Automated Border Control System using Blockchain Technology

By

Shanjita Akter Prome

161-35-1515

Department of Software Engineering

Daffodil International University

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY
Fall- 2019

APPROVAL

This thesis titled on “**Automated Border Control System using Blockchain Technology**”, submitted by **Shanjita Akter Prome**, **161-35-1515** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Prof. Dr. Touhid Bhuiyan **Chairman**
Professor and Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

--- **Internal Examiner 1**

Dr. Md. Asraf Ali
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

-- **Internal Examinar 2**

Asif Khan Shakir
Lecturer
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

-- **External Examiner**

Prof Dr. Mohammad Abul Kashem
Professor
Department of Computer Science and Engineering
Faculty of Electrical and Electronic Engineering
Dhaka University of Engineering & Technology, Gazipur

DECLARATION

It hereby declare that, this thesis has been done by me under the supervision of **Ms. Farzana Sadia, Lecturer, Department of Software Engineering, and Daffodil International University**. It also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Prome

Shanjita Akter Prome
ID: 161-35-1515
Department of Software Engineering
Daffodil International University

Certified by:

12/12/

Ms. Farzana Sadia
Lecturer
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

ACKNOWLEDGEMENT

First of all, I am grateful to the Almighty Allah for giving me the ability to complete the final thesis.

I would like to express my gratitude to my supervisor **Ms. Farzana Sadia** for the consistent help of my thesis and research work, through her understanding, inspiration, energy, and knowledge sharing. Her direction helped me to finding the solutions of research work. I would be delighted to express my extreme sincere gratitude and appreciation to all of our teachers of Software Engineering department for their kind help, generous advice and support during the research.

I also like to thanks my gratitude to **Delwar Alam** from BugsBD for sharing his pearls of wisdom with me during the course of this research. I also express our gratitude to all of our friend's, senior, junior who, directly or indirectly, have lent their helping hand in this venture. Last but not least, I would be must obliged to my family for giving birth to me at the first place and supporting me spiritually throughout my life.

Contents

LIST OF FIGURE

LIST OF NOMENCLATURE

Title	Abbreviation
POS	Proof of Stake
POW	Proof of Work
EVM	Ethereum Virtual Machine
GETH	Go Ethereum
P2P	Peer to Peer
DAPP	Decentralize Application

ABSTRACT

Currently, in this digital world, the passport is still a physical entity. Each passport contains various security and identity attributes to figure out the owner of the passport and also circumvent attempts at tampering with the passports. Fake passports are usually copies of genuine passports that are illegally modified by an unauthorized person. The most individuals get genuineness to show counterfeit visas. The system was unable to identify these fake passports. The individuals deceitfully acquired realness to their fake travel papers that expected genuine. And day by day this number increased with a large range. As a result, criminal activities have grown such as trafficking, smuggling, identity theft and so on. Currently, there is no mechanism available to immediately blacklist or revoke a suspected passport. It's a big challenge especially for Bangladesh to identify travel documents and made border control systems more secure. By using Blockchain Technology we will try to reduce the following problems. It is producing a wide scope of chances and potential outcomes in current travel document verification services. Blockchain is an unbribable peer-to-peer network that permits multiple validators/verified agencies to transfer value in a secure and transparent way. Our aim is to propose a decentralized application and all validators have to connect through the distributed ledger. To verify a passport each validator bet on the blocks and added to the chain. The validators mining the blocks continuously unless found any anomalies, if one validator gets any suspicious issue then the passport included in the blacklisted list. Moreover, we will be trying to maintain a passport list in a smart contract and if there any changes occurred then it will be immediately visible by all validators. In blockchain technology data is immutable and distributes the entire network to be encrypted format, so data breached is not possible. Also, make services more elegant and increasing efficiency.

KEYWORDS

Blockchain, Smart Contract, Passport Verification, Proof of Stake (POS), Proof of Work (POW), Consensus Algorithm, Decentralized, Solidity, Distributed Ledger, Ethereum Blockchain.

CHAPTER 1: INTRODUCTION

1.1 Background

Due to the global trend and evolution of travel vehicles, the number of overseas travelers is moderately increasing. Therefore the existing controlling system is done manually and requires a long queue for immigration. Thus diverse automatic systems were proposed to identify the passports using Refined Neural Network and fuzzy RBF network [18, 19, 20]. Automated border control systems have been in use for decades now in order to thwart illegal entry into countries and prevent terrorism and human trafficking. Borders between countries are strictly enforced to prevent the illegal movement of people or goods into the country [7]. A huge number of people across international borders daily. So it must have reported to all information about entries and exits that are performed daily. As it is data intensive and very crucial would be easily fabricated and furnished for unethical purposes. So these records should be immutable to any attack. Some people take advantage of these loopholes and get involved in illegal activities in the country that go unnoticed. Even though many countries digitized their passport process but it is limited to the country level [11] [12]. So it’s a great time to secure the passport authentication system, identify the blacklisted list as well as make a transaction-based system that covers all over the world. It is also imperative for nations to share their records to provide a strict and efficient control mechanism. At the same time, these records must be securely stored complying with privacy laws and regulations of that country. This has made it all the more imperative to implement systems to alleviate all the above concerns.

Blockchain network initially introduce a consensus algorithm, known as Proof of work (POW). In Blockchain, this algorithm is utilized to affirm exchanges and produce new blocks to the chain [1]. With POW, miners go up against one another to finish the transaction on the system and get remunerated. The proof-of-work hashing scheme Bitcoin uses is similar to Hash cash and based on SHA-256 hash function [38]. The verification of-work is finished by augmenting a nonce in the block until the worth is created that has the necessary number of zero bits toward the start of the block hash. When it is done, it can't be fixed without rehashing the computations. If it is somehow changed by a malicious attacker, then all the following blocks would have invalid hashes. The rule is that the longest chain that has the majority consensus in the network is the correct one, so if the attacker wishes to change a block, needs to have enough computational power to overcome the voting of the majority of honest nodes, thus entering the race problem.

The verification of the stake will make the accord instrument totally virtual. While the general procedure continues as before as confirmation of work (POW), the strategy for arriving at the ultimate objective is totally unique. In POW, the diggers unravel cryptographically hard riddles by utilizing their computational assets. In POS, rather than miners, there are validators. The validators lock up a portion of their Ether as a stake in the environment. Following that, the validators wager on the hinders that they feel will be added to the chain. At the point when the block gets included, the validators get a block reward with respect to their stake.

A smart contract is an agreement actualized, conveyed and executed inside the Ethereum environment. Smart contracts are the digitization of the lawful agreements. Brilliant agreements are conveyed, put away and executed inside the Ethereum Virtual machine. Smart contracts can store information. The Ethereum blockchain enables us to execute code with the Ethereum Virtual Machine (EVM) on the blockchain with something many refer to as digital agreement. Digital agreements are the place all the business rationale of our application lives. This is the place we'll really code the decentralized bit our application. Digital agreements are accountable for perusing and composing information to the blockchain just as executing business rationale. Smart contracts are fundamentally the same as the object-oriented concepts. A smart contract can invoke another smart contract simply like an Object-arranged article to make and utilize objects of another class. You can originate an instance of the contract and hail procedure to view and modify data. Ethereum currently runs smart contracts that oversee millions of dollars, generate their security highly sensitive. A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. In Ethereum Virtual Machine the programmers don’t usually write EVM code, instead they use a JavaScript like programming language called Solidity that compiles to bytecode.

1.2 Motivation of the Research

In the current border control system, the travelers starting with one nation then onto the next required a visa which is checked at the identification scanner at that point approve the data physically and exists out from the nation. The following procedure is to pass the data to the goal nation by the flight bearer. These frameworks have obviously added to the simplicity of air-travel particularly for residents and have helped alleviate extensive screening and congestions at airports. The downside being each of these systems have exposed us to new points of failures and security breaches and occur lots of unusual activity such as human trafficking, terrorism, passport duplication, unauthorized access and so many fraudulent activities. On the off chance that there is any change, the framework can't be refreshed as ahead of schedule as could be expected under the circumstances. So the current framework isn't ideal for a visa confirmation framework and recognizes blacklisted.

Ethereum is a distributed public blockchain network. An Ethereum blockchain is similar to the Bitcoin blockchain. The main difference is that Ethereum blocks contain not only the block number, difficulty, nonce, etc. but also the transaction list and the most recent state. For every transaction in the transaction list, the new state is created by applying the previous state. It represents a blockchain with a built-in Turing-complete programming language. It provides an abstract layer enabling anyone to create their own rules for ownership, formats of transactions, and state transition functions. This is done by involving smart contracts, a set of cryptographic rules that are executed only if certain conditions are met. Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications. Every node in the Ethereum network runs under EVM and executes its instructions. The smart contracts are translated into EVM code and then executed by the nodes. One of the most popular programming language for writing smart contracts is Solidity.

1.3 Problem Statement

The existing model is automatic but it cannot be globally embedded. In the current framework, fake passport holders can without much of a stretch get realness to traverse the border. What's more, the number is expanding at a high rate. A portion of the nations has attempted to digitalize their identification check process in spite of the fact that it can't recognize a blacklisted traveler. According to our nation's point of view the verification procedure isn't as digitalized as required. Additionally, the current framework is an authority over midway which is an extraordinary imperfection just as it can't give information security and data integrity. The main reason to increase criminal activities is the lack of globally sharing information. The existing system does not require global interoperability. User’s information only shared across the country, as a result other countries cannot verify the traveler’s document if they visit other countries. For example, if person A is from Bangladesh implies their identification data included just this nation, so if the person does any illegal activities then he will be a blacklisted person. But other countries unaware of the updated information. Also data security is a significant prerequisite of the current framework. As it is controlled over centrally so information break conceivable. Another essential motivation to require more protection is on the grounds that all the included entities are permit everybody of the information exchanges within the system which is not comply with the existed one. Another major challenge about the existing solution is that data integration. Data integrity refers to the assurance of data accuracy and reliability of data. The existing solution controlled by a centralized authority, so they can change or breach the data.

1.4 Research Questions

1. Question 1: How does our proposed model assistance with the innovation?
2. Question 2: How does our proposed solution is significant for Bangladesh?

1.5 Research Objectives

- To the proposed model uplifts step by step working procedures using blockchain technology.
- To indulge data security our proposed solution provide full security issue, which is a distributed ledger and mostly distinguish the blacklisted traveler.

1.6 Research Scope

In this paper we bring up a solution based on blockchain technology. We make a decentralized application using truffle framework and using ethereum blockchain. We try to cover smart contract with blockchain step by step workflow. Our proposed solution will be covered not only automated immigration process but also check the criminal activities. We build a P2P system which includes the validators and the travelers.

1.7 Thesis Organization

The first chapter of this part is foundation: essential information, history, and utilizations of blockchain innovation are delineated so as to all the more likely characterize explicitly perspectives in this proposal. It also included existed solution limitation of existed models. I would fling to recover the problems. The second chapter of this section gives an outline of accessible models and different projects that has been done by various researchers. After that, the third chapter bring some benefits to use blockchain technology and endorse a proposed model along with full working procedure. Additionally give an algorithm dependent on the proposed model and demonstrate step by step implementation procedure. The fourth chapter is about the implementing result of the proposed model and discuss about the result. At last fifth chapter upholds the overall process, some benefits of our proposed model that has compromised the existed approach and future plan.

CHAPTER 2: LITERATURE REVIEW

So Blockchain technology is reliable, secure and stipulates a solution to this leading problem. None of them choose a better, faster and more secure solution to this problem. Our goal is to provide an analysis of the vulnerabilities of the existing border control system and proposed a refine solution that is comparatively best than others. In this paper we explore a proposed solution which is implemented through blockchain technology. For this purpose, we have studied plethora of implementations using blockchain technology that will be helpful to implement our anticipated work.

2.1 Blockchain Technology

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Each block is linked to the previous one after validation and consensus of all participating nodes. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across all copies of the ledger in the network, and any conflicts are resolved automatically using established rules. A block of individual unit in a blockchain, record all transactions and block header. A block header keeps a collection of metadata about the block that contains a hash-value of its parent in the blockchain, and a hash of the aforementioned metadata and the data of the block itself [2]. It is a secure and more reliable technology. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.

2.2 Blockchain in Border Control System

In the early ages blockchain technology mainly instigated for the banking and finance sectors. But nowadays a shielded way for digital document sharing between distributed ledgers. And distributed ledger can approve a transaction by checking user’s information. The existing model is automatic but it cannot be globally embedded. As blockchain is a decentralized, distributed ledger and supports peer to peer network, so the approach will reach in a global state. Many researchers have already been exploring this technology in various sectors that will discuss in the literature review in chapter two.

A. Globally Digital Document Sharing

Actually, we need a passport so that we can travel the whole world. So it is a fundamental issue to access user’s information by distributed ledger across the world. If the information is not shared with other countries they are unable to verify the user’s identification, thence criminal activities have been increasing with an excessive rate. Through the blockchain technology, passport information can easily be shared with the verified agencies. And if there any change occurs then it will be visible by others as soon as possible. If there any criminal activities are done by them then the country would not provide approval and it will be added in the blacklisted list.

B. Real-Time Tracking

The existing system cannot provide a traveler’s current location. So when they passed from the country they are going to be out of network. So it is quite impossible to track them in the short term. However, our proposed model will provide the opportunity to trail someone at any moment. When a passenger passes a border a transaction will have done in the distributed system, by this they can be easily found. Simultaneously blockchain technology is well known for its security purpose, so data breach will be reduced.

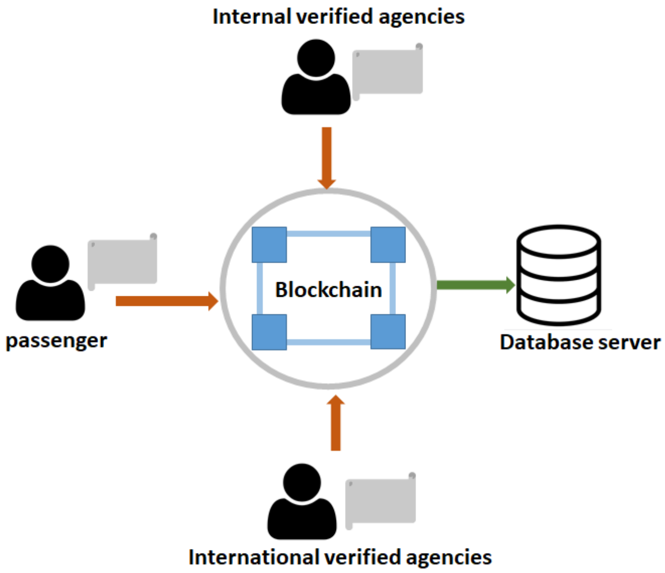


Figure 2 1: Blockchain utilization in border control system

2.3 Related Work

Digital document concept was first disclosed by Haber and Stornetta in 1991[1], they introduce digital document even with the collusion of time-stamping service. They proposed a procedure that maintain complete privacy of the document themselves. In 2008[2], Satoshi Nakamoto first introduced the concept of "bitcoin", a decentralized peer to peer online currency as well as proposed a solution of double-spending problem using peer to peer network. Buterin [2013] first proposed to build a new blockchain technology with unlimited freedom in building features, stronger light client properties as well as allows unlimited inter-transactional storage capability [3]. After that, a yellow paper gives a detailed secure decentralized transaction ledger that is Ethereum by Gavin Wood [4]. Zheng provide an overview of blockchain technology and differentiating some consensus algorithms [5], describe about Blockchain technology and its work process. Numerous divisions propose to build up their current arrangement and upgrade by utilizing blockchain technology, for example, the education sector, health sector, business segment, and even government sector. Tanesh and Vidhya [38], upholds the flaws of existing healthcare system and enhanced the model utilizing blockchain technology to propose a model using blockchain and smart contract. Blockchain technology used as a storage which is personal data management platform focused on privacy [36]. Blockchain technology is famous for their security purpose. According to the another paper Patel and Vasu [8] discuss about existing system, enlists the security vulnerabilities in existing system, strength the power of Blockchain technology proposed a solution with Hyperledger framework etc. Another project work [6] has been done to propose an ethereum based framework and analyzing the verification system. It describe about the verification process with smart contract and such contracts are generally written a Solidity, which is a JavaScript like language. Another Hyperledger project has been done by Panchamia and Byrappa [2017]. They proposed passport, visa and immigration management system using permissioned blockchain [7], Hyperledger Fabric. The increasing rate of fake passports take a great concern wherefore Kim and Kwangbaek [13] came up with intelligent immigration control system. Their focal point was passport recognition along with face recognition and using ART algorithm. In another related work Hanifatunnisa and Rifa [10] has done e-voting system through blockchain technology. In the e-voting system, they generate a decentralize application. They use smart contract to lock away the business logic. In the wake of checking or analysis related research work, we find the point by point of blockchain innovation. In spite of the fact that it was shaped in 2008 yet blockchain-based advancements have started through five to six years before. Blockchain is the best advancement, particularly in security purposes. Moreover blockchain technology already covered many aspects of digitalization.

CHAPTER 3: RESEARCH METHODOLOGY

A blockchain is a digital document which is not control over any centralized body and a distributed ledger system. Blockchain is a set of blocks which is connected to the previous one. In this paper we propose a solution of border control system and try to reduce the problems which are appeared in the current system. We also implement an algorithm which is run according our proposed solution.

3.1 Proposed Solution

In this section, we are proposing a transactional-based solution that verify the user identity accurately. In this solution, we will be using Ethereum Blockchain technology as a platform for information access for the verified users. We will be using smart contract that holds the user's information and deploy the contract with ethereum blockchain. We will describe all dependencies and various algorithms to govern that will govern the system. At last we will describe a workflow about how the system process. In the current situation, this solution will strongly help and enrich the passport verification system. Moreover, it will provide highly security of personal data. Ethereum blockchain gives us all the features that we need, a secure solution of and gives us the following advantages:

1. **A quick approach:** If there is any modification e.g. add some new information then it will be easy to deal with that and the updated information will reach the authorized person as soon as possible. This system will provide a quick verification system.
2. **Provide secure database:** Blockchain database that is not easy to copy or expose the data and an immutable system.
3. **Bring more transparency in the entire system:** The current system has a plethora of errors mainly due to people assessment in the system.

4. **Give origin of the information in the blockchain:** The main flaw of the current system is that the data is manipulated easily. By having blockchain based solution we will get two important features such as- immutability and data provenance.

In this chapter we explore the core concept about blockchain technology. In the recent years blockchain technology contributes various innovation challenges and efficiently provide a better solution than others. The vital reason to use blockchain technology is that it serves a decentralized approach and complete package of information security.

3.2 Proposed Model

We propose a blockchain-based solution for automated border controlling which is a distributed ledger, securely sharing data, verify document and blacklisted checker. Client security as well as record consistency have been attained by this asymmetric cryptography and consensus algorithm. The existing solution has compromised with the proposed one. Our point is to bring a distributed model that is expandable, globally usable and most secure. The key attributes which are cannot be corrupted, enhanced security, faster settlement and anonymity.

We have tried to diminish the criminal activities and reduce the unauthorized access. Thusly, the framework likewise lessens the time spent in errands requiring verification of the user identity and wipes out the need for any central authority in verification and management of identity information. Blockchain technology thought to be among one of the reasonable methods for putting away and sharing the passport information where miner persistently verified the digital document. Our step by step workflow is similar to the existing one with an indispensable difference that we are using blockchain technology. We proffer a model by exploiting blockchain technology and compared with existing one in some unequivocal parameters.

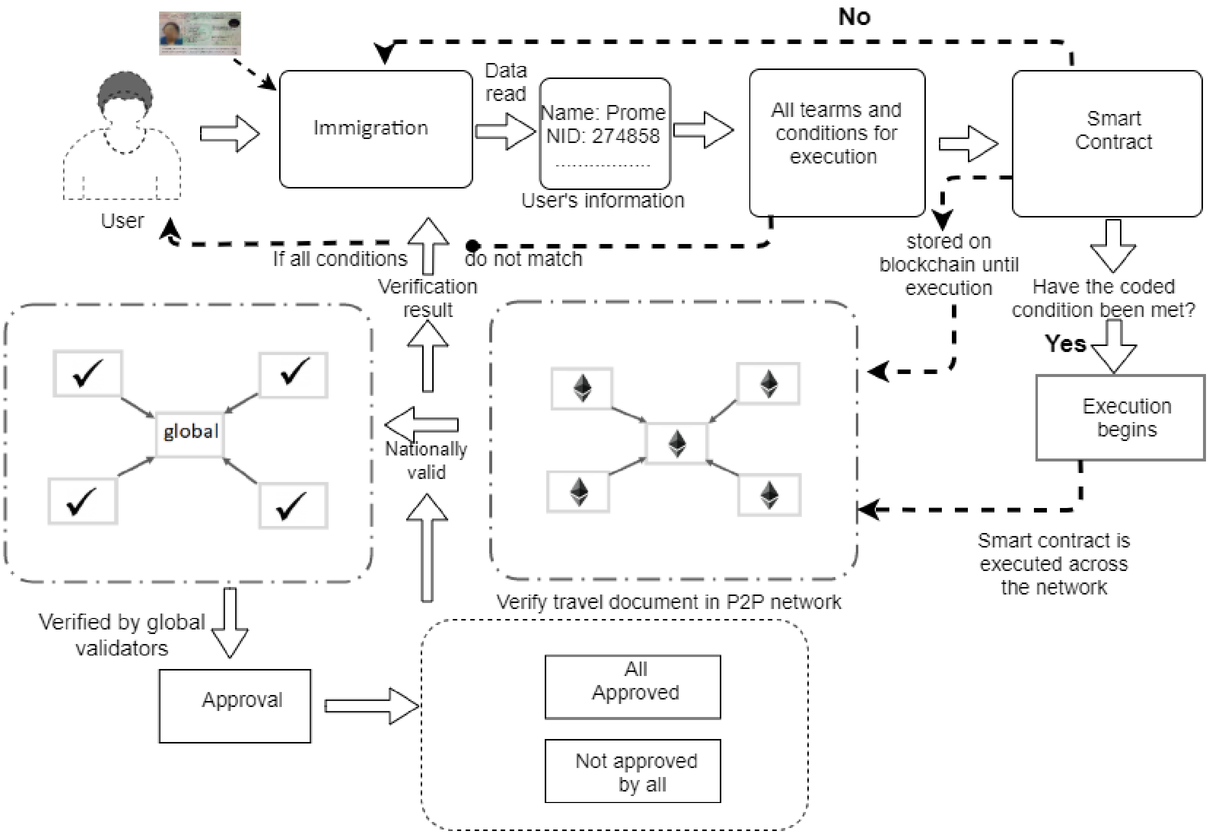


Figure 3 1: Automated Border Control System using Blockchain Technology

Referring to figure- 3.1, contemplating the immigration process, inch by inch approach to substantiate the user’s document nationally and globally. When the traveler scan their travel document each document contains different security and personality traits that can be utilized to recognize the proprietor of the identification and furthermore evade endeavors at altering the travel documents. Traveler’s information hoarded on distributed ledger in encrypted format and pledged the encrypted block as zero knowledge proof. Validators proceeds each transaction for verifying the information and scrutinize their criminal activities. For execution verify the legitimacy of the transactions in each block, once passed then continue next step to penetrate into the smart contract. All signatures are affixed in ledger that was proved by encrypted block also included verifiability. Smart contract used to gather precise and immaculate information from the successful transaction of a decentralized system when the transaction occurs putting away this data in a new block. Here smart contract is an immanent part for this decentralized application. Smart contract is a digital document that store all business logic. The blockchain properties which include an immutable record of data is stored in the digital document [34].

When a valid transaction is done and recorded on the chain [35] then a smart contract can be utilized to automatically trigger exchanges under specific conditions. Within distributed system amassed transaction cannot be tampered.

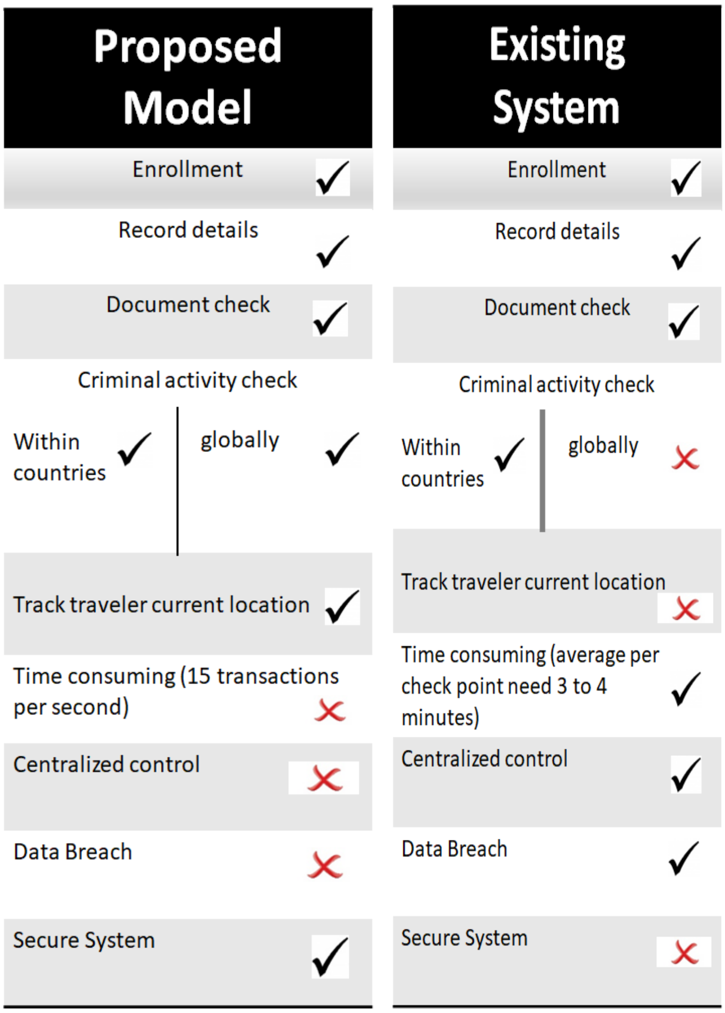
A simple contract in solidity can have an array defined for storing identities and associated logic records. This array can be used to store the identifying information about a passport. After being executing in a smart contract, the contract has to deploy into the blockchain as well as put away in blockchain until execution. Likewise, the logic has been check and if they met then the contract executed across the network otherwise back to the immigration process. When user's information passes through the immigration system, the information stored in distributed ledger traveler's along with country list which have been found in transaction history. When traveler pass the border country's validators check the digital document and identify if there any criminal activities nationally. At the moment of passing immigration, a transaction is done in the distributed ledger whereas validators persistently mining the data. In the event that there any changes happen, at that point, the proposed framework would require to refresh as quickly as time permits and it would be noticeable by others. While the latest transaction is stored, the unsphere transaction replaced as sphere. As follows each transaction verified and tracked efficiently. For this situation, a few protocols needed to guarantee the ledger such as proof of stake, a consensus algorithm use for our proposed solution. Consensus algorithm helps to update the distributed system securely [37]. Thus this process enables control over the movement of the suspected travel document. So the propose framework confirms the value matching with digital document, withal checking their crimes and following their last transaction.

For passing borders traveler's verification needed nationally and globally both. The country list that stored in blockchain will help to verify their travel documents globally. In the event the validators confirmed locally, whereas different nations included in the country list that has been stored in transaction history. On the off chance that there are any violations, by then the validators don't get their endorsement, without every single validator's endorsement considers as a blacklisted. On the contrary, if all the validators provide their approval then it considers as a valid, legal and approved travel document. Smart contract refers to recheck the logic, if match then the border gate would be opened. As contrasted with existing available contracts, a smart contract is quicker just as it additionally diminishes the ideal opportunity for executing and sending the traveler's information. Simultaneously it is a decentralized system, so no one has to control centrally. As it is very data-intensive, so data breach may be a great challenge. We attempt to decrease the accompanying issue by using the most secure technology blockchain.

The promotion with respect to the use of blockchain in the border controlling is a reality in the coming future as scientists are investigating different parts of blockchain in fringe controlling frameworks.

3.3 Comparison

In this section, we maintain such a significant number of contrasts between existing model and proposed model. Likewise expose the distinctions against earlier work. Moreover some countries already make their immigration system digitalized but Bangladesh cannot improve their border pass system which is a threat and also considered to be a risk zone.



Proposed Model		Existing System	
Enrollment	✓	Enrollment	✓
Record details	✓	Record details	✓
Document check	✓	Document check	✓
Criminal activity check		Criminal activity check	
Within countries	✓	Within countries	✓
globally	✓	globally	✗
Track traveler current location	✓	Track traveler current location	✗
Time consuming (15 transactions per second)	✗	Time consuming (average per check point need 3 to 4 minutes)	✓
Centralized control	✗	Centralized control	✓
Data Breach	✗	Data Breach	✓
Secure System	✓	Secure System	✗

Figure 3 2: Comparison between existed model and proposed model

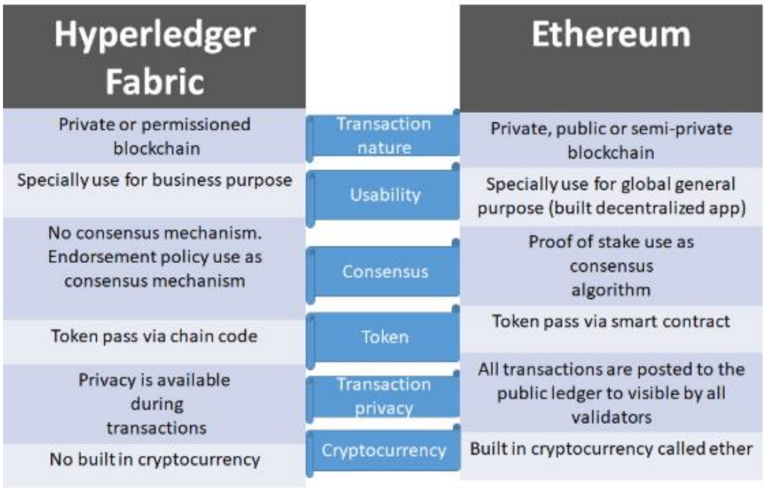
i. The existing framework is computerized however the identification document archives are filled in as locally or nationally that will be unraveled in our proposed framework.

ii. Existing system is control over centralized however our proposed solution is decentralized.

iii. Existing model unfit to recognize traveler's crimes that is done in different nations yet as a distributed record our proposed model effectively discovered this.

iv. The current model is tedious despite what might be expected our proposed solution can proficiently perform 15 transactions for each second.

v. By utilizing blockchain technology give information security where existing one isn't verify and perform information breach.



Hyperledger Fabric		Ethereum
Private or permissioned blockchain	Transaction nature	Private, public or semi-private blockchain
Specially use for business purpose	Usability	Specially use for global general purpose (built decentralized app)
No consensus mechanism. Endorsement policy use as consensus mechanism	Consensus	Proof of stake use as consensus algorithm
Token pass via chain code	Token	Token pass via smart contract
Privacy is available during transactions	Transaction privacy	All transactions are posted to the public ledger to visible by all validators
No built in cryptocurrency	Cryptocurrency	Built in cryptocurrency called ether

Figure 3 3: Differences between Hyperledger and Ethereum Blockchain

In the previous work, Patel and Vasu [8] proposed a solution with Hyperledger framework. It is a permissioned blockchain though ethereum give secure, quicker and productive solution. In Hyperledger fabric, there is a central body who maintain the endorsement policy. As they do not have any consensus mechanism, so the endorsement policy set as to validate the travelers. It may be a great flaw that the centralize point itself a vulnerable issue which is might be compromised.

3.4 Implementation

In this section we will portray an algorithm that will work as indicated by the proposed model. Here, gh= global host, h=host, t=traveler.

Algorithm-1: Passport Verification

```
procedure start (t, h)
  var HostMap= {}
  If (t=h) then
     gh = Partion (t=h)
     rst = gh + gh1 + gh2 +……ghn = result
     create ResultMap (rst)
       function ResultMap (rst) {
          [ ].map.call (rst, function (t, h) {HostMap [t]
          value in HostMap?
          return t;
        });
        function Checker (t) {
          If HostMap [t]. equals ResultMap [rst]
           return approved
         Else
           return not approved
        }
  end if
end procedure
procedure Partition (t, h)
  for t to h do
    if t! = h then
      rejected
    end if
  end for
end procedure
```

We have defined our user’s information that sample has shown below

```
Contract user {
        struct userInfo {
            •  uint id;
            •  string firstname;
            •  string lastname;
            •  string fathername;
            •   string expdate;
            •   string nationality;
            •   string gender;
            •   uint nId;
        }
  mapping(uint => userInfo) public candidates;

// Initialize user’s information
assert.equal (user [0], 1, "contains the correct id");
assert.equal (user [1], "Prome", "contains the correct    firstname");
assert.equal (user [2], "alam", "contains the correct            lastname");
assert.equal (user [3], "Shah Alam", "contains the correct fathername");
assert.equal (user [4], "23-03-2020", "contains the correct expdate");
assert.equal (user [5], "Bangladeshi", "contains the correct nationality");
assert.equal (user [6], "Female", "contains the correct gender");
assert.equal (user [7], 0, "contains the correct nId");
```

Deploy ethereum contract in truffle-

```
var user = artifacts.require("./user.sol");
var Migrations = artifacts.require("./Migrations.sol");
```

In the usage, we utilize the web3 javascript library to associate with the Ethereum blockchain. It can retrieves user account, send transactions and interact with smart contract.

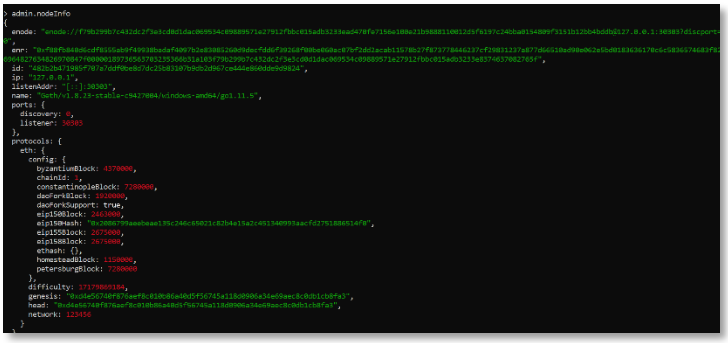
```
initWeb3: function() {
if (typeof web3 !== 'undefined') {
App.web3Provider = web3.currentProvider;
web3 = new Web3(web3.currentProvider);
else {
App.web3Provider = new Web3.providers.HttpProvider('http://localhost:7545');
web3 = new Web3(App.web3Provider);
}
return App.initContract();
},
```

CHAPTER 4: RESULT AND DISCUSSION

During the implementation we try to build a system based on the following proposed model which will have been done according to the proposed algorithm. First we build a private network using geth console. After that build a Dapp for storing user's information in blockchain.

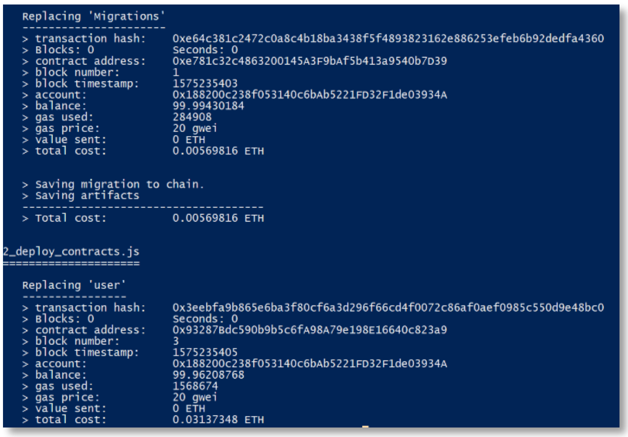
4.1 Build a Dapp

Blockchain Application lifecycle relies upon DApp, Token and Protocol. These three catchphrases are associated with blockchain through block creation to check a block in the blockchain arrange. The decentralized application is shortened by DApp. In Blockchain innovation DApp is running on Decentralized Peer to Peer organize which is utilizing Front-end package, for example, JS, HTML, and CSS additionally use Back-end innovation like as Solidity Smart agreement and use TestRPC server as a test situation. Blockchain utilizes DApp with digital agreements for the incorruptible or quick exchang



```
> admin.nodeInfo
{
  enode: "enode://f79b299b7c432dc2f3e3cd0d1dac069534c09889571e27912fbbc015adb3233ead478fe7156e188e21b9888110012d5f6197c24bba0154809f3151b12bb4bddb@127.0.0.1:30303?discport=
0",
  enr: "0xf88fb840d6cdf8555ab9f49938badaf4097b2e83085260d9decfdd6f39268f00be060ac07bf2dd2acab11578b27f873778446237cf29831237a877d66510ad98e062e5bd0183636170c6c5836574683f82
696482763482697084 7f00000189736563703235366b31a103f79b299b7c432dc2f3e3cd0d1dac069534c09889571e27912fbbc015adb3233e8374637082765f",
  id: "482b2b471985f707a7ddf0be8d7dc25b83107b9db2d967ce444e860dde9d9824",
  ip: "127.0.0.1",
  listenAddr: "[::]:30303",
  name: "Geth/v1.8.23-stable-c9427004/windows-amd64/go1.11.5",
  ports: {
    discovery: 0,
    listener: 30303
  },
  protocols: {
    eth: {
      config: {
        byzantiumBlock: 4370000,
        chainId: 1,
        constantinopleBlock: 7280000,
        daoForkBlock: 1920000,
        daoForkSupport: true,
        eip150Block: 2463000,
        eip150Hash: "0x2086799aeebeae135c246c65021c82b4e15a2c451340993aacfd2751886514f0",
        eip155Block: 2675000,
        eip158Block: 2675000,
        ethash: {},
        homesteadBlock: 1150000,
        petersburgBlock: 7280000
      },
      difficulty: 17179869184,
      genesis: "0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3",
      head: "0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3",
      network: 123456
    }
```

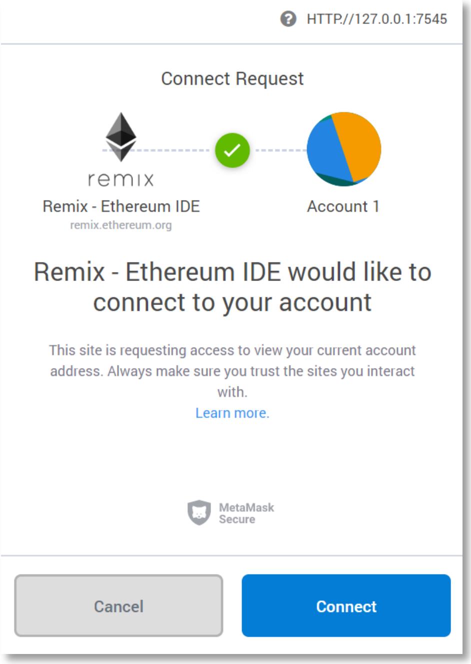
Figure 4 1: Admin node information



```
   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0xe64c381c2472c0a8c4b18ba3438f5f4893823162e886253efeb6b92dedfa4360
   > Blocks: 0            Seconds: 0
   > contract address:    0xe781c32c4863200145A3F9bAf5b413a9540b7D39
   > block number:        1
   > block timestamp:     1575235403
   > account:             0x188200c238f053140c6bAb5221FD32F1de03934A
   > balance:             99.99430184
   > gas used:            284908
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00569816 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00569816 ETH


2_deploy_contracts.js
=====================

   Replacing 'user'
   ----------------
   > transaction hash:    0x3eebfa9b865e6ba3f80cf6a3d296f66cd4f0072c86af0aef0985c550d9e48bc0
   > Blocks: 0            Seconds: 0
   > contract address:    0x93287Bdc590b9b5c6fA98A79e198E16640c823a9
   > block number:        3
   > block timestamp:     1575235405
   > account:             0x188200c238f053140c6bAb5221FD32F1de03934A
   > balance:             99.96208768
   > gas used:            1568674
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.03137348 ETH
```

Figure 4 2: Deploying smart contract

4.2 Mining Ethereum Blockchain using POS



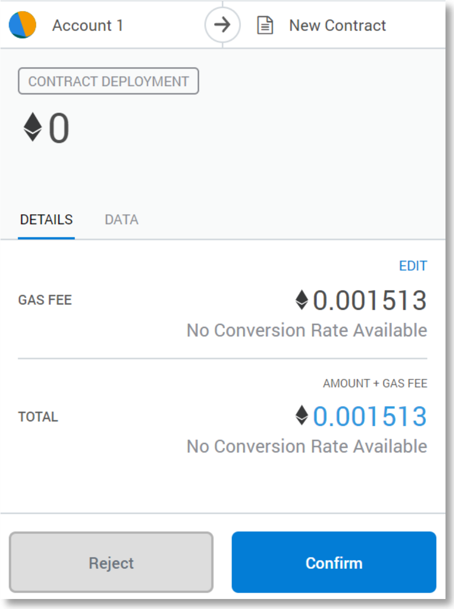
HTTP://127.0.0.1:7545

Connect Request

Remix - Ethereum IDE would like to connect to your account

This site is requesting access to view your current account address. Always make sure you trust the sites you interact with.

Figure 4 3: Test network to confirm account



CONTRACT DEPLOYMENT

♦0

GAS FEE ♦0.001513
No Conversion Rate Available

AMOUNT + GAS FEE
TOTAL ♦0.001513
No Conversion Rate Available

Figure 4 4: Test network to confirm smart contract

4.3 SWOT Analysis

SWOT is an abbreviation of strength, weakness, opportunity and threat. To complete any innovation SWOT analysis add efficiency. In this paper, we are using Ethereum blockchain. Ethereum is a distributed public blockchain network. So each transaction in the public ledger is verified by the consensus of a majority of the participants in the system. The main hypothesis is that the Blockchain establishes a system of creating a distributed consensus in the digital online world. We shot to do our best to build an efficient and secure system with the help of Blockchain technology as it provides a replete security system of the information. Moreover, Blockchain-based systems will provide cryptographically guaranteed immutability which helps with auditing and discourages any fraudulent activity.

Many countries have already accomplished their immigration process with digitalization. But in our country, the immigration system is not as digitalized as we need. Though it is automated but incapable of identifying criminal activities or fake travel document which get authentication smoothly. Our proposed solution reduce the major issue efficiently. In the proposed approach if there any changes occur then the distributed system will be updated quickly and notified the other validators which is a major strength in the approach. Moreover traveler’s each and every transaction contained in the distributed system which help to locate travelers immediately.

There is a feeble point in the proposed arrangement. Be that as it may, in the event that we space to give advance modules, at that point, it would be lessened. In the event that a traveler contains double visas and done their crimes against one identification, at that point, it would be smidgen hard to follow the explorer's crime.

In the event that we limit the frail purpose of this proposed innovations, at that point, it would be a well-suited approach for recognizing the traveler's criminal activities. Likewise, we can add a prediction algorithm to monitor the traveler's activities. Moreover in future, if it is explored the whole world then it would be a greatest innovation of blockchain technology. The proposed model is not implemented by another organization across Bangladesh, so presently there is no threat.

In this chapter we upholds the strengths, weakness, opportunity and threat of the proposed solution. We have to enhance our model to overcome the following weakness and explored blockchain technology properly.

CHAPTER 5: CONCLUSION AND RECOMMENDATION

5.1 Findings and Conclusion

There is a huge opportunity for enhancing blockchain innovation for process information exchanges all the more rapidly. Blockchain technology enhances the nationwide interrelation and reduce the centralized approach which is a major key component in the globalization.

In this paper, we have preferred a new approach to verify the travel document across all over the world. We have proposed out solution using blockchain technology. Our suggested model recommend a decentralized application and all the validators have to connect with each other through the peer-to-peer network. All the validators continuously mining the node. We reserve the data in a distributed ledger that is shared across all validators. At we have discussed the existing border controlling system and perceive limitations of the current process. We have conveyed that the security and trustworthy issue of existing process. After that we provide the motivation of using blockchain technology to reduce the current immigration problem as well as provide data security. Then we have ventilated our proposed model step by step with the help of an end-to-end workflow. After that we have shown a comparison between existing and proposed model. Especially the comparison prove the betterment of our proposed solution.

5.2 Recommendation and Future Work

In the time of proposing model we can’t get enough information about automated border control system using blockchain is patent under an organization. We would like to implement automated border control system in blockchain to track blacklisted traveler as early as possible and also interested to show how this proposed model can eliminate the fake passport holder list.

Moreover in the context of our future work, we plan to active the proposed model in the real world and enhanced our model more efficiently, feasible and a timesaving approach. To ameliorate our proposed model we will try to add user's real image along with their personal information and we recheck the image when the passport would be verified. That can smoothly endorse the user to access ledger data. Moreover we will try to implement machine learning to make better performance. We store all the data in blockchain (decentralized database) and verify the information without any mankind. Machine perform as a validator, thereby mould a better result and no data lost. We look forward to further improve the system with automated interface.

REFERENCES

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
2. Haber, Stuart, and W. Stornetta. "How to Time-Stamp a Digital Document, Crypto'90, LNCS 537." (1991): 437-455.
3. Buterin, Vitalik. "Ethereum white paper." *GitHub repository* (2013): 22-23.
4. Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* 151.2014 (2014): 1-32.
5. Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017.
6. Panchamia, Sanket, and Deepak Kumar Byrappa. "Passport, VISA and Immigration Management Using Blockchain." *2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM)*. IEEE, 2017.
7. Patel, Dhiren, and Vasu Mistry. "Border Control and Immigration on Blockchain." *International Conference on Blockchain*. Springer, Cham, 2018.
8. Aydar, Mehmet, and Serkan Ayvaz. "Towards a Blockchain based digital identity verification, record attestation and record sharing system." *arXiv preprint arXiv:1906.09791* (2019).
9. Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE, 2017.
10. . European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, "Operational and Technical Security of Electronic Passports," 2011.
11. Machine Readable Travel Documents, Seventh Edition, 2015. Online available: (8 December, 2019, 11:36 PM) https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf
12. Kim, Kwangbaek. "Intelligent immigration control system by using passport recognition and face verification." *International Symposium on Neural Networks*. Springer, Berlin, Heidelberg, 2005.
13. Topic-"Blockchain Technology in Passport Verification". Online available:

https://www.blockchainexpert.uk/blog/how-blockchain-helps-in-passport-verification (4 am, 12.4.2019)

14. . A. Pascual, K. Marchini, S. Miller, 2018 identity fraud: Fraud enters a new era of complexity (2018)
15. Risius, Marten, and Kai Spohrer. "A blockchain research framework." *Business & Information Systems Engineering*59.6 (2017): 385-409.
16. Vujičić, Dejan, Dijana Jagodić, and Siniša Ranđić. "Blockchain technology, bitcoin, and Ethereum: A brief overview." *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, 2018.
17. Kim, Kwang-Baek, Young-Ju Kim, and Am-Suk Oh. "An intelligent system for passport recognition using enhanced RBF network." *International Conference on Computational and Information Science*. Springer, Berlin, Heidelberg, 2004.
18. Kim, Kwang-Baek. "Passport Recognition using Fuzzy Binarization and Enhanced Fuzzy RBF Network." *Journal of Korean Institute of Intelligent Systems* 14.2 (2004): 222-227.
19. Kim, Kwang-Baek, Jae-Hyun Cho, and Cheol-Ki Kim. "Recognition of passports using FCM-based RBF network." *Australasian Joint Conference on Artificial Intelligence*. Springer, Berlin, Heidelberg, 2005.
20. Holotescu, Carmen. "Understanding Blockchain Opportunities and Challenges." *Conference proceedings of» eLearning and Software for Education «(eLSE)*. Vol. 4. No. 14. ” Carol I” National Defence University Publishing House, 2018.
21. Bogner, Andreas, Mathieu Chanson, and Arne Meeuw. "A decentralised sharing app running a smart contract on the ethereum blockchain." *Proceedings of the 6th International Conference on the Internet of Things*. ACM, 2016.
22. Mettler, Matthias. "Blockchain technology in healthcare: The revolution starts here." *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2016.
23. . Dhillon, Vikram, David Metcalf, and Max Hooper. "Recent Developments in Blockchain." *Blockchain Enabled Applications*. Apress, Berkeley, CA, 2017. 151-181.

24. Labati, Ruggero Donida, et al. "Biometric recognition in automated border control: a survey." *ACM Computing Surveys (CSUR)* 49.2 (2016): 24.

25. Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

26. Serrano, Will. "The Random Neural Network with a BlockChain Configuration in Digital Documentation." *International Symposium on Computer and Information Sciences*. Springer, Cham, 2018.

27. Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016.

28. Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." *2015 IEEE Security and Privacy Workshops*. IEEE, 2015.

29. Hileman, Garrick. "State of blockchain q1 2016: Blockchain funding overtakes bitcoin." *CoinDesk, New York, NY, May* 11 (2016).

30. Borrows, Maisie, Eleonora Harwich, and Luke Heselwood. "The future of public service identity: blockchain." (2017).

31. R. C. Merkle, Protocols for public key cryptosystems, in: Security and Privacy, 1980 IEEE Symposium on, IEEE, 1980, pp. 122–122 (1980).

32. (8 December, 2019, 11.31 PM) Topic: Blockchain Technology with smart contract. Online available:

https://www.researchgate.net/publication/328230865_Blockchain-based_Smart_Contracts_-_Applications_and_Challenges

33. Bonneau, Joseph, et al. "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies." *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015.

34. G. Zyskind, O. Nathan and A. ’. Pentland, ”Decentralizing Privacy: Using Blockchain to Protect Personal Data,” 2015 IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180-184

35. Baliga, Arati. "Understanding blockchain consensus models." *Persistent*. 2017.

36. Elrom, 2019: “The Blockchain Developer” New York, USA, Apress.

37. Bentov, Iddo, et al. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake." *IACR Cryptology ePrint Archive* 2014 (2014): 452.