Personalized Secure E-Identity Card

Varun Potluri, Karthik Veerla, Ganesh Tummala

Abstract- Blockchain technology is a new technology in digital platforms for making transactions in a decentralized manner. Blockchain is used for last some year for bitcoin. over the last ten years, the record-keeping technology Bitcoin network behind it named as is blockchain. Each block has a cryptographic hash of the preceding block, a timestamp, and a transaction are all included in the blockchain. As a result, it is noticeable for security on an identity card. If we implement blockchain technology for digital identity card it is very secure for the user. Identity card has personal information and some important information included. The identity card like aadhar card, pan card, Passport etc. are have lot personal and important information, if we are not use securely then it will use for any illegal work so it is harmful to keep our identity card in non-secure storage. Now these identity cards are stored in file with encryption method which will hacked by hackers. So we propose our system for blockchain technology is used for identity card using. In our proposed system we are using blockchain and IPFS server which is immutable server which helps us to system will more secure. Once one transaction will have done before the transaction the block will be created which is hash of information like date, time etc. and this block send to blockchain which will maintain all block. For implement the blockchain we will use Ethereum platform. This solution is secure and more trusted than traditional models.

Keywords- Blockchain, Identity card, IPFS server, Ethereum.

1. INTRODUCTION

Blockchain is an new and growing technology. In recent years, it has been applied to almost any major area which benefits human life, not only just financial use cases. It includes wellness, gaming, government systems, software/electrical engineering, and a variety of other fields.

Blockchain with personalized identity card: An new approach for personalized secure identity system which is implemented by the use of blockchain and IPFS server as a new trend. The user ID is stored and can be retrieved using blockchain. In order to access user ID a Block can be retrieved and checked. It is also secured and encrypted by implementing blockchain both internally and externally; internally for access to the list and externally for identity monitoring.

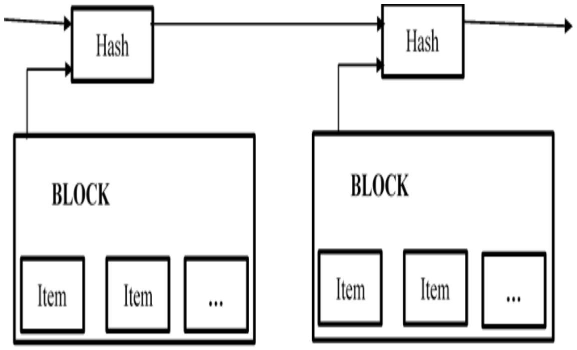
Blockchain is a decentralised and distributed ledger that has had a significant impact on money use cases (such as remittance) and business use cases over the last few years (e.g. documents). Users of blockchain-based applications have the ability to add their data to this distributed ledger. sers would have faith in the blockchain because it uses consensus mechanisms to verify and collect transactions into blocks. Blockchain, in addition to being a distributed ledger, is often thought of as an open ledger

where online transactions are registered and users can link, submit, and validate their transactions.

Without involving any central hub or authority, decentralised operations are also known as user to user or peer to peer operations. The term "transparency" refers to the data being publicly embedded in the network. Security provides encryption technology that works for both public and private keys. The public key in bitcoin, for example, is the user's address, while the private key is a password to access the transaction. Here are some of the Blockchain’s benefits and drawbacks. They're important to think about when creating blockchain-based applications. It's also worth noting that, due to its benefits, blockchain is assisting society/humans in a variety of ways. Its drawbacks are the lack of certain features.

1.1 Blockchain technology

Blockchain may be a one-of-a-kind technology that enables new distributed software architectures, there are some other components that can able to get the agreements which are coming from the shared of the. Blockchain is not a Complex technology, But why such a technology called a Blockchain that is what we have to Find Out so to easy way to Understand there are Series of Blocks where is No other sense of these Words. sometimes we have to understand the “Block” and “Chain”. We know when we talking about blockchain when we are working on Digital Data or in different words Digital Information, block can be get as Public Databases are understood by chains. Cryptocurrencies, Thanks to their promising use of the technology, blockchain applications have become a big phenomenon in the last year. Bitcoin [6] is the biggest and most important of them all, and it, as well as newer currencies such as Ethereum, is currently on the forefront of cryptocurrency industry, There were 1,600 distinct currencies and a market capitalization of about a trillion dollars. last year but is now over 300 billion as defined in Satoshi Nakamoto's original Bitcoin paper [6].The Blocks Records or store the Information who is taking part in the Transaction, A Block is which is Sufficient for your Splurge Purchase from E-commerce Website which record or Saved your name along with the E-commerce Name, The Ecommerce Website will never record your data with your Actual Name rather they Store there with your Unique Information such as Digital Signature or Particular ID The Information stored in each block like the Every Information which Different which is than Other Blocks like in some cases Like if you and your friend have same Names each Block stored in a simple way called Hash and that helps to know the Difference from other Block, Lets understand with an Example You have Purchased a two similar Transactions , You as a User of that E-commerce Website will never Understood the Difference Between both transaction but each traction have each Block because of that Unique Code . The network itself necessitates a bare minimum of structure. Messages are sent with the greatest care possible, nodes can join and depart the network at any time, with the longest proof-of-work chain acting as evidence of what transpired while they were gone. The Blockchain concept is implemented and used by Bitcoin to allow transactions to be recorded authenticated the majority of people of computational. Every transaction is checked and confirmed by the majority of network nodes that are actively computing transactions in a network. The transactions that have been validated are then piled in a non-changeable order. As a reward, all computers that used computing resources to validate a data block earn some cryptocurrency. As a result, all transactions are verified by a large number of machines. It's impossible to tamper with a transaction's authentication since gaining control of the bulk of the network's verification technique would necessitate an unsustainable amount of processing power.



1.2 Aim of Project

This project's aim is to use blockchain technology and the IPFS server to solve the problems with the current system by increase the protection of user documents, and increase transparency in the system. The aim of this research is to decide how to use blockchain as a service to implement a distributed system.

The authority supplies the user with a digital certificate that uses digital signature technology to validate the user's identity and enable network access.

1.3 Objectives of the Project

The objectives of the systems development and event management are:

1. The authority issues the a digital certificate that uses digital signature technology to validate the identity of the user identity and grant access to network services.
2. Upload documents on ipfs server and maintain the blockchain.

1.3 Scope of the Project

Many companies and universities in Europe and beyond are becoming increasingly interested in blockchain technology. Blockchain, a relatively new advancement in computer science, is a global, cross-industry, and disruptive technology that will accelerate over the next few decades, worldwide economic growth is expected.

In current days' lot of system providing secure storage to store documents but in this systems no transparency is provided to store our personal documents, So, we provide secure system using blockchain technology.

These systems are being developed to address this problem despite the fact that security concerns remain. Blockchain is a relatively new technology that can be used to improve data protection. The block chain's immutability aids in overcoming the problem of certificate forgery.

1.4 **Methodology**:

For develop this system we will use JAVA technology for backend and ui. We use IPFS server for store the encrypted data. For blockchain platform we will use ethereum. In this system when user will upload identity card it will encrypt using encryption algorithm.

2. PROBLEM DEFINITION

2.1 Problem Statement

Nowadays documents are extensively required for any Official/Government work or schemes may it be for admission in school/college or opening a bank account or take benefit of government schemes. As some of the documents like Aadhar card, Passport etc contain sensitive information, it's a big threat for data security and privacy. Moreover, it's also difficult for the ordinary public to keep safely together and manage the physical copy of all the documents.

2.2 Existing System

In Existing System, the documents are stored in centralized system which not much secure. May be it will hack and break the security which is harms whole user's data.

2.3 Disadvantages of Existing System

1. Centralized architecture.
2. Lot of fraud because lack of transparency.
3. Not trustworthy.

2.4 Proposed System

In proposed system, we are using blockchain and IPFS server which is immutable server which helps us to system will more secure. User first register in this system then he/she will upload documents, before uploading the document the system will encrypt the file and encrypted file will uploaded to ipfs server and same time transaction hash code maintained by ethereum.

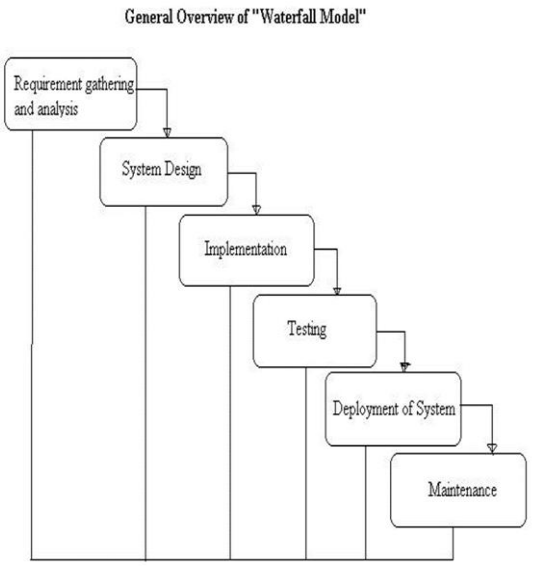
2.5 Advantages of Proposed System

1. Every document on Blockchain is 100 per cent verified:
2. Organizations can quickly create and integrate blockchain applications using any traditional front end development platform without having to understand the underlying blockchain technology.
3. It improves the accuracy of result.

3. PLANNING

3.1 Software development life cycle

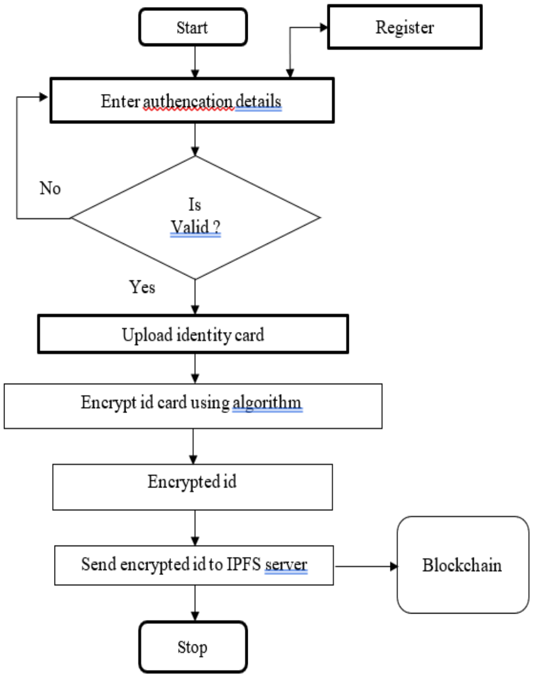
The entire project spanned for duration of 6 months. In order to effectively design and develop a cost-effective model the Waterfall model was practiced.


General Overview of "Waterfall Model"
Requirement gathering and analysis
System Design
Implementation
Testing
Deployment of System
Maintenance

3 DESIGN & IMPLEMENTATION

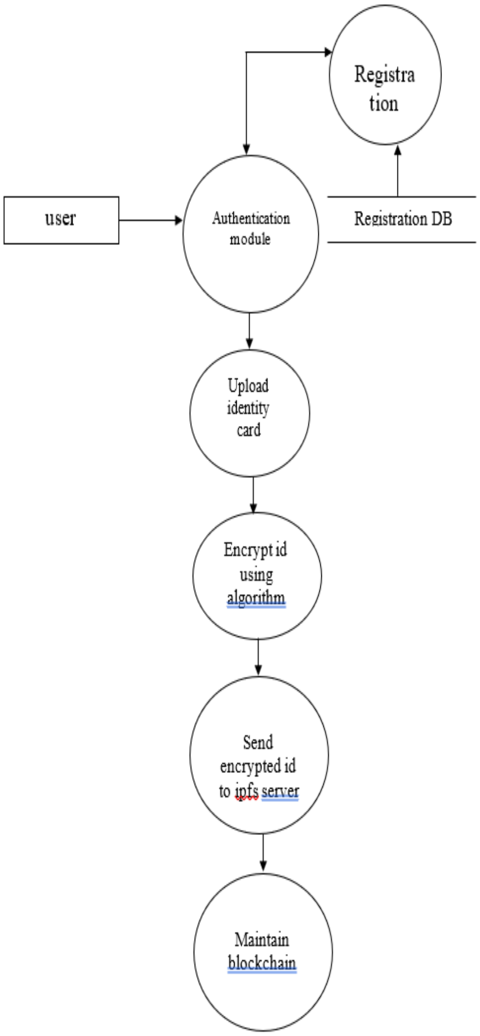
3.1 Flowchart

A flowchart is a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by Arrows are used to connect them. A solution to a problem is depicted in this diagrammatic representation. These boxes and arrows do not represent process operations; rather, they are indicated by the order of operations. Flowcharts are used in a variety of industries to analyse, create, document, and manage a process or programme.

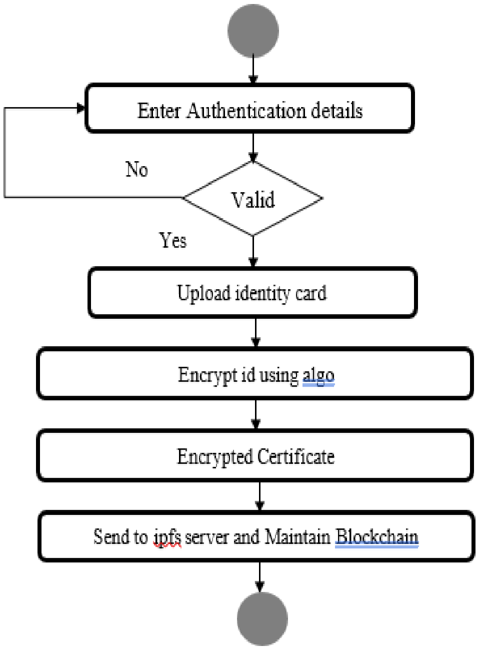

Start
Register
Enter authencation details
No
Is Valid ?
Yes
Upload identity card
Encrypt id card using algorithm
Encrypted id
Send encrypted id to IPFS server
Blockchain
Stop

3.2 Data Flow Diagram(DFD)

In an information system, a data flow diagram is a graphical depiction of data flow. It's also possible to utilise a data flow diagram to visualise data analysis. It is standard practise for a designer to first create a context-level DFD that depicts the path and external entities. This context-level DFD is then exploded to reveal further information about the device under consideration.



3.3 Activity Diagram



4 FUTURE MODIFICATION

In the future, we can work on the Real Life Environment to test the prototype, which would include HEIs, students and companies. The way we present our Concept could be further validated. Furthermore, we can modify this framework blockchain such that each course is allocated a unique blockchain address and a pool of tokens. We will enhance security in the future by using biometric authentication.

5 CONCLUSION

The proposed system would use blockchain technology to help build a trustworthy version that will be used in higher credit and grading systems in education As a demonstration of idea, we demonstrated a prototype implementation of the system framework, which is based on the open-source Ark blockchain platform. Thus by using the Personalized Secure E-Identity Card, users will be able to safely submit documents to various institutions/ Government bodies without the fear of data theft. Users are now free from the fear of losing the documents as they will be stored in digital format.It will also facilitate the user to personalize the card with only the required documents providing the feature of addition or deletion of a document.

6 REFERENCES

[1] C. K. Wong and S, S. Lam “Digital signatures for flows and multicasts”, WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.

[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: 2015, O'Reilly Media.

[3] B Department of Distribution Management, Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology, "Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[4] Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349

[5] P. C. van Oorschot and J. Clark, “SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements,” IEEE S&P'13, 2013, pp. 511–525.

[6] D. Choffnes, D. Levin, and others, L. Zhang, D. Choffnes, D. Levin, and others, “Analysis of SSL certificate reissues and revocations in the wake of Heartbleed,” in ACMIMC'14 Proceedings, November 2014, pp. 489–502.

[7] R. Ford and M. Carvalho, “Moving-target defenses for computer networks,” 73–76 in IEEE Security & Privacy, vol. 12, no. 2. Mar.-Apr.2014.

[8] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.

[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, “Rbac standard rationale: Comments on ” a critique of the ansi role-based standard

access control”, ”IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.

[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy-preserving access control model based on blockchain technology in iot,” Advances in Information and Communication Technologies in Europe and the Middle East and North Africa. 523–533 in Springer, 2017.

[11]L. Y. Chen and H. P. Reiser, “Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, june 1922, 2017.” Springer, 2017.

[12]Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

[13] M. Warasart and P. Kuacharoen, “Paper-based Document Authentication using Digital Signature and QR Code,” no. Iccet, 2012.

[14] J. van Beusekom, F. Shafait, and T. M. Breuel,“Text-line examination for document forgery detection,” Int. J. Doc. Anal. Recognit., vol. 16, no. 2, pp. 189–207, 2013.

[15] Mahamat, M. B. (2016), A Web Service Based Database Access for Nigerian Universities’ Certificate Verification System.

[16] Osman Ghazali, Omar S. Saleh, “Cloud Based Graduation Certificate Verification Model”.

[17] Dr. David Argles, Lisha Chen-Wilson, "Towards a Framework of A Secure E-Qualification Certificate System."

[18] “Blockchain and Smart Contract for Digital Certificate,” by Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen.