# Implementation of Private Blockchain in Smart Card Management System

Saha Reno[1*], Md. Robaitul Islam Bhuiyan[1], Mamun Ahmed[1], M.A. Monyeem[1]

[1]Department of Computer Science & Engineering, Bangladesh Army International University of Science and Technology, Cumilla, Bangladesh.
[*]saha.reno@baiust.edu.bd

**Abstract: Nowadays Blockchain technology is adopted for various services by a good number of global companies. Blockchain technology ensures integrity of ledgers, privacy of transaction and authenticity of transactions without a centralized control actor. In this paper, we are focused on using this technology in citizen identification system of Bangladesh. A Certification Authority ensures that the information which is not genuine and tempered is not added in our proposed decentralized network. One of the most preferable and suitable consensus algorithms for private Blockchain system known as Proof of Authority (PoA), is used to secure the mining process as every miner in the system are known entities, thus protecting the system from 51% attack, which is indeed a major drawback of the public Blockchain system. Once a block is mined and distributed across the network, no information could be deleted or modified and the system becomes counteractive against any fraudulent attacks.**

**Keywords:** *private blockchain, permissioned blockchain, smart contract, proof of authority, smart card*

## 1. Introduction

To facilitate digital services to the people, identification system is an important factor. In Bangladesh a unique identification number is being provided by the government. This identification number is important for various purposes like voting, Visa application, SIM registration, Job application and various sorts of government services.

Various fraudulent activities regarding this identification system are becoming common phenomena in Bangladesh. Many immigrants are getting identification number using illegal way as they are not citizen of this country because of some corrupted people in the authority.

As this arrangement is centralized, any unethical concern can intentionally temper the original information. Moreover, this identification system is still distributed and segmented between different government agencies and it causes problems to the users as they have to do the registration for each service and have to remember the sign in information individually.

Blockchain technology was introduced as Bitcoin's underlying technology. Because of its distributed and decentralized nature, it is being used in various field of technology as it is practically quite impossible to add, modify or delete records of a transaction.

In this paper, a blockchain based Smart Card system is proposed which is both private and permission. As the information is stored in a peer-to-peer and distributed manner across the network, it is impossible to temper any information stored inside each block as a form of transaction. All of the identification related data are stored in one decentralized network from which only approval from the system's Certification Authority (CA) is required to access any specific Smart Card information which is immutable in nature. Moreover, the system uses Proof of Authority (PoA), which ensures that all the miners are known entity, so that the system can be protected against any fraudulent attacks occurred by the anonymous miners in public blockchain scenario.

## 2. Related Works

Blockchain is a peer-to-peer, decentralized and distributed database system which could be either public or private in nature [1]. Prior to storing any dataas a form of transaction in a block, the agreement made by all the nodes in the system must be ensured first. Once information is written in the block, it cannot be further tempered, removed or reversed by any peer. All the blocks of the system, except the first one which is known as Genesis Block, are linked with the block situated behind the musing a cryptography hash, formsa chain-like architecture which is the core reason behind the robust security it provides [2]. Ethereum, which is built upon the decentralized and distributed nature of blockchain infrastructure, is an open source platform used to automate any blockchain based system byone of its distinctive features named Smart Contract[3]. This smart contract define sell the terms and conditions, the users who are permitted to use the system and the rules for making a valid transaction. After the contract's deployment on the chain, it will not be possible to modify the blocks of code inside that contract. To execute a smart contract, the participating nodes of the system must fulfil the conditions which are responsible to invoke this self-executing computer program [4].The identification system of the past decades is insecure, complex, time consuming and full of middleman. It has always been the subject to unethical intruders, downtime of the system, unavoidable system upgrades and license fees, as well as hardware constraints and network traffic obstructions [5]. At present there are still challenges in verifying user identity, authenticating and authorizing user. As the system is distributed, a large amount of user data is provided to service provider that increases the probability of fraud [5] [6].Recently there was a massive data leak of 46.2 million mobile users [7]. There is a possibility that their personal details, mobile number, addresses may have fallen into wrong hands [7].

At present, many organizations are using this blockchain technology to implement different types of identity verification systems. These newly developed frameworks are way more secure than the classical ones. ShoCard [8] allows us to store our personal information in an identity document in the Blockchain. After being digitally signed by the owner, the document gets both encrypted and hashed. Next, the document is sent to the blockchain network and the decentralized app generates a public and a private key against that document. The authenticity of a person's identity can be verified using the public key generated by the system but modification of personal information requires private key [22]. OneName [9] provides an identity service that allows users to bind their names and bitcoin addresses to social accounts, which is equivalent to providing a public Bitcoin address and digital signature for each social account. The Bitnation project [10] aims to create virtual nations on the blockchain platform for the purpose of making the services provided by the government globally accessible. This decentralized platform requires its users to register as a Bitnation"Citizens" and after successful registration they will receive Bitnation's "World Citizen Identity Card". After a person is assigned Bitnation citizenship, he/she is able to access all the self-accredited services offered by this Bitnationproject [23].

## 3. Preliminaries

An easy way to comply with the requirements stated in the Author Guide [1] is to use this document as a template and simply type your text into it. PDF files are also accepted, so long as they follow the same style.

### *3.1. Blockchain*

Blockchain refers to a chain of blocks which stores transactional information in such a way that the digital data inside the blocks are immutable. It can be thought of as a public ledger which is distributed and decentralized. One or more transactions must occur for a block being created. Each of the blocks store time, date and type of the transactions inside it. It also stores the information about the person executing the transaction. These blocks have their own unique hash which distinguishes them from each other. Using a mechanism named 'Consensus', blockchain ensures that no fraud transactions can occur or the transactions inside these blocks cannot be omitted or changed [11][12]. Proof of Work is one of the many Consensus mechanisms; in which a miner mines a block by making sure that no fraud transactions are being stored in the blocks or no intruder can modify the information residing in the blockchain. To temper a blockchain, 51% attack must occur, which refers to an attack made by a large number of miners or just by one single block validator taking over 51% of the system's computing power, which is still hypothetical and almost impossible [13].

### *3.2. Ethereum*

Ethereum is an open source, decentralized blockchain based system which has a unique functionality named Smart Contract. Developers can use this platform to build decentralized applications and what makes this system distinguishable from other blockchains is that it is programmable; therefore, new kinds of applications can be built using Ethereum's own programming language known as Solidity. Time required to mine a block is comparatively much lower than any other blockchain based systems [15][16][17]. Ethereum has its own cryptocurrency known as Ether which is, after Bitcon, is the second most popular crypto-currency in the world [18]. Besides Ether, Ethereum also supports many standard tokens which are not crypto-currencies but essential for Initial Coin Offerings (ICO) to raise fund from public for a future project or new crypto-currencies to be developed [19]. Moreover, there are various test networks for Ethereum besides the main network, all of which can be used to test a newly developed decentralized application whether it has any kinds of flaw and working according to the desired functionality [3]. After testing in any of the test networks, if the dApp works perfectly, then it can be transferred to the main network for the actual deployment in the Ethereum network.

### *3.3. Smart Contract*

Smart Contract refers to a piece of computer code which controls the whole decentralized app built by a developer. It manages all the transactions being executed without third parties. This contract includes the terms and conditions of the agreement between buyer and seller; necessary for a transaction to be executed, which are written into lines of code [4]. Smart Contract is also refereed as a computer protocol running on top of Ethereum blockchain system under which both parties agree to interact with each other. The programming language used to develop the smart contract is known as Solidity. After writing the smart contract, it needs to get uploaded to Ethereum's main network or test network [3].

### *3.4. Proof of Authority*

Proof of Authority is one of the most popular algorithms used in consensus mechanism for private and permissioned blockchain, capitalizes on the value of identities, which means the validators of the blocks do not stack coins to be nominated for mining a block. Instead, they stake their own reputation which is used as the only criteria for being selected by the authority of the system [14]. Transactions and blocks are mined by these pre-approved participants and act as moderators of the system. This model relies on a small number of block validators, thus making the system highly scalable [20]. It also enables the companies to maintain their privacy while still receiving all the benefits and security of blockchain technology [21].

## 4. Proposed Framework

### *4.1. Development of Private and Permissioned Blockchain*

Ethereum based Private Blockchain is used to build up the system. The system is permission based, meaning that not everyone can join the system and remain anonymous. A Certification Authority (CA) makes sure of the fact that only those users who have permission to join the system can be a part of the network to act as a miner or execute any transaction. Another role which is played by the CA is to certify whether a transaction made by any node of the network is valid or not. Here, the transactions contain all the relevant information of a person's Smart Card. All the terms and conditions of the system are written in a Smart Contract using which the CA verifies an authentic transaction.

### *4.2. Development of Smart Contract*

Smart contract is a procedure or code written using programming languages like Java or go and is stored in the blockchain network. Smart contract defines the conditions on which all stakeholders agree. It is like paper contracts agreed by stakeholders and executed programmatically.
Smart contracts are essential to ensure that data is entered in to the ledger by the correct Stakeholder.Since the smart card data is sensitive to each agency or country, we need to have strong permissions logic to govern it. For example, Permission to enter or modify citizen related data in blockchain should be assigned only to Election commission authority of Bangladesh. However other stakeholders can query citizenship related data (read access) from the blockchain based on certain conditions if required.

For this paper, we have two major algorithms that will be used as logic.

*ALGORITHM 1 - Issue of Smart card*

```
Require:
    The Smart card issuing agency role is defined and
    added in the blockchain.
Ensure:
    Smart Card issuing agency role restricted to add
    only Smart Card related data. The agency will have
    permission to update Smart Card status (Issued,
    Renewed and Revoked) and query details of a
    particular citizen.
Inputs:
    Smart Card application details submitted by the user
    or request from Government agencies to revoke Smart Card.
if initiator of transaction is Smart Card issuing agency
then
        Identity Verification << Persons Identity key
        KYC Verification << Persons Identity key
        Police Verification << Persons Identity key
    if all required verification pass
    then
        Smart Card application accepted.
        WriteToBlockchain (Smart Card accepted)
    else if request from Government agency to revoke
    then
        Smart Card revoked.
        WriteToBlockchain (Smart Card revoked)
    else
        Smart Card application rejected.
        WriteToBlockchain (Smart Card rejected)
else
    Invalid transaction
end if
```

Only Smart Card Issuing agency can add or modify the personal details of citizen using this algorithm. The result of this algorithms will be a final single object that will hold all details of a person which can be a source of truth for any public, private and security agencies for verification, current status of a person or any other details.

*ALGORITHM 2 – Querying capabilities from the Blockchain*

```
Require:
    Smart Card details defined and added in the blockchain.
Inputs:
    Person's Identity key provided by the person and
    Querying Agency Details.
Output:
    Person's object consisting of Smart Card
if Querying Agency is having permission
then
    if querying for Smart Card Details
    then
        Return Smart Card details.
    else
        Invalid transaction
    end if
```

This is the logic for querying capabilities that is designed to ensure that only relevant data is retrieved based on the permission level that the agency has.

### *4.3 Development of Smart Contract*

The nodes which are assigned the task of gathering Smart Card information, collects the data from the server of Election Commission. After data collection, the node converts this information into cryptographic hash using SHA-256 hashing algorithm and sends the hash to CA along with the source of the received information, which is Election Commission Server, as a transaction request. The CA receives both the hash and source address from that specific node. Smart Contract in the CA's end contains a method which again collects a person's necessary data from the server, converts it into cryptographic hash and compares between this calculated hash with the received hash. If the two hashes are identical, then the CA provides a validation certificate to that node which ensures the genuineness of the data.

### 4.4 Digital Signatures from CA for Certificate Authentication

Certification Authority provides its digital signature in the certificate of genuineness by encrypting the certificate two times; first encryption is executed using CA's own private key and the second encryption is done using miner's public key. The reason behind the two-time encryption is to ensure both the confidentiality and proper authentication. After receiving the certificate of genuineness from any specific node, the digital signature verification phrase is executed by the authorized miner.

In this step, the miner first decrypts the received encrypted version of the certificate by its own private key and then second decryption is performed using CA's public key.

After all the decryptions, if the miner finds the appropriate certificate information, then the certificate is proved to be signed digitally by CA.

The generation and verification processes of digital signature are illustrated using Fig. 2.

### 4.5 Using Proof of Authority (PoA) as Consensus to Mine Blocks

After receiving the certificate, that particular node requests the miners to broadcast the transaction in the network. A group of miners, whose identities are known and are appointed by the CA, checks if the requesting node contains the certificate of authorization and starts to mine a block which holds a particular person's Smart Card information.

This block is then broadcasted to all the available nodes of the network. There are several algorithms available for consensus purpose to mine a new block, but Proof of Authority (PoA), especially designed for private blockchain system is more popular and secure than Proof of Stake (PoS) and also than the original consensus protocol named Proof of Work (PoW). This PoA is used in the system as it is prone to the 51% attack because of the miners cannot remain anonymous. These miners are determined by the authority/admins of the system. PoA ensures that any malicious behavior noticed from the miners does result in sacking that fraud miner from the network as the identity of the miner is known.

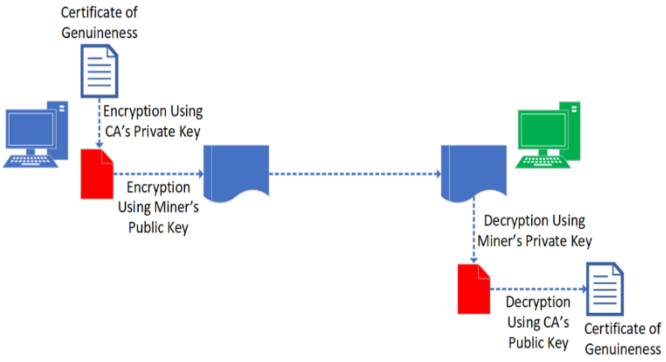

Certificate of Genuineness
Encryption Using CA's Private Key
Encryption Using Miner's Public Key
Decryption Using Miner's Private Key
Decryption Using CA's Public Key
Certificate of Genuineness

***Fig.1:****Generation and Verification of Digital Signature*

### 4.6 Broadcasting the Notification of Successful Transaction Execution using Hyperledger

Hyperledger is a blockchain based platform which is used to develop permissioned and private distributed ledger. One of the useful features of Hyperledger based networks is Event. If some of participating nodes of a blockchain network subscribe to a particular event, they get notified when a particular transaction gets executed. This feature is utilized in the following manner:

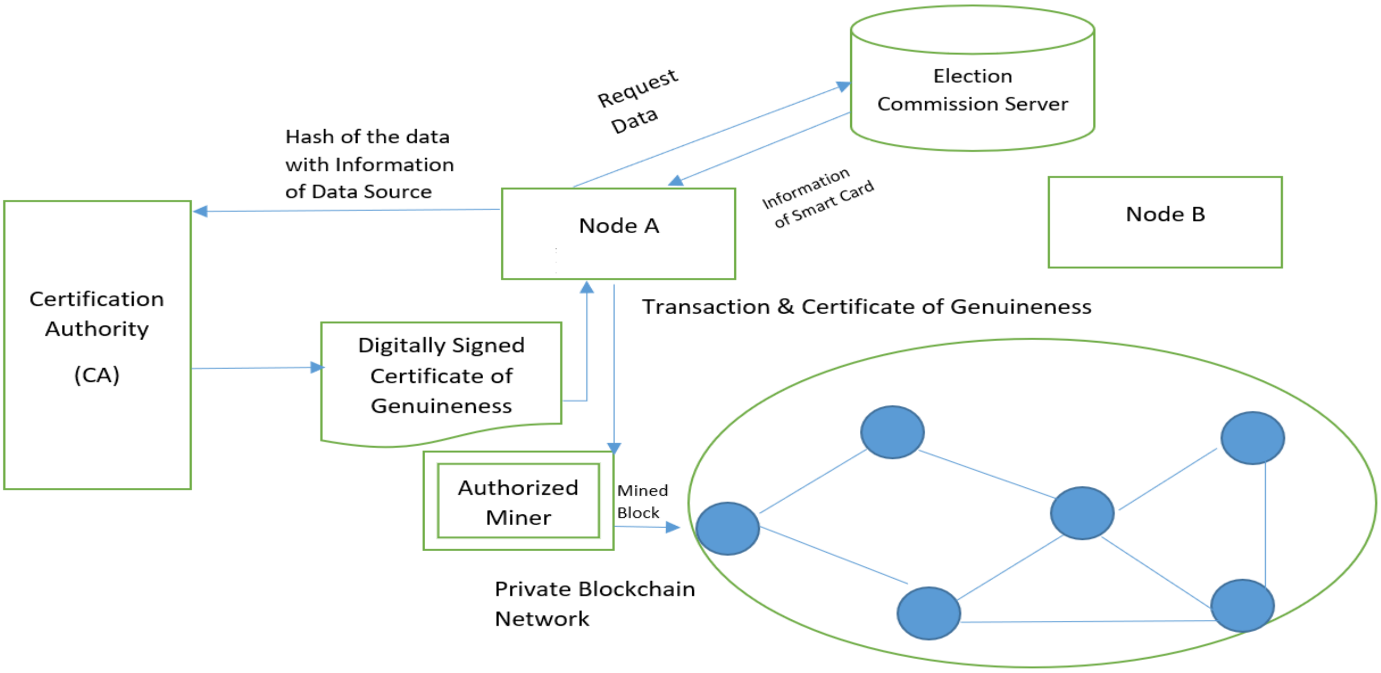

Election Commission Server
Request Data
Hash of the data with Information of Data Source
Information of Smart Card
Node A
Node B
Certification Authority (CA)
Transaction & Certificate of Genuineness
Digitally Signed Certificate of Genuineness
Authorized Miner
Mined Block
Private Blockchain Network

***Fig. 2:*** *Blockchain based Smart Card Information Storing Framework*

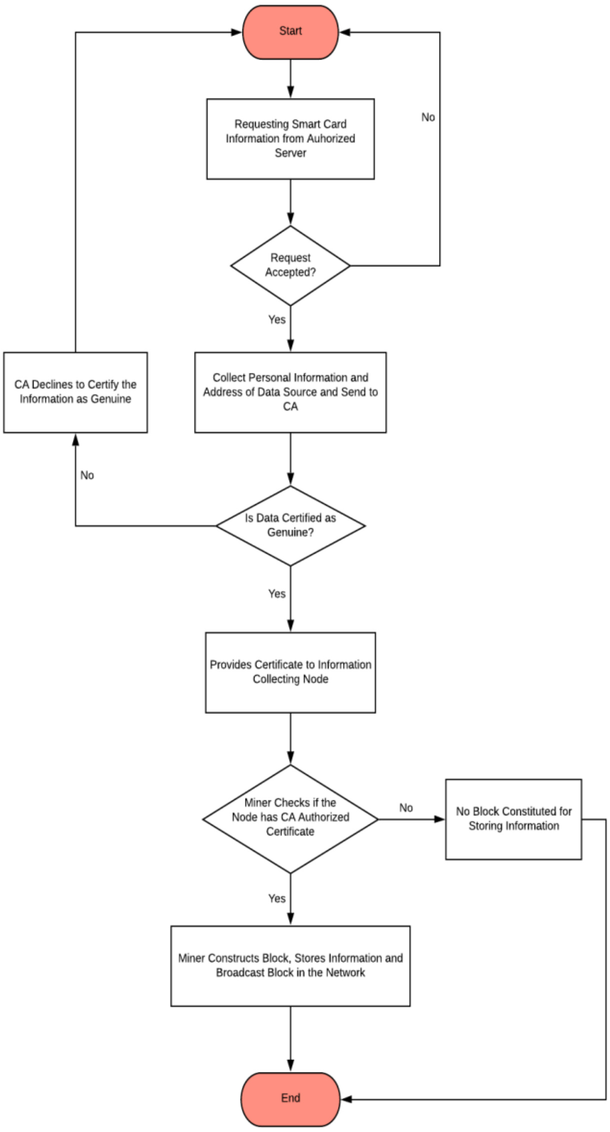
(i) For each of the activities related to the smart card based transactions, an event is created.

(ii) For example: When a smart card is issued, an event against this transaction is emitted and all the participants get notified about this activity.

(iii) Similarly, an event is triggered for updating the information of a particular smart card and thus all the nodes inside the network are notified about this update.

(iv) An event carries some of the necessary information about a specific transaction: type of the transaction, timestamp of the transaction, transaction ID etc.

The workflow of our proposed system is illustrated using Fig. 3.

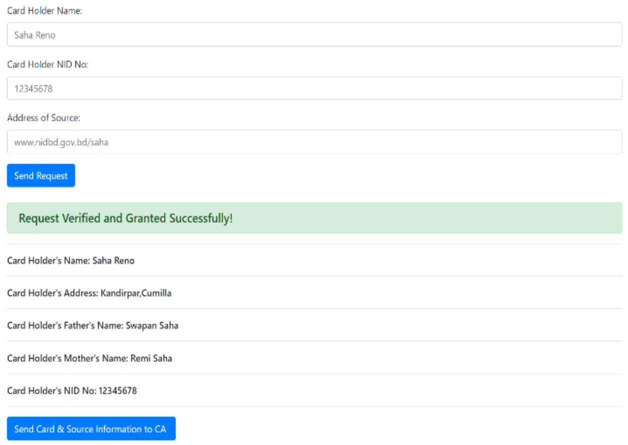


Start
Requesting Smart Card Information from Auhorized Server
Request Accepted?
No
Yes
Collect Personal Information and Address of Data Source and Send to CA
CA Declines to Certify the Information as Genuine
Is Data Certified as Genuine?
No
Yes
Provides Certificate to Information Collecting Node
Miner Checks if the Node has CA Authorized Certificate
No
No Block Constituted for Storing Information
Yes
Miner Constructs Block, Stores Information and Broadcast Block in the Network
End

***Fig.3:*** *Flowchart of Blockchain based Smart Card Information Storing System*

## 5. Result

There are three separate front-ends available for the CA, information collecting node and the accessory of the information stored in the P2P network respectively for the purpose of interaction with the system. Node which serves as data collector requests the server from which the information is collected to send data about a specific person's smart card by providing NID number and the address of that server. If the data source finds the request as a valid one, then it sends the desired information about the smart card to the requesting node. After collecting these data, both the smart card information and source address are sent to the CA by the archivist node for verification and certification purpose. The following figure represents the interactive front-end for the purpose mentioned above.



Card Holder Name:

Saha Reno

Card Holder NID No:

12345678

Address of Source:

www.nidbd.gov.bd/saha

Request Verified and Granted Successfully!

Card Holder's Name: Saha Reno

Card Holder's Address: Kandirpar,Cumilla

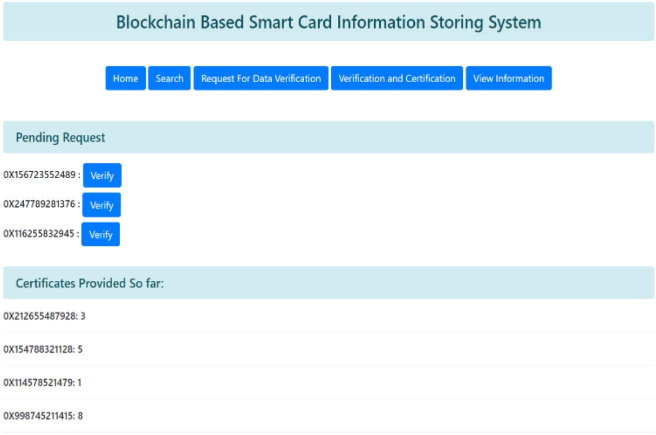
Card Holder's Father's Name: Swapan Saha

Card Holder's Mother's Name: Remi Saha

Card Holder's NID No: 12345678

***Fig.4:*** *Requesting the Server to Send and Retrieve Smart CardInformation*

Various nodes are in charge of data collection and sending the smart card information to the CA. The following webpage informs the CA about the pending authorization requests. Address of each data collector node is displayed



Blockchain Based Smart Card Information Storing System

Pending Request

0X156723552489 :

0X247789281376 :

0X116255832945 :

Certificates Provided So far:

0X212655487928: 3

0X154788321128: 5

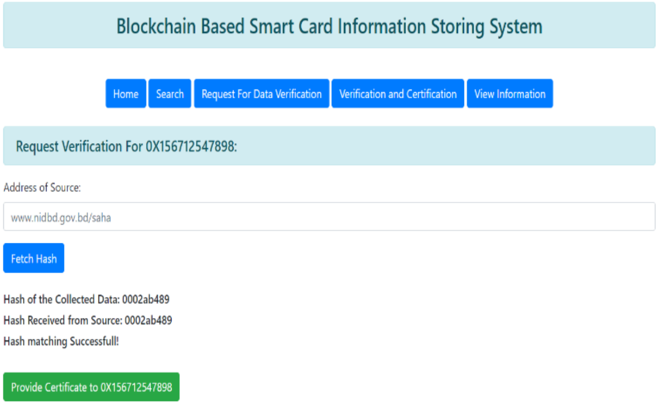
0X114578521479: 1

0X998745211415: 8

***Fig.5:****Observing the Pending Approval Request and Number of Certificates Provided by CA*

and the CA can select an address's request by simply clicking the 'Verify' button, which it wants to certify as a genuine one. This webpage also shows the number of certified requests against each information gathering node.

After clicking any of the 'Verify' buttons, another window pops up, which contains the procedure to verify whether the request is to be certified or not. CA puts the address of the source in the text field and presses the 'Fetch Hash' button to fetch the cryptographic hash of the original data. After retrieving the hash, smart contract which is acting as the back-end of the verification process for CA checks if the hash fetched from the source does match with the hash generated from the downloaded information. If both the hashes are identical, then the smart contract enables the button for providing the certificate to the node gathering smart card information.


Blockchain Based Smart Card Information Storing System

Home
Search
Request For Data Verification
Verification and Certification
View Information

Request Verification For 0X156712547898:

Address of Source:

www.nidbd.gov.bd/saha

Hash of the Collected Data: 0002ab489

Hash Received from Source: 0002ab489

Hash matching Successfull!

Provide Certificate to 0X156712547898

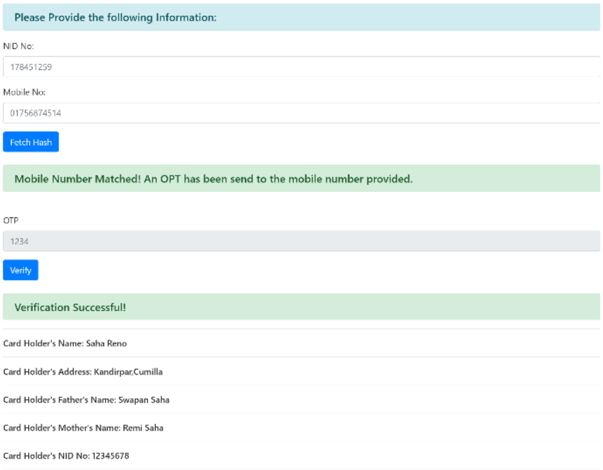
***Fig.6:****Verifying the genuineness of the retrieved data and Providing Certificate by CA*

After checking the validity of the certificate being hold by the node which is requesting the network to broadcast its collected information, the miner mines a block to store the received data and transmits the block to each pair of the node. When the block successfully gets mined, any person can view the recorded information by providing the NID and registered mobile number. An OTP is sent to that cellular number and successful verification of OTP leads the viewer to view overall information about the smart card he/she aspires to.

Our system uses a customized version of Proof of Authority consensus where each authorized miner has their own stakes. These stakes contain crypto currencies which are the miner's reward for successful mining.Miners' reputations are set based on the amount of finances inside their stakes. The selection of a miner to mine a block depends on the miner's reputation.

If some malicious behavior is detected from miner's activity, he/she is penalized and some of the crypto currencies are seized from the miner's stake. As a result, tempering the network will bring financial loss to them and they are discouraged to do any fraudulent activities. This protocol prevents 51% attack in our system by the following means:

(i) To carry out a 51% attack, the attacker must obtain 51% crypto currency of our system. Acquiring this amountofcrypto currencyis expensive and difficult to accumulate.


Please Provide the following Information:

NID No:

178451259

Mobile No:

01756874514

Mobile Number Matched! An OPT has been send to the mobile number provided.

OTP

1234

Verification Successful!

Card Holder's Name: Saha Reno

Card Holder's Address: Kandirpar,Cumilla

Card Holder's Father's Name: Swapan Saha

Card Holder's Mother's Name: Remi Saha

Card Holder's NID No: 12345678

***Fig. 7:*** *Accessing a Specific Smart Card Information from the Distributed Network*

(ii) Moreover, if a miner owns 51% of system's crypto currency, then he/she may face a major financial crisis if the exchange rate of system's crypto currency decreases drastically; which is a common scenario for many crypto currencies.

For the above reasons, it is not feasible for any attacker to execute a 51% attack in our system.

As we have used both Ethereum and Hyperledger for developing a private and permissioned blockchain network for your system, it delivers the following benefits:

(i) Ethereum can be used to develop a system's own cryptocurrency. This customized cryptocurrency is used for the security against 51% attack (which is already discussed above) which increases the scalability of our system.

(ii) As Hyperledger is a private blockchain, the transactions executed inside our system are only visible to the nodes participating in the network. The information about each of the transactions cannot be accessed from outside the network, which is a major disadvantage of public blockchain

(iii) Access control is more reliable and customizable in our system as Hyperledger is exercised. Hyperledger has a wide range of access control mechanism which controls the accessibility limit of the system resources for a particular participant. For example: CRUD operations against the system can be distributed as per the role of a particular node. A node may have access to only RETRIEVE and UPDATE operations, while the nodes at upper tier has access to all the CRUD operations, thus creating a much more reliable and secured network.

(iv) The utilization of Proof of Stake features inside the system's Proof of Authority consensus protocol makes the system more robust than the systems using Proof of Work, by defending major blockchain related attacks (e.g., 51% attack).

## 6. Discussion

In our work, we have constructed a framework consisting of all the securities and advantages provided by the blockchain technology to mitigate the shortcomings of the existing smart card information storing method. Our system is more robust and offers more stability and reliability than the classical one. Inclusion of private and permissioned mechanism makes the system obstructive against different types of attacks observable in public blockchain.

## 7. Conclusion

Although private and permissioned blockchain is used to implement the identification information storing system to overcome various drawbacks of public blockchain, it still has some limitations. Existence of Certification Authority makes the system a bit centralized where most of the decisions are made by this CA. If CA becomes corrupted, then the network will be descended into anarchy. To overcome these problems, further research needs to be done and is open for debate. Afterward, this blockchain based model will surely eliminate most of deficiencies of the existing system by restricting the fraudulent activities done in the classical digital ID information storing method.

## 8. References

[1] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder. “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”. Princeton University Press, 2016.

[2] Yong Yuan and Yuefei Wang. “Development status and prospect of blockchain technology”. Journal of Automation, 42(4):481–494, 2016

[3] Vitalik Buterin. “A next-generation smart contract and decentralized application platform”. Available: https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf/, 2014.

[4] Melanie Swan. “Blockchain: Blueprint for a New Economy”. O’Reilly Media, Inc., 2015.

[5] Alizadeh Mojtaba, A.S., Zamani Mazdak, Baharun Sabariah, Sakurai Kouichi.“Authentication in mobile cloud computing: A survey”. Journal of Network and Computer Applications,2016. 61: p. 59-80.

[6] Shu Yun Lim, M.L.M.K.,Tan Fong Ang.“Security Issues and Future Challenges of Cloud Service Authentication”. Acta Polytechnica Hungarica, 2017. 14(2): p. 69-89.

[7] TheStar, M’sia sees biggest mobile data breach, in TheStar. 2017.

[8] Pete Rizzo. “Blockchain identity startup shocard raises 1.5 million”. 2015.

[9] Sebastian. “What is Onename? how does the web application work?”, May 2016.

[10] Melissa Jun Rowley. “Aiding refugees? yes, the blockchain can do that and more”. aiding-refugees-yes-the-b_b_8149762.html, September 2015.

[11] Sachchidanand Singh, Nirmala Singh.“Blockchain: Future of financial and cyber security”. IEEE Xplore, 04 May 2017

[12] Ethan Heilman, Leen AlShenibr, Foteini Baldimtsi, Alessandra Scafuro and Sharon Goldberg,Boston University, George Mason North Carolina State University.“TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub”. Eprint Publication, Jun 5,2016.

[13] One Ledger IO, “Oneledger: Public Blockchain Whitepaper”. One Ledger, Jun 18, 2018

[14] Xinle Yang, Yang Chen, Xiaohu Chen. “Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information”. IEEE Xplore, Jan 2, 2020.

[15] Dejan Vujiˇci´c, Dijana Jagodi´c, Siniˇsa Randi´c, “Blockchain technology, bitcoin, and Ethereum: A brief overview”. IEEE Xplore, 26 April 2018.

[16] Mixin Network Organization.“Mixin: A free and lightning fast peer-to-peer transactional network for digital assets”. Whitepaper Pagoda, Jun 19, 2018.

[17] David Vorick , Luke Champine.“Sia: Simple Decentralized Storage”. Nebulous Inc, November 29,2014.

[18] Nicolas Van Saberhagen. ”Monero : Crypto V2.0”. Whitepaper Database, October 17,2013.

[19] Gianni Fenu, Lodovica Marchesi, Michele Marchesi, Roberto Tonelli.“The ICO phenomenon and its relationships with ethereum smart contract environment”. IEEE Xplore, 29 March 2018

[20]Medium. Proof of Authority Consensus Model with Identity at Stake. Nov 11, 2017. Available Online: https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

[21] Binance Academy. Proof of Authority Explained. Feb, 2020. Available Online: https://www.binance.vision/blockchain/proof-of-authority-explained

[22] Bitcoin Exchange Guide. ShoCard – Secure Blockchain Digital Identity Privacy Management? July 12, 2017. Available Online: https://bitcoinexchangeguide.com/shocard/

[23] Tokens 24. What is Bitnation? April 23, 2018. Available Online:https://www.tokens24.com/cryptopedia/coinguides/what-is-bitnation