An Interoperable Model For Blockchain Based Passport Information System

Jayashree.A[1], Gayathry.S[2], Rupa kesavan[3]
[1, 2] Dept of CSE
[3]Assistant Professor, Dept of CSE
[1, 2, 3] Prince Shri Venkateshwara Padmavathy Engineering College

Abstract- *This project is a novel innovative methodology for fortifying passport particulars against tampering and misusing from intruders.The proposed system is autonomous of any existing blockchain platform and its truly open to future enhancement .The citizen's vital informations are stored in the blockchain via the blocks which follows the smart contracts. Blockchain eliminates unauthorized access using the cryptographic algorithm SHA-256 .The consensus has a unique hash function ,when a new block is created it will backreference the previous block forming a chain .Modifying any of the block the Proof of Work algorithm putsforth an computationally mathematical puzzle for all the blocks and once a resilence is obtained the transaction is considered valid and the changes are made otherwise the blockchain is infeasible to modify .The main aim of the application is to deliver the needs of the citizen ,the Issuing Authority and the third parties to understand the architecture and to prevent citizen private information against privacy and security.*

Keywords- Consensus, Smart Contracts, Proof of Work, Cryptographic Algorithm SHA-256

I. INTRODUCTION

The growing demand for passport associated services across large and small cities a new secured application is necessary to protect passport information. The various countries across the globe are implementing latest technologies to secure their citizen passport information.These information may appear simple may they are very complex to handle and secure it from hackers.The existing security system uses a centralized server to store the information ,and a trusted third party is necessary to access those information.

But in blockchain the information is stored in a distributed ledger that restricts the intruders from hacking the information. The consensus Algorithm does not rely on a centralized authority whenever an modification is made an acceptable resolution is needed for further processing.

The Proof of Work Algorithm is a concept of solving a computationally challenging puzzle,when a new block joins a blockchain.It needs the participant nodes to prove that the work done qualifies them to give the access to add a new block.Then it connects to available blocks in the chain ,backreference is created so that the block becomes immutable. The main contributions of the project are enhancing transparency ,the Accessibility of the information and the security of the information.

II. PROPOSED SYSTEM

The proposed system is an decentralized methodology providing a secure protocol to handle passport information system using Blockchain.It is a network of nodes enhancing efficiency for creating ,managing and transferring records . The utility and functionality of the proposed system is divided into four components they are

1. Blockchain
2. Citizen Nodes
3. Issuing Authority Nodes
4. Provider Network

The citizen nodes are the end user's records.The Issuing authority has the access to modify the blocks.Provider Network contains the storage manger whose work is to store and maintain the information.The proposed system has the below Smart contracts

1. Citizen Contract
2. Permission Contract
3. Consensus Contract
4. Service Contract

Citizen Contract lists the transaction records that belong to the specific citizen.When the relationship between the blocks are defined the citizen contracts are created.

Permission Contract holds a rundown of reference of providers stating where a client has records with and to get the

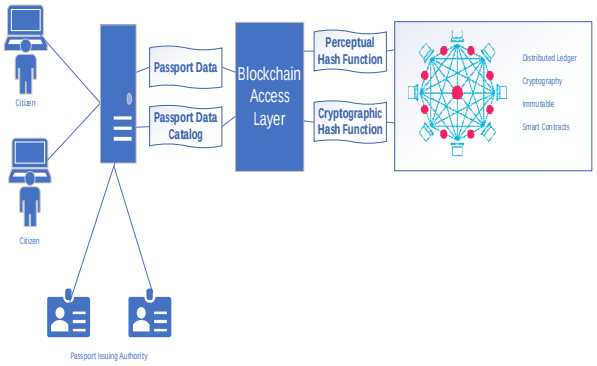
rights that are to be determined by the providers or arrangement.

Consensus Contract is a dynamic way for reaching the agreements among the stakeholders.

Service Contract helps in establishing the chain, helps in agreement records and different connections that are held.

These contracts allows the stakeholders to interact directly without no intermediaries. The transactions are consensus that is in the blockchain all updated are performed via consensus,Central authority has no role on controlling and updating the blocks .The system also uses proof of work algorithm that throws a computationally mathematical puzzle when a block is requested for modification and once a valid solution is obtained the changes are ,made otherwise the blockchain resist to make changes to the records, making them tamper-proof and trusted .

III. SYSTEM ARCHITECTURE



The graphical representation of the architecture includes the principles, elements and components of the proposed system. Here the citizen will initially engage to the passport registration portal and all the citizen details will be stored in the passport server. The passport issuing authority goes for the verification and after checking the credentials the officer approves the request .The verified citizen record is located in the passport data section. The passport Data catalog is maintained for the quick access of the data.

The next part is the blockchain access layer,it partitions the textual data and creates the perceptual hash function and the pictorial data are provided a cryptographic hash function. Then the respective information are stored in blocks, each block is chained with the other block with their hash values. The blockchain overall appears as a distributed ledger.It also follows the smart contracts to manage the blockchain.

IV. EXISTING WORK

In previous studies the citizens record submitted are put away locally at the provider's information system,the administration and support related information are on the provider side,and the provider is given access to alter these records.Likewise ,the providers can also question the records from typical clients when they need.The given access rights to the databases,clients and providers have additionally raised the issues for security and protection of the system..In the above case a trusted third party is needed to verify the documents which is indeed an difficult task.And also all details are stored in a centralized server which is very tough for server maintenance.

V. RELATED WORK

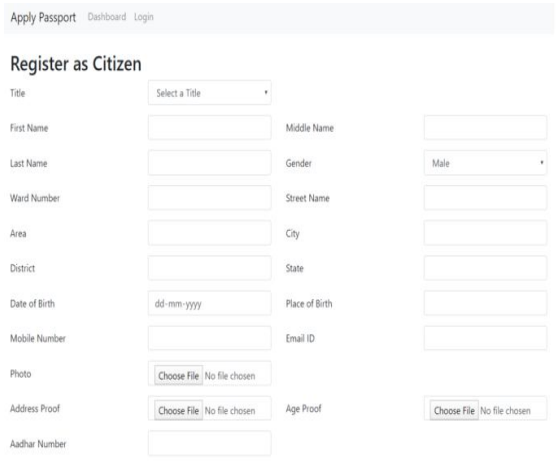
1. A design for photovoltaic plants for financing platform on blockchain that enables customers to do cashless financial transactions with vendors in village.That helps in decentralized verication and become minners,which provides higher efficiency and performance.
2. An application of blockchain technology in accounting field that ensures security for transaction information.It is encrypted with a public key, private key and a secret key.It also followed consensus mechanism to judge the accuracy of the messages.It not only process accounting of accounts but also analysis of financial data.
3. Blockchain in logistics and supply chain were there are few intermediatory third parties allowed with some restrictions to access the data.Ledger data is maintained between the blockchain at matching random intervals which makes the technology secure from hackers.
4. An effective randomization framework for Pow consensus algorithm applied in bitcoin architecture that reduces the execution time required to calculate the hash value.The number of instructions-set required to compute the pow consensus is also reduced.

VI. MODULES

1. Apply for passport
2. Passport Verification
3. Manage Blockchain.

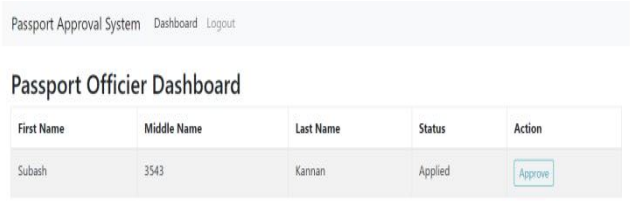
1. Apply For Passport:

The application automates the management of passport administrative tasks for passport issuing office.It is basically an online passport platform through which a web application portal manages citizen database (i.e)public registration,online verification of data anytime ,anywhere.With passport registration the data and files are stored online. Once the registration is completed we can able to track the progress seamlessly.By this way we are in a position to feel,view and control on what is happening in our request.



2. Passport Verfication:

A passport verification software solution can automate the entire process which helps to minimize the errors.The passport verification officer is intimated as soon as a request for new passport comes in and the respective officer logins into the portal with his login credentials and checks on the new request and he is granted to approve or reject or hold on the request depending upon the geniunity of the citizen details.



3. Manage Blockchain:

A passport transaction is a record of the passport data transfer often identified by its hash value. A passport block can contain multiple transactions and they are recorded.The citizen transactions should be valid otherwise it will not included in the blockchain. The passport nodes that check for validity is called as mining nodes. The information of the citizen are put in blocks and these blocks are chained together making the data immutable.When a block is chained to other blocks those data can never be changed.The passport blocks in the blockchain contains specific hash value for each block according to cryptographic algorithm SHA-256.Each block contains an back reference of the previous block .The first node of the blockchain that is mining node,they check for valid transaction in the blocks.When changes happen to a block the hash value of the previous block changes making it immutable

.

VII. FUTURE IMPROVEMENTS

The application can be further enhanced to support the below mentioned public sector departments:

1. The government certificates(i.e) the birth and death certificates.
2. Citizen services.
3. School certificates.
4. University degrees.

VIII. CONCLUSION

The blockchain-based passport system that we have introduced, uses consensus that enables secure and cost-efficent process while ensuring public privacy.Blockchain technology offers the possibility to overcome the limitations and adoption barriers in implementing the passport security, enhancing integrity and lays ground for transparency.So that , the countries of greater size would be supported with greater throughput.

REFERENCES

[1] Marco Conoscent , Antonio Vetr` and Juan Carlos De Martin ,"Blockchain for Internet of Things"(2016).
[2] Konstantinos Christidis and Micheal Devetsikiotis, "Blockchain and Smart Contracts for the Internet of Things"(2016).

[3] Arman pouraghily, Md nazmul Islam ,Sanidip Kundu and Tilman Wolf,"Poster Abstract:Privacy in Blockchain-Enabled Iot Devices"(2018).
[4] Zibin Zheng,Shaoan Xie,Hongning Dai,Xiangping Chen and Huaimin Wang,"An Overview of Blockchain Technology:Architecture,Consensus, and Future Trends(2017).
[5] Llya Sukhodoiskiy and Sergey Zapechnikov,"A Blockchain-Based Access Control System for Cloud Storage(2018).
[6] Sumathy Kingslin and Rafath Zahra,"An Effective Randomization Framework to POW Consensus Algorithm of Blockchain[RPOW](2019).
[7] Yuqi Huang,Ping Yang, zejian Liu and Yuhua Lyu,"A Design of Photovoltaic Plants Financing Platform Based on Blockchain Technology(2018).
[8] Guido Perboli, Stefano Musso and Mariangela Rosano,"Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases(2018).
[9] Aino Nordgen ,Ellen Weckstrom,Minna Martikainen and Othmar M Lehner,"Blockchain in the Fields of Finance and Accounting(2019).
[10] N.S Tinu " A Survey on Blockchain Techology-Taxonomy,Consensus Algorithms and Applications(2018).