

<<Implementation Block chain for personal data>>

By

[Yash R. Sompura

19MCA067]



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Ahmedabad 382481

[Implementation Block chain for personal data]

Major Project/Internship Report

(Major Project for MCA-VI and Internship for MCA-IV)

Submitted in partial fulfillment of the requirements

For the degree of

Master of Computer Application

By

[Yash R. Sompura

19MCA067]

Guided By

[Dr. Devendrasinh Vashi]

[DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING]



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Ahmedabad 382481

CERTIFICATE

This is to certify that the major project entitled “[Implementation Block chain for personal data]” submitted by [Yash R. Sompura (19MCA067.)] towards the partial fulfillment of the requirements for the degree of Master of Computer Application of Nirma University is the record of work carried out by him/her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination.

[Dr Devendrasinh Vashi]

[Assistant Professor]

Computer Science and Engineering Dept.,

Institute of Technology,

Nirma University,

Ahmedabad

Dr Madhuri Bhavsar,

Professor and HOD,

Computer Science and Engineering Dept.,

Institute of Technology,

Nirma University,

Ahmedabad

Dr Rajesh N. Patel
Director
Institute of Technology
Nirma University,
Ahmedabad

Statement of Originality

I, Yash R. Sompura, roll no: 19MCA067, give undertaking that the Major Project entitled “Implementation **of Block chain for personal data**” submitted by me, towards the partial fulfilment of the requirements for the degree of Master of Computer Application of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place:

Endorsed by

DR. Devendrasinh Vashi

Project Guide Name

(Signature of Guide)

ACKNOWLEDGEMENT

I would like to express my gratitude to Dr. Devendrasinh Vashi (Department of Master of Computer Application) for his unwavering and unbiased support during the whole research and development time, as well as for guiding me throughout the Major project phase. They created a conducive climate for me; without them, I would not have been able to attain my goal. Despite their busy schedules, they were always there for me and a fantastic source of inspiration. They were widely accessible both during and after college hours. That is something for which I am grateful.

I would also like to extend my gratitude to our Head of department Ma'am Dr. Madhuri Bhavsar and our Director Sir Dr. R. N. Patel for providing me with all the facilities that were required to complete this project.

I feel a mixture of appreciation, delight, and tremendous satisfaction as I express my gratitude to all individuals who have contributed directly or indirectly to the project's successful completion.

ABSTRACT

Block chain is a cutting-edge computing paradigm distributed data storage, peer-to-peer transfer, and consensus processes and other types of digital encrypted data computing technologies into a single system. It is decentralized, secure, and open to the public. The block chain is highly reliant on digital encryption. The security of user identity and transaction data is a prerequisite for block chain adoption. Block chain technology is both improved and harmed by advances in encryption technology. Hash functions, asymmetric cryptosystems, and digital signatures are briefly discussed on the basis of encryption. It indicates the presence of cryptography across the block chain system. The current state of block chain security is examined, and future research directions are anticipated.

Objective

The goal of the block chain for personal data is to allow for the distribution and storage of information while preventing unauthorized editing. As a result, the block chain created is immutable and irreversible, as the completed transactions are neither deleted or changed. Because this block chain is for private data, there is a system in place to ensure that the data or hashed data (which is irreversible) is never erased. Because the data is hashed and the block is hashed, the chain has double security, making the data safe and indestructible to attackers. This aids the block chain's passive security once again.

Scope

As we all know, the future of block chain technology is mostly in the sector of cybersecurity. Furthermore, despite the fact that the block chain is open source, it nevertheless manages to keep data private through the use of security settings and verifiers. Data is encrypted to eliminate risks from unwanted data tampering and to avoid data breaches to a large extent. When it comes to personal data on the block chain, data privacy is critical, as data leakage is unacceptably dangerous for private information. The hashed data hides the original information. However, the hash of the block protects the block from attack, giving the data double security. This sort of security mechanism is being considered in the project in order to make data transfer very safe for personal data via peer-to-peer transmission.

TABLE OF CONTENTS

No.		Name of Content	Page No.
1		INTRODUCTION	
	1.1	Project Profile	9
	1.2	About the Organization	10
	1.3	Introduction to block chain	11
2		SYSTEM STUDY AND ANALYSIS	
	2.1	Problem Statement	12
	2.2	Feasibility Study 2.2.1 Operational Feasibility 2.2.2 Technical Feasibility 2.2.3 Financial Feasibility 2.2.4 Scheduled Feasibility 2.2.5 Modules of project	12 14
3		DEVELOPMENT ENVIRONMENT	
	3.1	Programming Environment 2.3.1 About Front-End 2.3.2 About Back-End	16
4		SYSTEM DESIGN AND DEVELOPMENT	
	4.1	State of Art (parameters)	17
	4.2	Gantt Chart	18
	4.3	Data Dictionary	18
	4.4	Diagram's 4.4.1 System Flow Diagram 4.4.2 Class Diagram 4.4.3 Context Diagram 4.4.4 DFD level 1 4.4.5 DFD level 2 4.4.6 User Manuals	20 21 22 22 23 24
5		TESTING	
	5.1	Functionality Testing	28

6		CONCLUSION AND FUTURE ENHANCEMENT	
	6.1	Conclusion	30
	6.2	Future Enhancements	30
7		BIBLIOGRAPHY & REFERENCES	
	7.1	Books References	31
	7.2	Web References	31
8		Plagiarism Screenshot	32

Chapter – 1 INTRODUCTION

1.1 Project Profile

Project Title	Implementation Block chain for personal data
Frontend	HTML, BOOTSTRAP
Backend	PYCHARM:- 2022.1 (python):- 3.8
Enrollment No	19MCA067
Name	Yash Sompura
Company Name	Institute of technology Nirma university
CompanyAddress	Nirma university SG. Highway Opposite SGVP
Internal Guide	Dr. Devendrasinh Vashi

1.2 About the Organization:

- Nirma University's Institute of Technology, founded in 1995, is a renowned educational center that offers diverse undergraduate, postgraduate, and doctorate programs in Engineering and Technology.
- The National Institute Ranking Framework (NIRF-2020) **places** the Institute at number 131 out of over 4,000 engineering colleges throughout the country.
- The Institute is routinely ranked first in the state and among the top 15 self-financed universities in the country by prominent rating organizations.
- The Institute is known for its artificial intelligence and machine learning capabilities, and it has partnered with the State University of New York at Binghamton to form a Data Science Center of Excellence as well as a Robotics and Automation Center.
- For More Details: - <https://technology.nirmauni.ac.in/>

1.3 Introduction of Block chain: -

A block chain is a distributed database, which means that the database's storage devices aren't all connected to the same Computer system. It keeps track of a growing set of organized records known as blocks. A date and a timestamp are to be connected with each block of previous block.

A block chain is a collection of data-storing blocks. Santoshi Nakamoto created block chain in 1991. A block chain is a publicly accessible ledger. After data has been placed in a block chain, it is exceedingly impossible to change it. Block chain is a distributed database with qualities such as decentralization, traceability, non-tamper-ability, security, and reliability.

Block chain, is a representation of a database with a large number of users, keeps all transaction information on the block chain, which has stringent security standards. Block chain is a peer-to-peer independent network. There is no requirement for nodes to trust one another, There is also no primary node. As a result, transactions on the block chain must protect the confidentiality of transaction information through insecure networks while simultaneously maintaining transaction integrity.

Chapter – 2 System Study and Analysis

2.1 Problem statement: -

For to store digital data/Record for security it requires block chain expertise to update. More expensive to handle. Overcome to this problem block chain for personal data comes into picture, in this we can store data into the block chain with hiding important details for security of the user with the Masking method with its timestamp, date, hash data or encrypt data of the blocks.

2.2 Feasibility Study: -

To find the optimum system that matches performance criteria, a feasibility study is conducted. A feasibility study is intended to give a broad overview of the major difficulties surrounding a company concept. The goal is to determine any "make or break" difficulties that might put your company out of business in the marketplace, you'll be successful. In other terms, a feasibility study examines if an idea is practical. whether the concepts are coherent The feasibility study gives a wealth of data for the business strategy. To determine the project's feasibility, for example, a wide market is needed. This data serves as the foundation for the market part of the report business strategy.

2.2.1 Operational Feasibility:

The proposed system will meet the operational requirements like system Transaction of data in blocks and in full block chain, date, Timestamp, hashed data/encrypt and user can transact the data into the blocks with the help of Masking method for hiding the personal data. If user has some knowledge of Block chain, user can operate this application easily. It provides easy user interface. From the user's perspective, operational feasibility has been examined. This application once deployed, can run easily without any maintenance at this point of time.

2.2.2 Technical Feasibility:

The system is a flask-based simple web application. System can be accessed in any platform has little consideration for the open source community or Microsoft Technology, only thing needed is that Python (PY-charm) Framework must be installed at application system. I am able to perform the task on time. This system can be simply supported by any system's hardware and software needs. The system can also produce its required output. The proposed system must provide Transaction of data in blocks and in full block chain, date, Timestamp, hashed data/encrypt and user can transact the data into the blocks with the help of Masking method for hiding the personal data. Technical guarantees include accuracy, reliability, accessibility, and data security.

2.2.3 Financial and Economical Feasibility:

Economic feasibility addresses to the following issues: Software resource requirement of the proposed system is Python(PY-charm) Framework that are our organization already owns them and there is no need for extra investment. The advantages accrue as a result of declaring the system financially sustainable from the system has to be related in comparison to the expense of developing the system. It needs the Flask server which can run this system which is already company has. The hardware requirement of the system is at least a PC for an administrator to handle the web application. The project's development costs are not vastly larger.

2.2.4 Schedule Feasibility:

Typically, this means estimating how long will it take for the system to work and develop, and if can be completed in a given time period using some methods like payback period. The schedule feasibility of a project determines how timely it is. Are the project timeframes acceptable, considering our level of technical knowledge? Some projects are initiated with specific deadlines. It's important to figure out if the deadlines are required or desired.

2.2.5 Modules of the project:

1) **Transaction:** - In this project the transaction function to initialize new transaction of data of our block chain. On-chain transactions occur in a block chain update after being validated or authorized.

- **Proof of Work:** - In this it will validate the block chain by consecutive blocks with the help of proof of last block. This method will be used to confirm the transaction, produce additional blocks in the chain, and compete against one another to finish the network transaction.
- **Consensus method:** - we have used this function to verify or check in proof of work that the chain has been replaced or not of data.

2) Administration: - In this we have developed a UI for the block chain.

- **Full chain:** - In this it will show the all transaction of the chain with its timestamp, full block hashed data, date, node etc
- **Last block:** - In this it will mine the data with the previous block with its hash key.
- **Data Allowance:** - In our project the data allowance is used for to check the datatypes of the row which user selected (STR, INT, Float) for respective hidden columns.
- **Security:** - For the security we have used SHA-256 for to create a hashed data or encrypt data of all row in the column and also we have created a particular encrypt data for the whole single block.
- **Masking:** - we have done masking when the user selects the particular columns from the check box it will hide the data in the blocks.

3) Data set: In this we have created dynamic data for CSV formats so
So we can add any of the data set of CSV for data input
into the blocks of block chain.

Chapter-3 Development Environments

3.1 Programming Environment:

3.1.1 Front-End:

- **HTML:** - The coding used to organize a webpage and its content is known as HTML. HTML is widely used to format web pages utilizing the language's many tags. If you know HTML well, you can edit an existing web template to build a website.
- **Bootstrap:** - Bootstrap is a popular front-end tool for building cutting-edge websites and apps. It's free and open source, and its main goal is How use the color, size, font, and layout options in Bootstrap to a web project.

3.1.2 Back-End:

- **Python:** - Python is a high-level, interactive, and object-oriented scripting language. We have use Python for back-end purpose in this we get easily inbuilt Libraries for user needs. Python operates on a wide range of hardware platforms and offers a consistent user interface.
- **Flask:** - Python-based Flask is a micro-web development framework. Flask is a simple and lightweight Python framework for web development. It provides developers more dynamic and is therefore new developers more easy accessibility because You may easily create a web application and fast with only one single python file.

Chapter-4 System Design and Development

4.1 State of Art (Parameters: - Node latency, Block chain scalability, Transaction and Consensus, Centralization)

Author	Year	Parameters comparison				Key Contributions
		1	2	3	4	
Angraal et al.	2017	N	Y	Y	Y	The security of block chain transactions and scalability for decentralized systems is challenging to achieve.
Crosby et al.	2015	N	Y	Y	Y	For a decentralized or partially centralized block chain, distributed consensus will revolutionize our digital world.
Garry Gibson	2020	Y	Y	N	Y	Data transfer utilizing secure block chain (bitcoin's block chain) in a peer-to-peer format at a low cost.
Dansehgar et al.	2018	N	Y	Y	N	The block chain technique enables the hash value to be checked for security with distributed consensus and scalability for data transaction loads.
Marbough et al.	2020	Y	Y	N	N	Every node on the block chain is required to keep all approved transactions, which presents a problem. Because the block size and time interval asked to generate new blocks are restricted, this is a difficult task.
Proposed	2022	Y	Y	Y	Y	The centralized block chain with user end node latency accepts transaction that are in a queue for just user end node latency to be countable for any data set size.

4.2 Gantt Chart:

	Month 1		Month 2		Month 3		Month 4	
Requirement Gathering								
Research Work								
Designing								
Coding								
Testing								
Completing documentation								
Final Presentation								

4.3 Data Dictionary:

Hidden data details

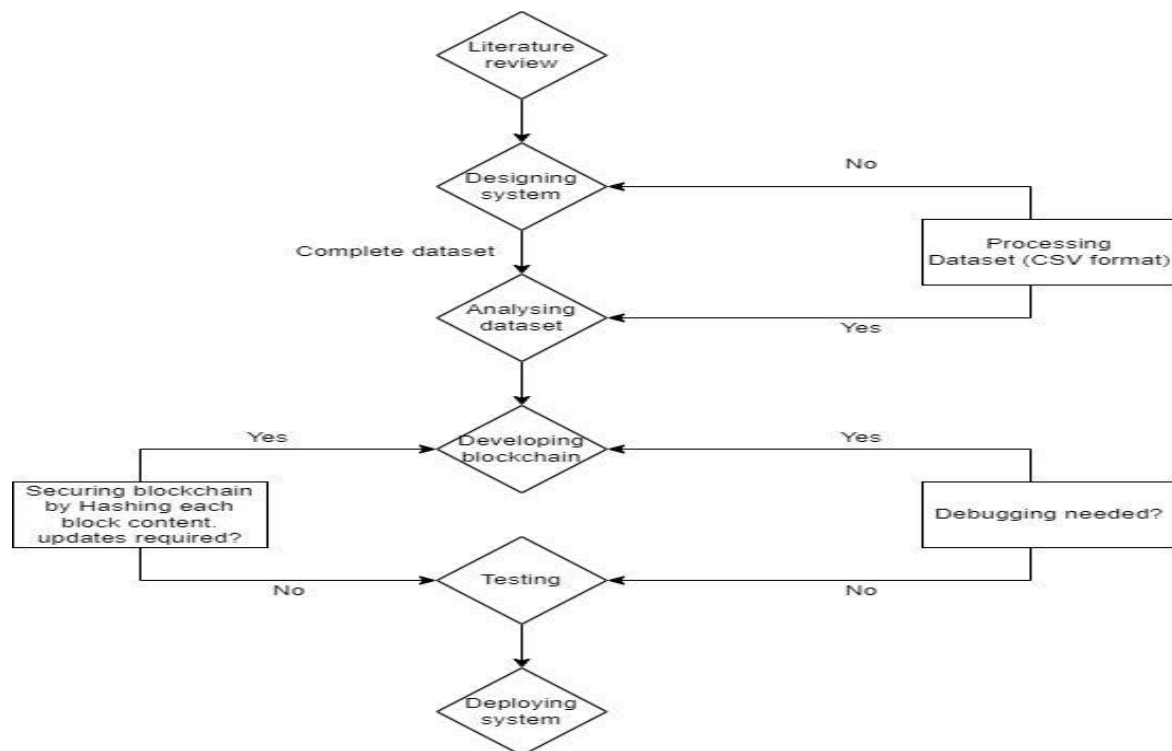
No.	Fieldname	Field type	Field size	Constraint	Description
1	User_id	Int	10	Primary key, Auto Increment	Unique id for user
2	Contact_no	Long Int	10	Not Null	User contact no
3	Email_id	VARCHAR	128	Not Null, Foreign Key	Email of user
4	Password	VARCHAR	16	Not Null	Password of user
5	Account_no	VARCHAR2	64	Not Null	Bank a/c no of user
6	Address	VARCHAR2	256		Address of the user
7	Issued	Boolean	2	Not Null	sanction or not
8	Cast	VARCHAR	32		Cast of the user

Displayed data details

No.	Fieldname	Field type	Field size	Constraint	Description
1	Age	Int	3	Not Null	Age of the user
2	Gender	VARCHAR	16	Not Null	Gender of the user male/female
3	Cast	VARCHAR	32	Not Null	Cast of the user
4	Marks	Int	4	Not Null	Marks obtained by the user
5	Time	Timestamp	8	Not Null	Check the time
6	IFSC code	Long Int	128	Not Null, Unique	IFSC code of user bank

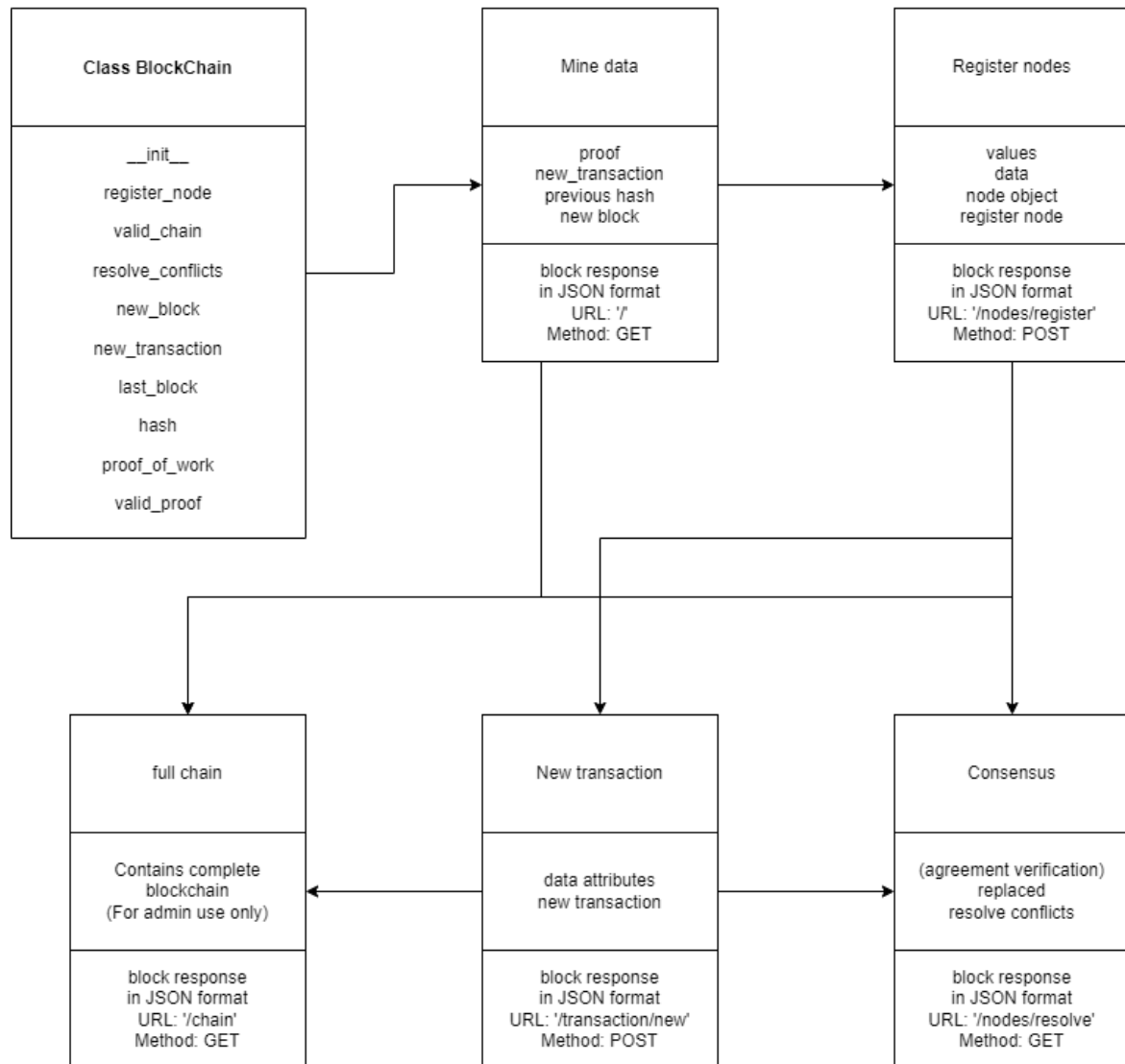
4.4 Diagram

4.4.1 System Flow Diagram:

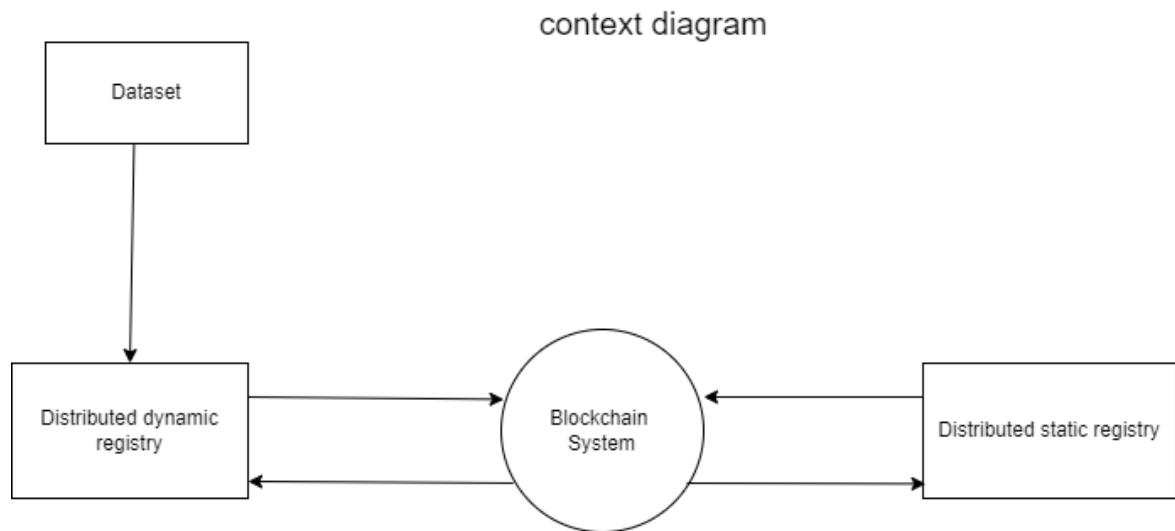


4.4.2 Class Diagram:

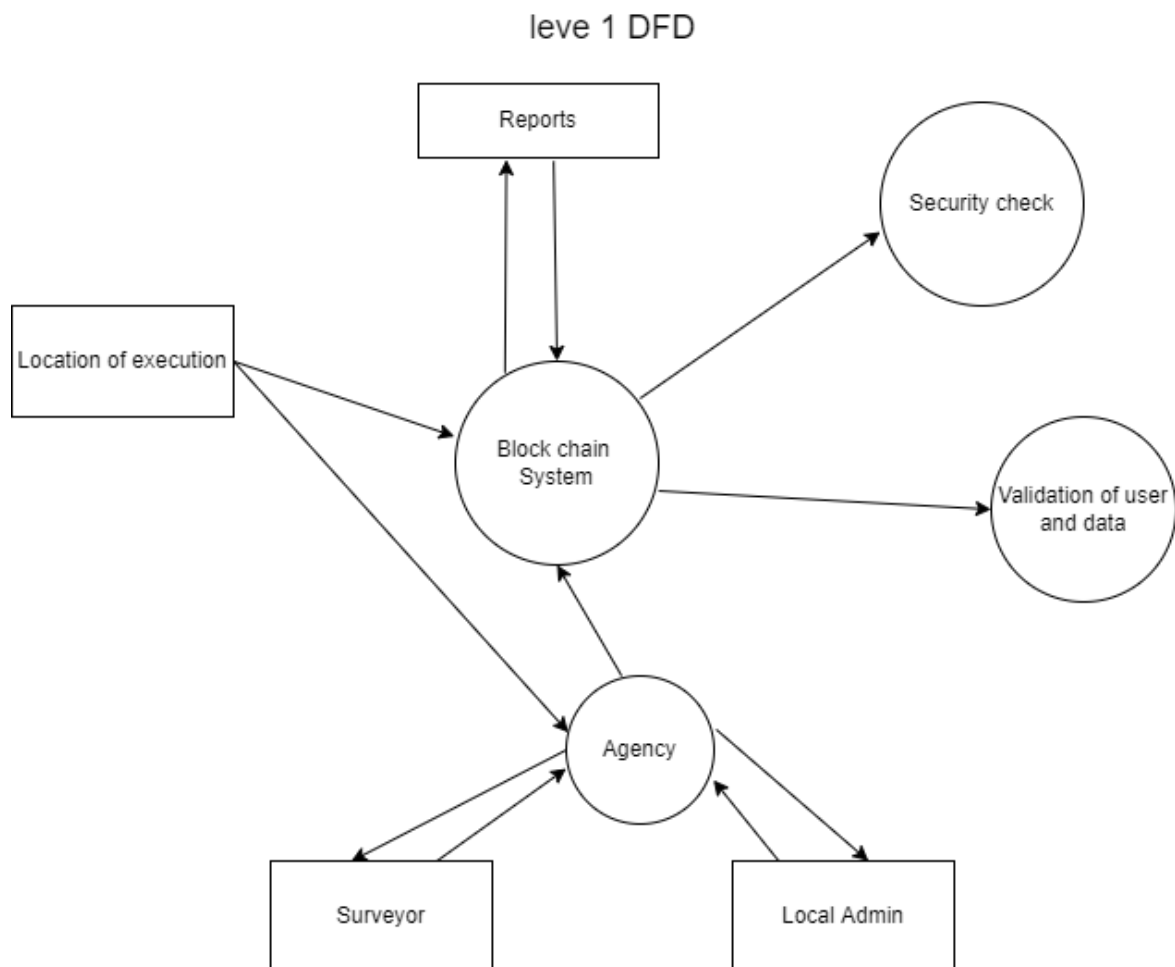
Class Diagram

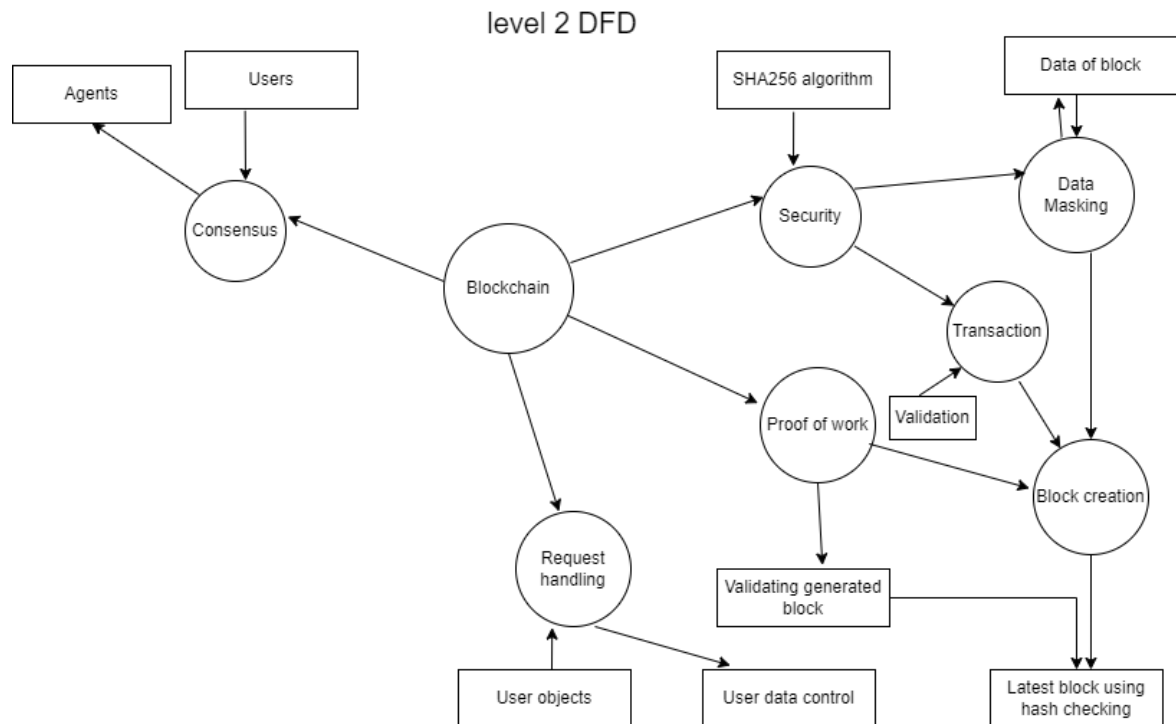


4.4.2 Context Diagram:



4.4.2 DFD level 1:

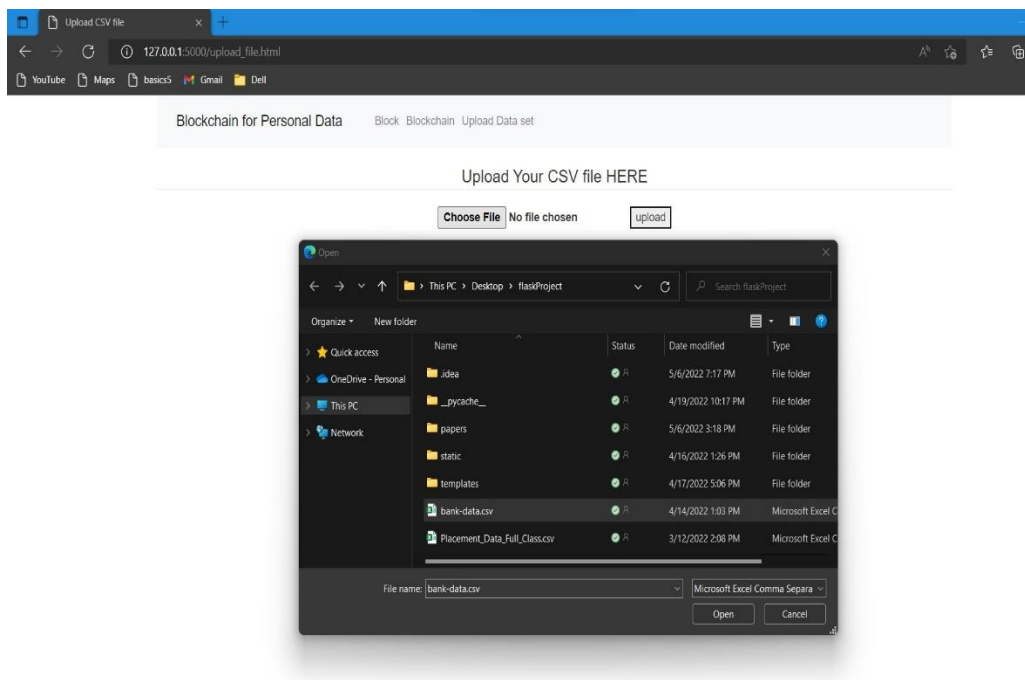


4.4.4 DFD Level 2:

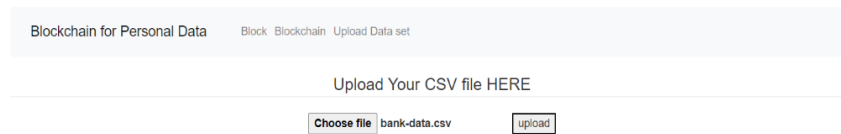
4.4.5 User Manuals:



1) Description: - This is our home page.



2) Description: - This is our data set page where you can upload Dataset from the drive.

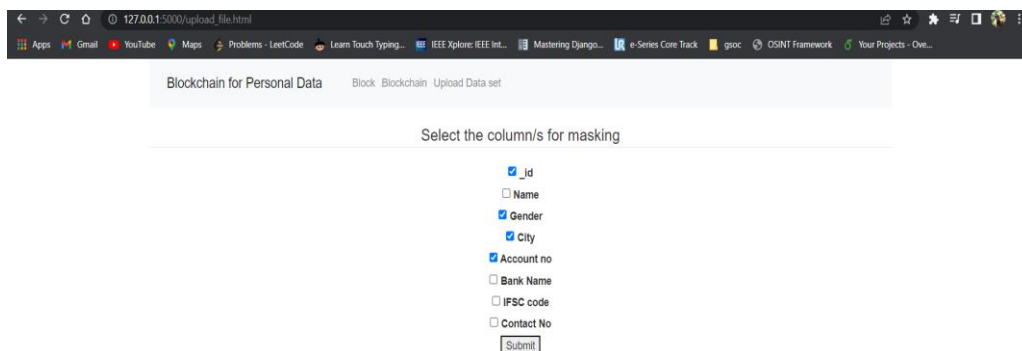


Blockchain for Personal Data Block Blockchain Upload Data set

Upload Your CSV file HERE

bank-data.csv

3) Description: - The data has been uploaded.

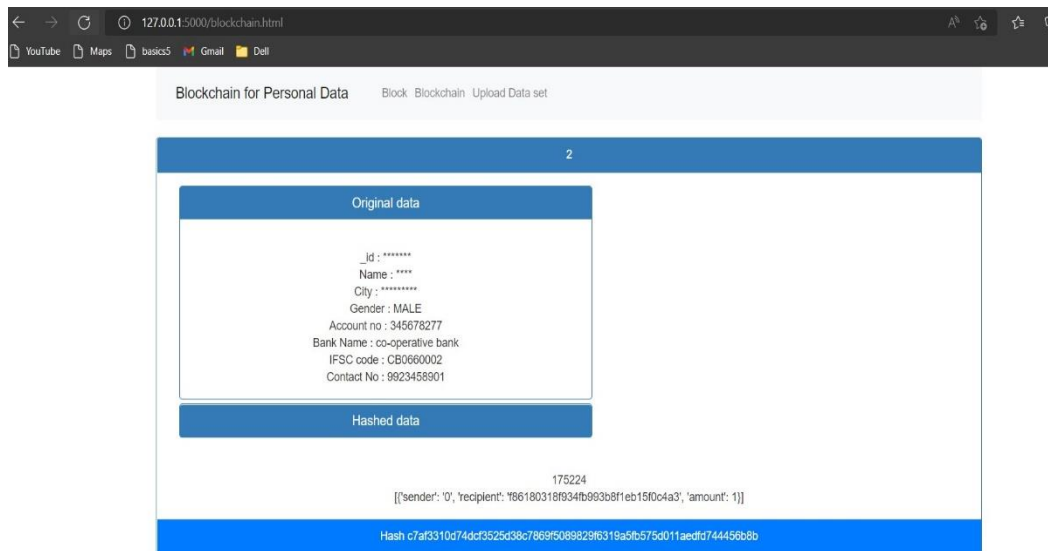


Blockchain for Personal Data Block Blockchain Upload Data set

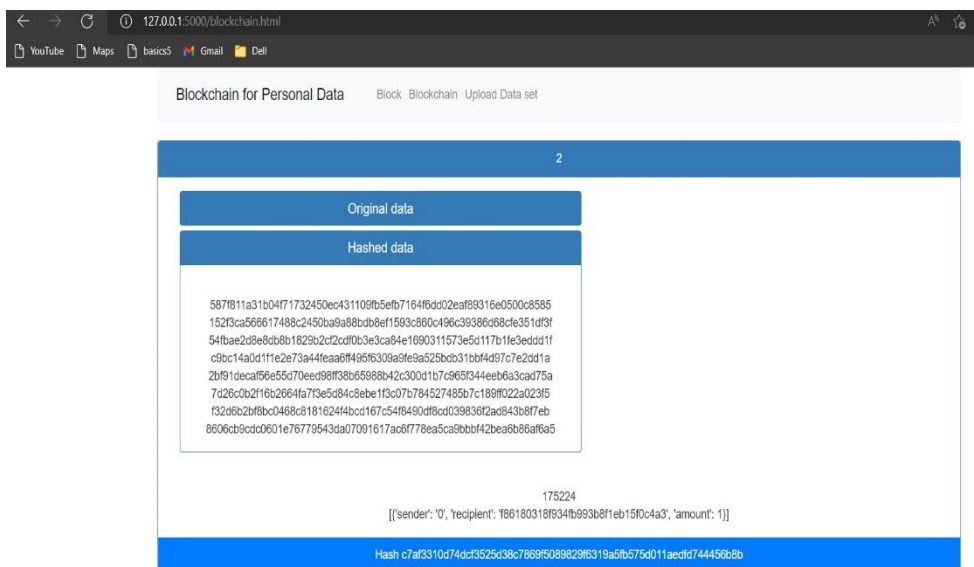
Select the column/s for masking

☒ _id
☐ Name
☒ Gender
☒ City
☒ Account no
☐ Bank Name
☐ IFSC code
☐ Contact No

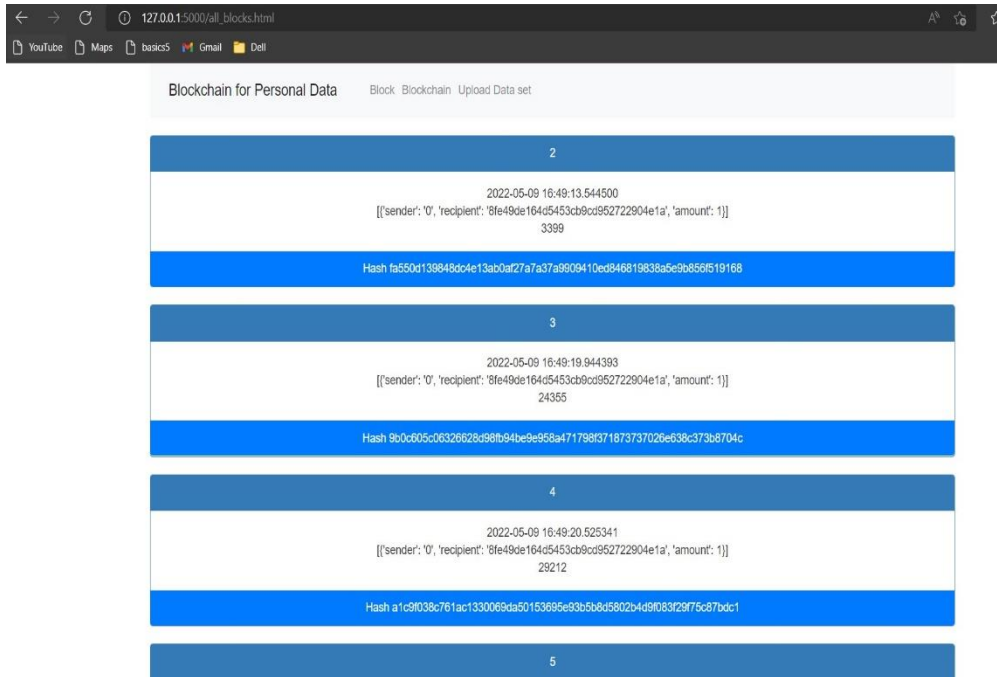
4) Description: - This is our Masking column's from that you can hide the data into to block.



5) Description: - This is our block page in this it will creates the Blocks and showing our Masking columns and data with hiding our details.



6) Description: - This is our hashed data of our original data and showing its particular hash key.



The screenshot shows a web browser window with the address bar displaying '127.0.0.1:5000/all_blocks.html'. The browser's address bar also shows icons for YouTube, Maps, basics5, Gmail, and Dell. The page title is 'Blockchain for Personal Data'. Below the title, there are three tabs: 'Block', 'Blockchain', and 'Upload Data set'. The main content area displays a list of three blocks, each with a blue header bar containing the block number (2, 3, and 4 respectively). The first block (Block 2) has a timestamp of '2022-05-09 16:49:13.544500', a transaction data field containing '[{"sender": "0", "recipient": "8fe49de164d5453cb9cd952722904e1a", "amount": 1}]', and a value of '3399'. Its hash is 'fa550d139848dc4e13ab0af27a7a37a9909410ed846819838a5e9b659f519168'. The second block (Block 3) has a timestamp of '2022-05-09 16:49:19.944393', the same transaction data, and a value of '24355'. Its hash is '9b0c605c06326628d98fb94be9e958a471798f371873737026e638c373b8704c'. The third block (Block 4) has a timestamp of '2022-05-09 16:49:20.525341', the same transaction data, and a value of '29212'. Its hash is 'a1c9f038c761ac1330069da50153695e93b5b8d5802b4d9f083f29f75c87bdc1'. A fourth block header bar with the number '5' is visible at the bottom of the list.

Block	Blockchain	Upload Data set
2	2022-05-09 16:49:13.544500 [{"sender": "0", "recipient": "8fe49de164d5453cb9cd952722904e1a", "amount": 1}] 3399 Hash fa550d139848dc4e13ab0af27a7a37a9909410ed846819838a5e9b659f519168	
3	2022-05-09 16:49:19.944393 [{"sender": "0", "recipient": "8fe49de164d5453cb9cd952722904e1a", "amount": 1}] 24355 Hash 9b0c605c06326628d98fb94be9e958a471798f371873737026e638c373b8704c	
4	2022-05-09 16:49:20.525341 [{"sender": "0", "recipient": "8fe49de164d5453cb9cd952722904e1a", "amount": 1}] 29212 Hash a1c9f038c761ac1330069da50153695e93b5b8d5802b4d9f083f29f75c87bdc1	
5		

7) Description: - This is our full block chain with the date, timestamp, particular blocks hash key, node.

Chapter-5 Testing

5.1 Functionality Testing: -

- In this type of testing we have checked the functionality of our application i.e. block chain.
- In this we have compared all the function test like home page, upload data set, upload csv file page, upload success, masking column for hidden data, submit button, block page, hashed data, full block chain.
- Functional tests are used to verify that the output of a software programme meets the functional requirements by giving acceptable input.

Test Case_id	Test Name	Input	Output	Test result
TC_1	Home page	- Check User able see home page by run the app on click. (http://127.0.0.1:5000/)	User can see	Pass
		- Check whether user can able to see the buttons on the navigator and it is clickable or not at home page (block, block chain & upload data set.	User able to see and its clickable.	Pass
TC_2	-Upload data set	- Check The user could use upload data set button.	User able to click the button.	Pass
	-Uploading Csv file page	- check whether user can able to see uploading file page and check if the file can able to select or not from the drive by clicking on choose file button.	User see the file page and also able to select the file from the drive.	Pass
	- Upload	-Verify that the user has permission to use the upload button.	User can able to click.	Pass

TC_3	- Masking columns	- Check whether user can able to see the masking columns of the data set after click on upload button and user able to select the random check box.	User able to see all the columns and able to select the random checkbox.	Pass
	- Submit Button	- Look for a clickable submit button.	Button is clickable	Pass
TC_4	- Block page	- Check whether user can able to see the masking columns and can able to see the masked columns and unmasked columns in the block or not.	masked and unmasked columns visible.	Pass
	- Hashed data	- Check whether user able to see the hashed data of the columns by clicking on toggle button.	User can able to see hashed data by clicking on toggle button.	Pass
TC_5	- Full block chain	- Check whether the user can able to see the full chain blocks with the date, timestamp, node of the block and hashed of the particular block	User can able to see the full chain of the particular blocks with its necessary details.	Pass

Chapter – 6 Conclusion and Future Enhancement

6.1 Conclusion:

We have come to the conclusion that personal or sensitive data should not be given to other parties since they are sensitive to abuse and fraud. Users should instead be allowed to own and control their data while ensuring security. Our Platform enables the feature to store personal data dynamically and hiding Important details of the user in the block chain for user security. Furthermore, the block chain identifies the user as the data's owner. However, if a user has a significant volume of data to store digitally for security, block chain for personal data is a chevalier choice.

6.2 Future Enhancements:

- Try for to make system more user Friendly.

Chapter – 7 Bibliography & References

7.1 Book reference:

<https://www.guru99.com/blockchain-tutorial.html#6>

<https://medium.com/@mushtaque87/flask-in-pycharm-community-edition-c0f68400d91e>

7.2 Web reference:

<https://youtu.be/RzHvb7FuNAw>

<https://youtu.be/vGn3xiL9zYQ>

Turnitin Originality Report

19mxa067 Block chain by Yash Sompura

From paper (Personal)



- Processed on 13-May-2022 15:57 IST
- ID: 1835375585
- Word Count: 3018

Similarity Index

7%

Similarity by Source

Internet Sources:

7%

Publications:

1%

Student Papers:

N/A

sources:

- 1 2% match ()
Owston, James Martin. "Survival of the Fittest? The Rebranding of West Virginia Higher Education", Marshall Digital Scholar, 2007
- 2 1% match (Internet from 06-Jul-2020)
<https://customwritings.co/external-factors-affecting-hyatt-regency/>
- 3 1% match ()
<http://www.it.iitb.ac.in/~bepj/llassignment/voip3/assign2/umlfinaldraft.htm>
- 4 1% match (Internet from 04-Feb-2022)
https://www.studymode.com/v1/turnitin_essay/268931
- 5 1% match (Internet from 23-Feb-2019)
https://baadalsg.inflibnet.ac.in/bitstream/10603/113456/10/10_chapter6.pdf
- 6 < 1% match (Internet from 18-Jan-2022)
<https://uniassignment.com/essay-samples/information-technology/possession-at-untrusted-stores-in-cloud-computing-information-technology-essay.php>
- 7 < 1% match (Internet from 28-Mar-2019)
<https://www.bestinterviewquestion.com/python-interview-questions>
- 8 < 1% match (Internet from 05-Aug-2014)
<http://www.slideshare.net/GonzaloSantiago/design-and-implementation-of-compiler>