which is mined. This transaction is again broadcasted, and event listener updates the off-chain storage according to chaincode logic. Patent access is granted to the business1 with royalty credit.

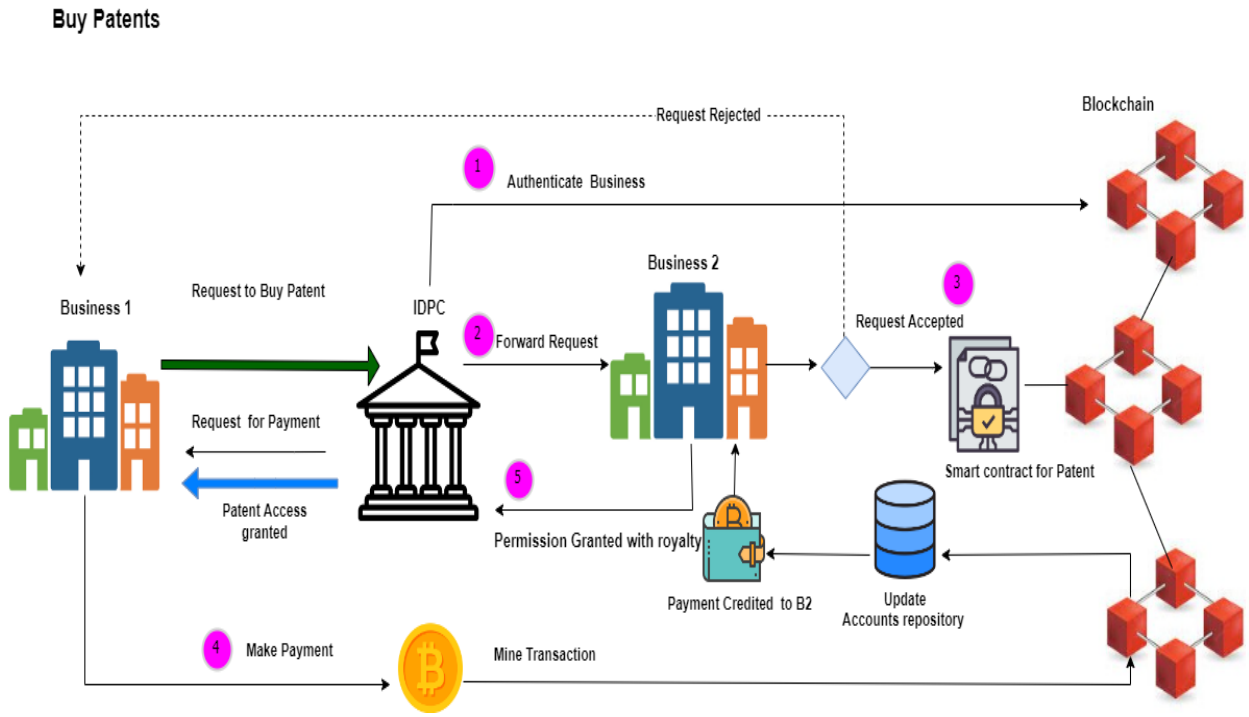


Figure 4. 8 Buy Patent

4.4.6 Tax Calculation Module

Since the business profile is created on the blockchain so the peer nodes can view or access them based upon the rights. Here, FBR can play a great role in automatic tax calculation and collection. A chaincode is written which is triggered after every fiscal year to collect taxes from the businesses. Taxes are debited in the form of cryptocurrency from business accounts and debited to the FBR accounts. This transaction is broadcasted to the blockchain network and off-chain repositories are updated accordingly.

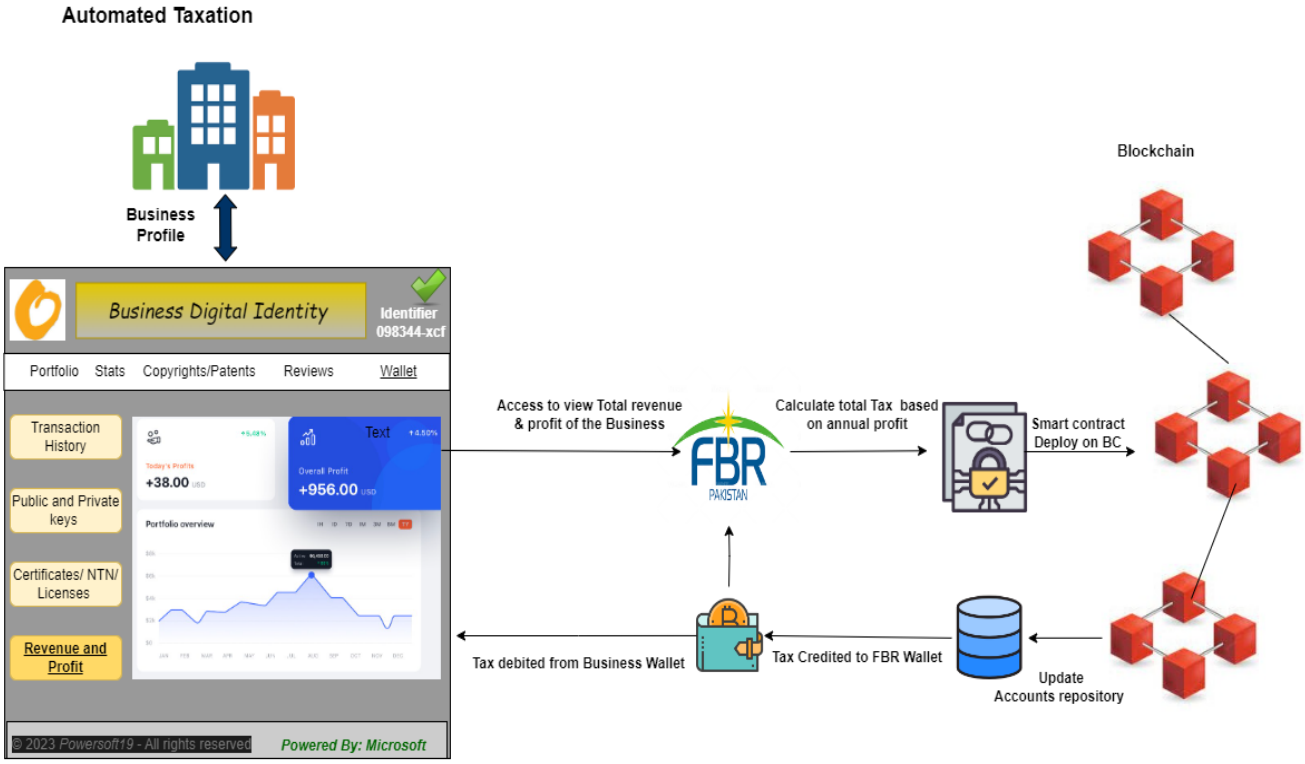


Figure 4. 9 : Automated Taxation

4.5 Summary

This chapter describes the framework for Pakistan to secure and automate their traditional methods for business related process and IPs protection using blockchain, deep learning and software engineering practices. The framework is based on event driven architecture for internal application communication and peer to peer architecture style for blockchain networks. Workflows are defined to legally automate the system according to national regulations and laws.

5. Results and Analysis

5.1 Overview

We concentrate on demonstrating the reliability of our results via meticulous data collecting, analysis, and documentation procedures in order to verify research utilizing grounded theory (GT). This makes it easier to guarantee that the theories or frameworks that are developed as a consequence are supported by the data and are appropriate for use in the context of the research.

The validation of our proposed framework is based on a questionnaire survey for the qualitative evaluation. We have conducted a comprehensive comparison of our proposed framework with the traditional framework of Pakistan to identify its loopholes and comparison with other existing blockchain types to highlights the ways how our framework excels in so many domains. The Questionnaire is attached in the Anex A as a reference.

5.2 Questionnaire Result and Analysis

5.2.1 Background and Introductory Analysis

Targeted Audience: To evaluate our proposed model, we have conducted a survey among the business owners, IT professionals and government employees from respective sectors. We received a total of 98 responses. Their valuable insights, business needs, and recommendations are considered as essential components for bolstering the legitimacy and applicability of our framework. All the targeted audience has either bachelor's or master's degree.

Business Category and their Intellectual Property: Experts own/work on diverse categories of business i.e Product based business/ Project based business/ Service based business and others. This diversity helps us to better evaluate our framework in all business dimensions.

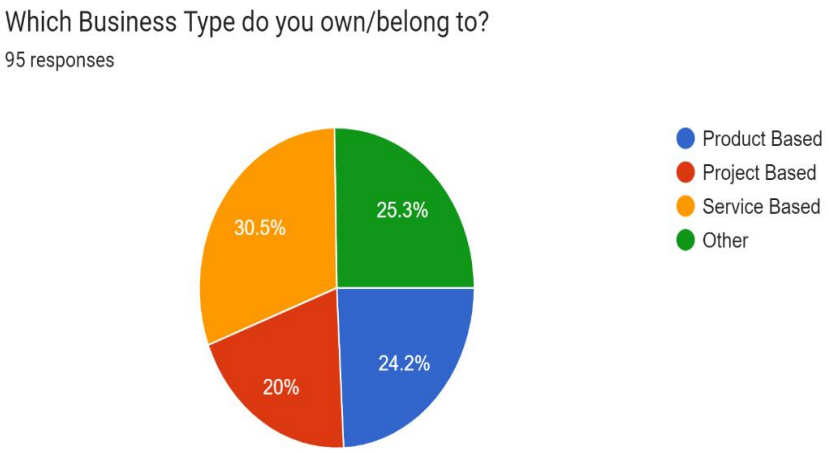


Figure 5. 1 Respondent business Type

According to the survey, 71% of the business industry has not protected their intellectual property which shows the lack of awareness of securing the intellectual property rights. This has adversely affected our business's growth in so many ways.

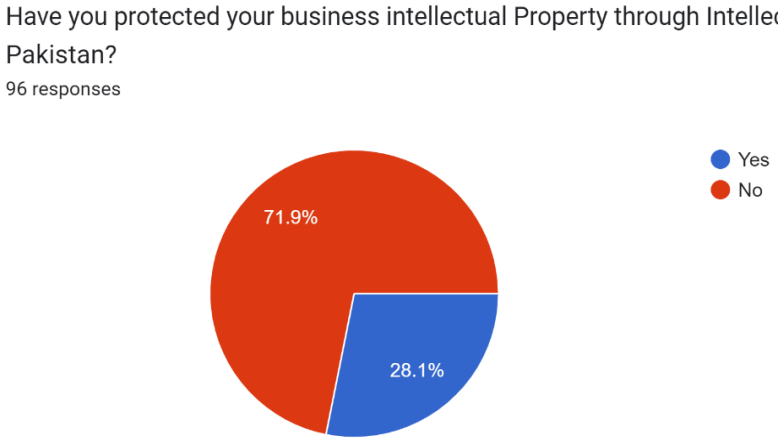


Figure 5. 2 Respondent IP protection

5.1.2 Challenges and Loopholes in Traditional Framework

Registering a business is not as easy as it seems to be. People face a lot of problems to register their business and intellectual property due to complex regulatory systems where they have to visit multiple times to get their registration which is one of the causes of the delays in processes and corruption occurs due to the involvement of dishonest people in this process. People have no transparency in their registration and documentation and their data can be breached. Moreover, business gets registered without any validation of business model and their intellectual property rights with already existing business which adversely affects them. There are many other challenges that people suffer in our traditional systems.

Figure 5. 3 Challenges for business/ IP Registration

70% of the expert pay their business taxes while 82% are not satisfied with the current tax management system of Pakistan. The point to ponder her is that the remaining 30% do not pay their taxes due to any means. One of the reasons is that business takes advantages from internal resources with their references or corruptions to cut down their business taxes and save their profit. 82% of the people are not satisfied with the existing poor taxation system of Pakistan because even if they pay taxes, it is believed that their taxes are not utilized well.

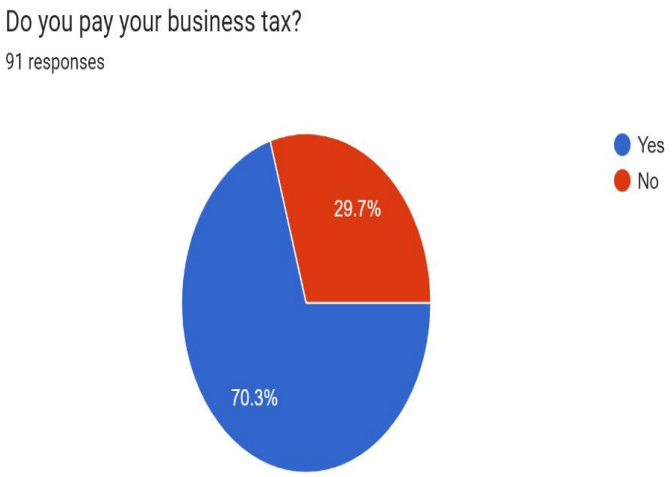


Figure 5. 4 Business Tax

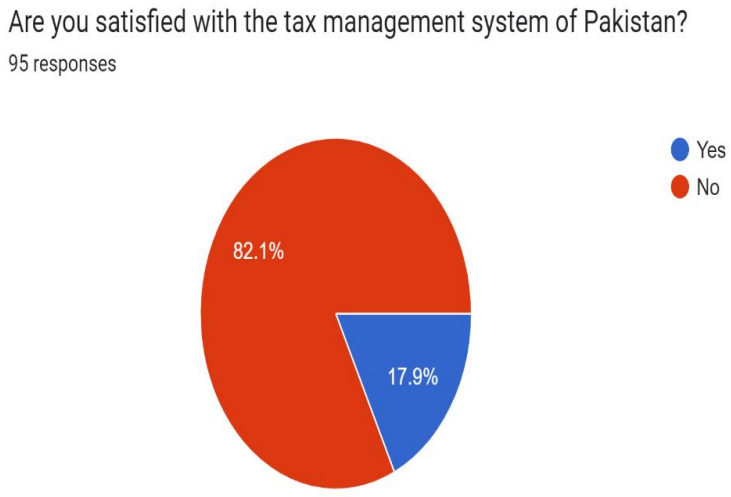


Figure 5. 5 Tax management satisfaction of respondents

Businesses normally don't register their intellectual property and even if they do they believe that it is still not secure because a lot of pirated products and services are available in the local market. There is no proper or automated system that automatically detects their infringements, so the Intellectual Property owner has to identify their claims by themselves and submit their

conflicts in case of any infringements to get it countered. Accordingly, to our survey 42% are neutral because they haven't bothered to protect their IP while 39% are collectively dissatisfied even after securing their IPs. While a small percentage of are satisfied with the protection of IPs in Pakistan.

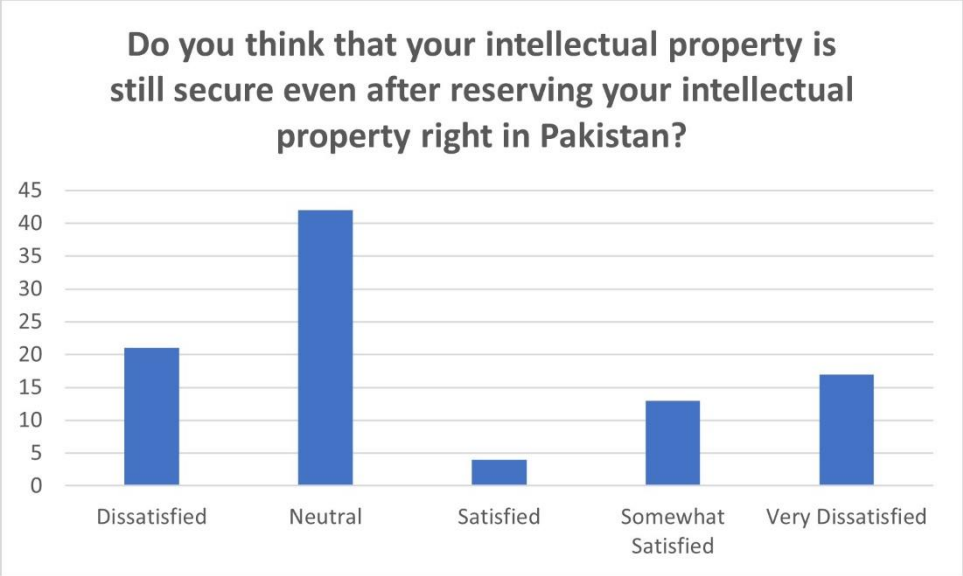


Figure 5. 6 IP Protection after Rights Reserved

5.1.3 Evaluation of the Proposed Framework

Blockchain Business Ecosystem: Blockchain provide a secure network for the businesses, investors, and government bodies to switch to a secure digital platform to engage with each other by preserving their identity, data, documents, and assets in a tamperproof hash-based system. 80% of the people believe to be a part of this network. Their business digital identity will promote business authenticity, secure and transparent trading, accountability in their total revenue and profits, fast and effective business-related processes. Authentication of the business registered by the government will increase trust and confidence in the investor before making any business deal or investing in any business. The digitalization by means of blockchain will also enhance collaboration among the interlinked departments (SECP, IPO and FBR) to expedite the business process.

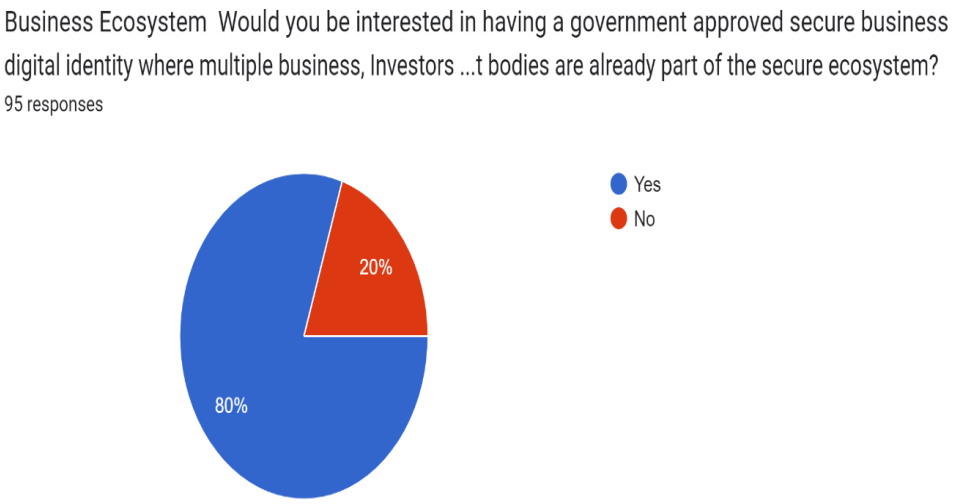


Figure 5. 7 Business Digital ecosystem

82% of the people believe that having a digital wallet linked to each business identity will store all the government related transactions and business transactions and map them onto the blockchain such that their data is unaltered by every means and protected from breaches. Moreover, all the transaction history will be maintained. Similarly, for government bodies like SECP, FBR and IPO can maintain their certifying transactional history in a decentralized manner.

Business Data Storage:

21% of the respondents feel uncomfortable about sharing their business data. 48.4% respondents feel neutral while only 24.2 % of people are moderately comfortable and 6.3% are comfortable.

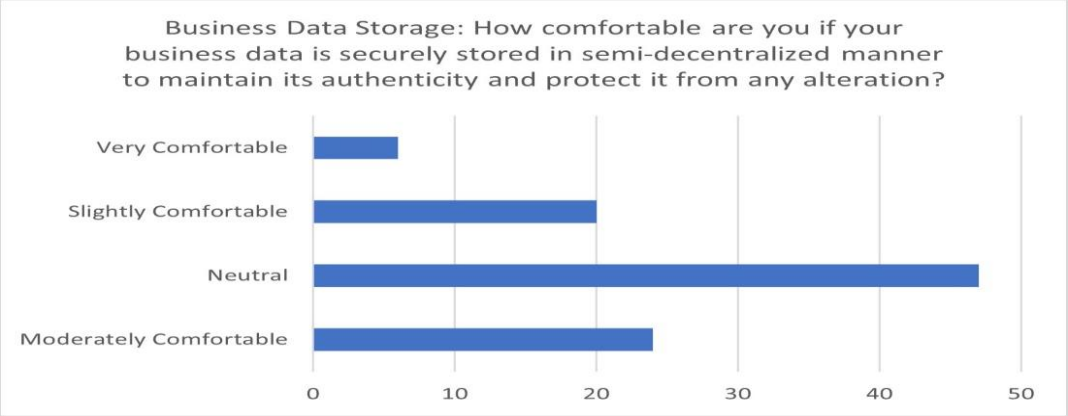


Figure 5. 8 Data storage

This view shows that businesses don't prefer to share their essential data due to data breaches. Data storage is critical to the business because attacks on the data may result in huge loss, so business prefer to store their data in-house. So our proposed framework uses blockchain decentralization nature and encourages business as well as government organization to process their data using hashing algorithm (SHA-256) and Asymmetric encryption algorithms to store it off-chain which link is stored on the blockchain. Moreover, the chaincodes written in hyper ledger fabric blockchain for access management restricts the unauthorized access to data and maintains data consistency.

Business Taxation:

As proposed in our blockchain business digital ecosystem, the FBR can directly view a business revenue and profit as per access management chaincodes so the automated taxation will cut off the intermediaries, reduces corruption and complex system challenges. Collectively 51% of respondents agree that the increased collaboration in blockchain business digital ecosystem will help foster economic growth because business taxes will automatically reach the desired department account. 29% are neutral to the increase in economic growth while 12% disagree.

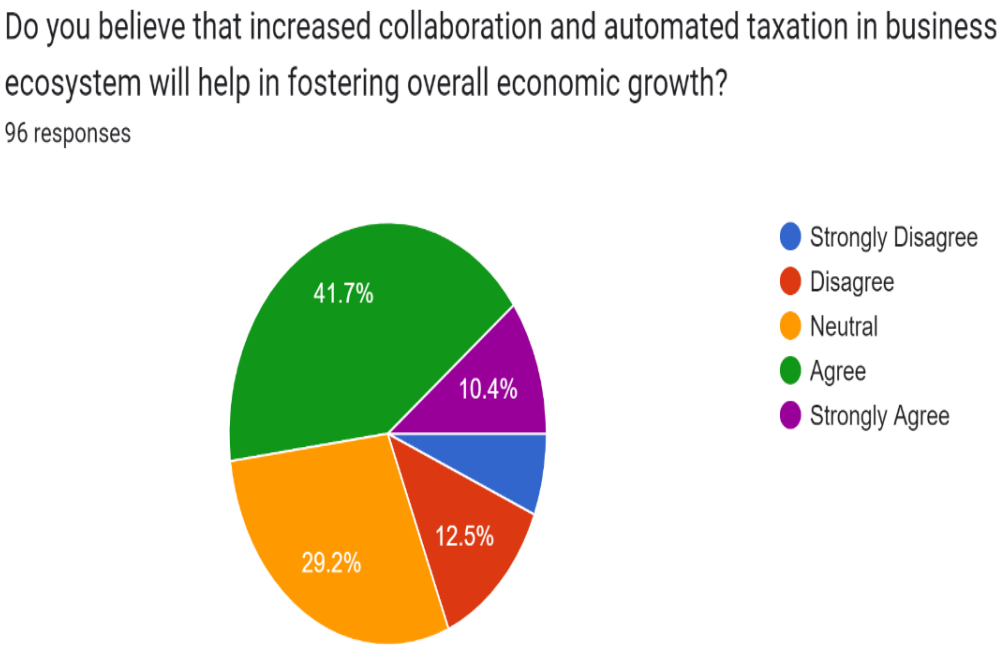


Figure 5. 9 Business Auto Taxation

Intellectual Property Protection:

Collectively 50% of the respondents believe that instead of using traditional techniques for patent registration and protection, the use of machine learning/AI would better protect them. Our proposed framework suggests the use of Natural language processing for document classification and document similarity for infringement detection that matches the patent with prior published patents. These techniques increase the efficiency of patent protection. 37% respondents are neutral about the adoption of these techniques. Since blockchain binds the data

with its header so the IP data and its ownership of IP is protected and broadcasted to the whole ecosystem.

.

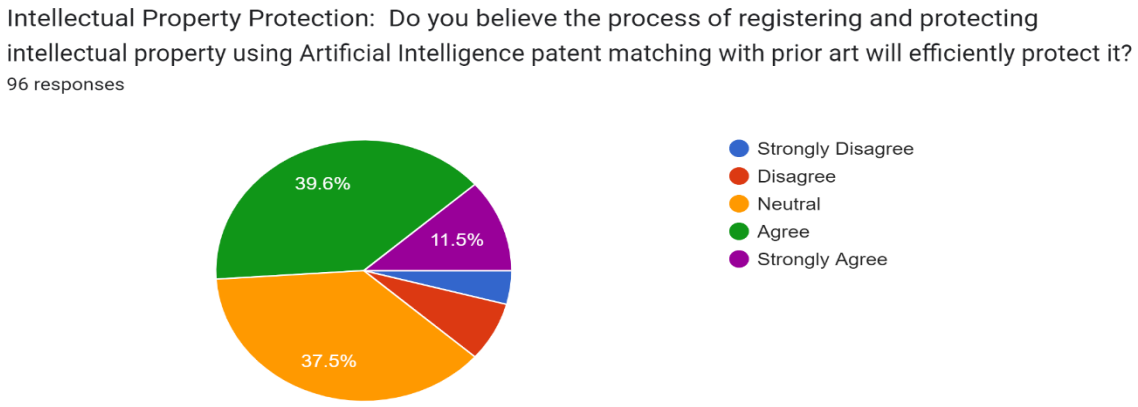


Figure 5. 10 IP protection using ML /AI

The automated selling of patents allows owners to get royalty credit of their innovations so thorough our proposed framework patent owners can securely share their innovations binned with their ownership in a secure and transparent way. According to our survey, 36% or respondents are moderately comfortable in automating their patent selling and receiving rewards through our proposed system while 16% are quite comfortable and 41% of respondents are neutral.

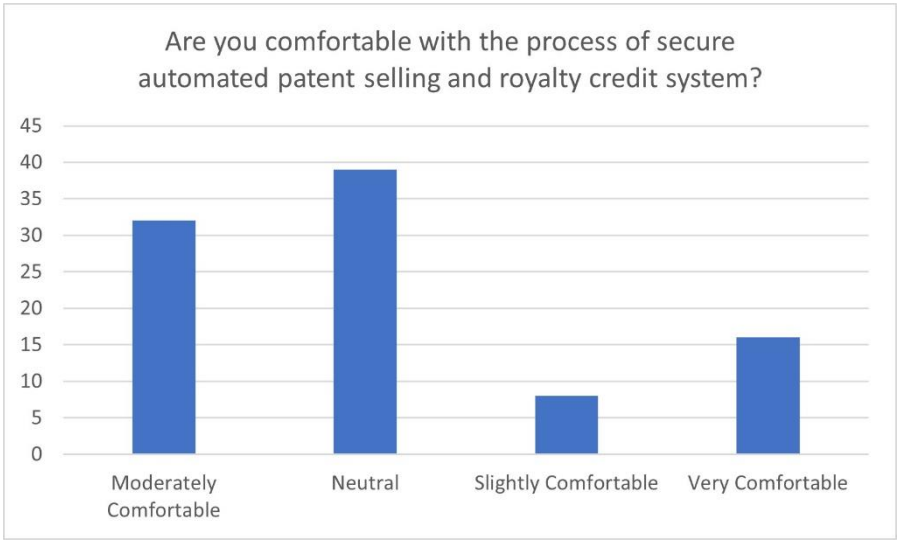


Figure 5. 11 Patent Selling and Royalty

5.3 Grounded Theory Results and Analysis

The table below shows the comparison among regulatory frameworks and other types of blockchain and our proposed architecture with the features needed by the system and justify by analyzing how our framework supports them.

Table 2 Analysis of framework based on features needed

Sr.	Features	Traditional Methods	Public Blockchain	Consortium Blockchain	Consortium Blockchain with Event Driven Architecture (Chosen)	Analysis of our Proposed framework for Pakistan
1.	Immutability	Low	Very High	High	High	The data/information written on the blockchain can't be changed or altered so business/IPs/ govt. bodies data is secured
2.	Transparency	Low – only within organization	Very High for all the nodes	High – depends on system	Medium to High – restricted to authorized nodes	Only govt. bodies will have complete transparency of the system depending on their access rights, so all the transactions are secured from any external access.
3.	Identity	High- anyone can join business but known to limited people	Very High – anyone can join the network	High – Validated nodes can join the network	High – Validated nodes can join the network	Business can only get identity if approved by the Validators only then business identity is visible with identifier to all the nodes in the network so they can be authenticated. It helps in making

						reliable and faster decisions.
4	Historical Records	Kept in databases – prone to threats	Kept on Blockchain - Publicly decentralized	Kept on Blockchain – trusted participant maintain data but data interruption if coordination breaks down over time.	Kept on Blockchain& Off-chain - trusted participant maintains data and Event listener maintains coordination over time.	The historical records of govt. bodies, businesses and IPs are persistent and continuously maintain security and privacy.
5	Ecosystem	Single company System	Totally Achieved	Easily Achieved	Easily achieved with increased interoperability & collaboration.	Increased exchange of information among users, investors, business, and govt. bodies. Interoperability and collaboration enhance trust, efficiency, and transparency.
6	Efficiency	Too low	No. of transaction per second are quite low	No. of transactions can be high	No. of transactions are high by using BZFT consensus mechanism	Reliable and swift processing of transactions enhances efficiency for rapid and effective transactions for seamless business operations and IP management.
7	Privacy	High	Very low chaincodes allow actions for specific address sending the transaction	High – ensured at various levels	High – ensured at various levels	Chaincodes maintains strict control over blockchain access and various levels that accommodates data privacy and access requirements within regulatory framework and business ecosystem. IPs are protected by owners through chaincodes written once they get their

						patents into the blockchain network
8.	Scalability	N/A	Poor scalability if nodes increase	High – by deploying more blockchains on the same node or by integrating off-chain storage	High – by deploying more blockchains on the same node or by integrating off-chain storage while event listener continuously updates them.	Off-chain and blockchain collectively handles the scalability of expanded business activities, IPs management, transactions volumes to maintain responsiveness.
9	Cost	N/A	High	Typically Low	Typically low	Since it is consortium blockchain so the cost to add a business and IP patent is quite low whereas if the business and their IPs remains unprotected it will make a huge loss to the businesses and Pakistan's Economy.
10.	Security	Low	Low – openness and decentralization introduce vulnerabilities	High	High	The confidentiality is achieved by encryption mechanism on off-chain storage. Data is always Availability on blockchain to the authorized nodes. Integrity of data is maintained by hashing the data and linking each block to the blockchain.

5.4 Summary

This chapter summarizes the results and analysis of the proposed framework. A questionnaire and grounded theory were designed to support our study. The grounded theory explains the need of proposed framework in the context of Pakistan businesses. The survey

study took reviews from stake holders who belong to business, IT, security, and economic domain. Survey provides the facts that most of the businesses face challenges during the registration till IP patents. It is the need of stakeholders to change the old ways and bring forward a framework robust and able to accommodate the desired business and national requirements. Based on the literature, comparing the traditional methods and blockchain types with proposed framework we analyze that proposed architecture is scalable, efficient, secure and reliable to implement for the economic growth.

6. Conclusion and Future Work

6.1 Conclusion

The proposed framework holds the promise for tackling Pakistan's particular business difficulties and IP protection. The entire design of the architecture, which includes everything from user registration to intellectual property protection, shows a holistic approach to modernizing corporate operations while protecting intellectual property rights. The system provides a decentralized architecture using Event-driven architecture style and peer-to-peer architecture style that improves security, transparency, and collaboration among enterprises, government agencies, and individuals by harnessing the power of Hyperledger Fabric blockchain technology. This framework is well-suited to Pakistan's national requirements, providing a streamlined process for business registration, intellectual property protection, and effective tax management. As technology advances, the incorporation of blockchain technologies has the potential to transform how organizations function and communicate, fostering innovation, economic growth, and regulatory efficiency. This study not only gives a thorough architectural model, but it also highlights blockchain's potential to alter Pakistan's corporate ecosystem and intellectual property landscape.

6.2 Limitations of Framework

While the framework's design has benefits, it also has drawbacks. First, its blockchain technology might introduce complexities for users unfamiliar with decentralized systems. Maintaining the framework's compliance with changing technology and regulations may be difficult. Finally, switching from existing systems to this new design may entail considerable initial investment and a learning curve for all parties.

6.3 Future Work

For future considerations, a lot of research needs to be done on the working of patent matching using machine/deep learning technique and its integration with the blockchain. The proposed framework can be implemented according to the workflows in hyper ledger fabric for the deployment purposes. Moreover, security and scalability can be considered for further improvements.

References

[1] Garcia-Garcia, Julian Alberto, Nicolás Sánchez-Gómez, David Lizcano, María José Escalona, and Tomás Wojdyński. "Using blockchain to improve collaborative business process management: Systematic literature review." IEEE Access 8 (2020): 142312-142336.

[2] Wang, Junyao, Shenling Wang, Junqi Guo, Yanchang Du, Shaochi Cheng, and Xiangyang Li. "A summary of research on blockchain in the field of intellectual property." Procedia computer science 147 (2019): 191-197.

[3] Blockchain Structure https://www.geeksforgeeks.org/blockchain-structure/ [Online: Accessed on April 2023]

[4] How to register a business in Pakistan " https://www.graana.com/blog/how-to-register-a-company-in-pakistan/#:~:text=Log%20in%20to%20e%2Dservices,online%20form%20and%20submit%20it. " [Online: Accessed on April,2023]

[5] SECP "https://www.befiler.com/blog/function-of-the-securities-and-exchange-commission-of-pakistan" [Online: Accessed on April, 2023]

[6] FBR https://en.wikipedia.org/wiki/Federal_Board_of_Revenue [Online: Accessed on May, 2023]

[7] Threats to FBR https://www.globalvillagespace.com/fbr-faces-more-than-70000-cyber-attacks-every-month/#:~:text=The%20Federal%20Board%20of%20Revenue,Raises%20Revenue%20Project%20(PRRP). [Online: Accessed on May 2023]

[8] Marchesi, Lodovica, Michele Marchesi, Roberto Tonelli, and Maria Ilaria Lunesu. "A blockchain architecture for industrial applications." Blockchain: Research and Applications 3, no. 4 (2022): 100088.

[9] EU Blockchain Observatory Forum. https://www.eublockchainforum.eu/eu-blockchainobservatory-forum. [Online; accessed 2023-02-07]. Feb. 2001.

[10] Medium – Where good ideas find you. https://medium.com. [Online; accessed 2023-

02-07]. Jan. 2001.

[11] What is e-Residency | How to Start an EU Company Online. https://www.eresident.gov.ee/. [Online; accessed May 2023].

[12] A Offerman. Swiss City of Zug issues Ethereum blockchain-based eIDs. 2018.

[13] Pöhn, Daniela, and Wolfgang Hommel. "Reference Service Model Framework for Identity Management." IEEE Access 10 (2022): 120984-121009.

[14] Wöhrer, Maximilian, Uwe Zdun, and Stefanie Rinderle-Ma. "Architecture design of blockchain-based applications." In 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 173-180. IEEE, 2021.

[15] Janjua, Pervez Zamurrad, Ghulam Samad, and Nazakat Ullah. "Intellectual property rights (IPRs) and economic growth in Pakistan." *The Pakistan Development Review* 58, no. 3 (2019): 225-237.

[16] Jan, Junaid. "The Development of Intellectual Property Laws in Pakistan: Challenges and Suggestions." *The Pakistan Journal of Criminal Law* 2, no. 1 (2022): 36-44.

[17] Mecozzi, Rodolfo, Giuseppe Perrone, Dario Anelli, Nicola Saitto, Elia Paggi, and David Mancini. "Blockchain-related identity and access management challenges:(de) centralized digital identities regulation." In *2022 IEEE International Conference on Blockchain (Blockchain)*, pp. 443-448. IEEE, 2022.

[18] Blackman, Michael. "Intellectual property: a power tool for economic growth-Kamil Idris. WIPO, 2002. ISBN 92-805-1113-0. Hardback, 377 pages. Price: CH60." *World Patent Information* 4, no. 25 (2003): 359-360.

[19] de Beer, J. (2016). Evidence-Based Intellectual Property Policymaking: An Integrated Review of Methods and Conclusions. *The Journal of World Intellectual Property*, 19(5-6), pp.150-177.

[20] Ahmed, Naveed, Bakht Munir, and Ali Nawaz Khan. "Intellectual Property Rights and Economic Development: A Case Study of Pakistan."

[21] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: Decentralized business review (2008), p. 21260

[22] Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT express*, *6*(2), 93-97

[23] El Bassam, N. (2021). Blockchain. In *Distributed Renewable Energies for Off-Grid Communities* (pp. 447-450). Elsevier.

[24] Jeyabharathi, D., Kesavaraja, D., & Sasireka, D. (2020). Cloud-Based Blockchaining For Enhanced Security. *In Handbook of Research on Blockchain Technology* (pp. 171-181). Academic Press.

[25] Meunier, S. (2018). Blockchain 101: What is blockchain and how does this revolutionary technology work?. In *Transforming climate finance and green investment with Blockchains* (pp. 23-34). Academic Press.

[26] Laaper, S., Fitzgerald, J., Quasney, E., Yeh, W., & Basir, M. (2017). Using blockchain to drive supply chain

[27] Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), 6793-6807.

[28] Kasi, N. R., Ramani, S., & Karuppiah, M. (2022). Blockchain architecture, taxonomy, challenges, and applications. *Blockchain Technology for Emerging Applications*, 1-31.

[29] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130-139.

(Shrimali and Patel, 2022)

[30] Jesse Yli-Huumo et al. “Where is current research on blockchain technology?—a

systematic review”. In: PloS one 11.10 (2016), e0163477

[31] Michael Crosby et al. “Blockchain technology: Beyond bitcoin”. In: Applied Innovation 2.6-10 (2016)

[32] Chris Elsden et al. “Making sense of blockchain applications: A typology for HCI”.

In: Proceedings of the 2018 chi conference on human factors in computing systems.

2018, pp. 1–14.

[33] Abhishek, P. M., D. G. Narayan, H. Altaf, and P. Somashekar. "Performance Evaluation of Ethereum and Hyperledger Fabric Blockchain Platforms." In 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-5. IEEE, 2022.

[34] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." In Workshop on distributed cryptocurrencies and consensus ledgers, vol. 310, no. 4, pp. 1-4. 2016.

[35] Savelyev, Alexander. "Copyright in the blockchain era: Promises and challenges." Computer law & security review 34, no. 3 (2018): 550-561.

[36] Alanzi, Haifa, and Mohammad Alkhatib. "Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review." Applied Sciences 12.23 (2022): 12415.

[37] Bao, Z.; Wang, Q.; Shi, W.; Wang, L.; Lei, H.; Chen, B. When Blockchain Meets SGX: An Overview, Challenges, and Open Issues. IEEE Access 2020, 8, 170404–170420.

[38] Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. Future Internet 2021, 13, 24.

[39] Ra, G.; Kim, T.; Lee, I. VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things. IEEE Access 2021, 9, 75945–75960.

[40] Anthes, Gary. "Estonia: a model for e-government." Communications of the ACM 58, no. 6 (2015): 18-20.

[41] Moehrle, Martin. "Measures for textual patent similarities: a guided way to select appropriate approaches." Scientometrics 85, no. 1 (2010): 95-109.

[42] S. Arts, B. Cassiman, J. C. Gomez, Text matching to measure patent similarity, Strategic Management Journal 39 (1) (2018) 62–84.

[43] K.-K. Lai, S.-J. Wu, Using the patent co-citation approach to establish a new patent classification system, Information processing & management 41 (2) (2005) 313–330.

[44] E. Rodriguez, A. Donoso, R. Guzman, Measuring patent co-citation links with function, form, or component, Technological Forecasting and Social Change 94 (2015) 2–17.

[45] Q. Wang, L. Wang, Y. Wu, Identifying patent theme changes: a topic-based patent network approach, Technological Forecasting and Social Change 148 (2019) 119752.

[46] Y. Yang, P. P. Vergauwen, S. Van Passel, A novel approach to measure textual patent similarity: A study on green patents, Journal of Cleaner Production 301 (2021) 127008.

[47] M. Ahmad, M. Faisal, A new patent classification scheme based on the combined application of text mining techniques and WordNet, Journal of Intellectual Property Rights 27 (3) (2022) 165–178.

[48] G. Cascini, M. Zini, A systematic procedure to analyze patent conflicts, Research in Engineering Design 19 (4) (2008) 205–218.

[49] K. A. Younge, M. J. Burke, M. T. Dahlin, J. B. Olsen, N. K. Norton, P. D. Anderson, Predicting patent litigation: The role of exploration and exploitation, Research Policy 45 (7) (2016) 1364–1381.

[50] Z. Feng, Z. Yang, A Doc2Vec based patent abstract retrieval method, Journal of the Association for Information Science and Technology 71 (1) (2020) 2–13.

[51] Y.-A. Noh, Y.-G. Lee, Text mining based patent network: Analytical tool for high-technology trend, Journal of High Technology Management Research 26 (1) (2015) 39–50.

[52] J.-Y. Joung, J. Kim, Identification of core technologies based on patent analysis, Journal of Intellectual Property Rights 22 (6) (2017) 325–336.

[53] M.-C. Lee, J. Hsiang, A study on patent retrieval algorithm using BERT, Expert Systems with Applications 131 (2019) 56–66.

[54] H. Kadhim, A study of machine learning algorithms for text-document classification, International Journal of Computer Science and Network Security 19 (5) (2019) 74–81.

[55] M. Farouk, A unified model for semantic and syntactic sentence similarity, Applied Soft Computing 89 (2020) 106069.

[56] P. Dong, W. Dong, A linguistic perspective on text representation learning: From word vectors to discourse, Neural Networks 130 (2020) 56–73.

[57] L. Lan, D. Dong, M. Li, A similarity-weighted tree kernel for text classification, Knowledge-Based Systems 204 (2022) 106465.

[58] R. González-Carvajal, E. D. Garrido-Merchán, Comparative analysis of BERT and TF-IDF embedding methods in text classification tasks, Computers, Materials & Continua 64 (3) (2020) 1577–1594.

[59] N. Garg, S. Ramakrishman, Adversarial attacks and defenses in text, ACM Computing Surveys (CSUR) 53 (5) (2020) 1–34.

[60] K. Viji, P. Dhanalakshmi, S. Ayyasamy, A hybrid text similarity measurement method using Bi-LSTM with BERT-based word embeddings, Engineering Applications of Artificial Intelligence 100 (2022) 104037.

[61] Wang, S.; Pei, R.; Zhang, Y. EIDM: A Ethereum-Based Cloud User Identity Management Protocol. IEEE Access 2019, 7, 115281–115291.

[62] https://cointelegraph.com/news/koreans-to-have-access-to-blockchain-powered-digital-ids-by-2024 [Online: Accessed on April 2023]

[63] Sung, C.; Park, J. Understanding of blockchain-based identity management system adoption in the public sector. J. Enterp. Inf. Manag. 2021, 34, 1481–1505.

[64] Stockburger, L.; Kokosioulis, G.; Mukkamala, A.; Mukkamala, R.; Avital, M. Blockchain-enabled Decentralized Identity Management: The Case of Self-sovereign Identity in Public Transportation. Blockchain Res. Appl. 2021, 2, 100014.

[65] Liao, C.H.; Guan, X.Q.; Cheng, J.H.; Yuan, S.M.; Blockchain-Based Identity Management and Access Control Framework for Open Banking Ecosystem. pp. 450–466. Available online: https://ssrn.com/abstract=4039865 (Online : accessed on May 2023).

[66] Zhu, Peng, Jian Hu, Xiaotong Li, and Qingyun Zhu. "Using blockchain technology to enhance the traceability of original achievements." IEEE Transactions on Engineering Management (2021).

[67] Ragot, Sébastien, Antje Rey, and Ramin Shafai. "IP lifecycle management using blockchain and machine learning: Application to 3D printing datafiles." World Patent Information 62 (2020): 101966.

[68] Chen, Wei, et al. "Review on blockchain technology and its application to the simple analysis of intellectual property protection." *International Journal of Computational Science and Engineering* 22.4 2020): 437-444.