IMPLEMENTING A SECURE AUTHENTICATION SYSTEM FOR THE COLLEGE INFORMATION SYSTEM

[#1] V.Naresh Kumar, Assistant Professor,
[#2] V. Lalitha, Assistant Professor,
[#3] P.Sudheer Kumar, Assistant Professor,
Department of CSM,
SAI SPURTHI INSTITUTE OF TECHNOLOGY, SATHUPALLY, KHAMMAM.

ABSTRACT: Because of the rising popularity of cryptocurrencies, the use of blockchain technology is multifarious. Several firms have already adopted blockchain technology because to its inherent benefits, such as maintaining information confidentiality and anonymity. As an example, consider Internet 3.0. The concept of data freedom is important in the context of Web 3.0 because it allows users to exercise discretion in selecting which data to communicate to the server. The cryptographic wallet sends user data to a nearby device, whereas the computer only receives data from the previously stated wallet. Through the employment of this technique, individuals can directly protect their privacy. The user will change the data before sending it to the computer. Our team has created software that takes use of Web 3.0 improvements and incorporates blockchain functionality. The goal of this software is to assess students' participation habits and assign jobs to them based on their digital wallets. The prototyping paradigm was used to create the program in this study. Individuals' passwords used throughout the registration process linked to their respective addresses. Furthermore, the addition of the Web3 module permitted the insertion of additional phases into the testing procedure. After successfully completing the registration process, students can now access their data in accordance with their particular job tasks.

Keywords: Authentication, Blockchain, Role-Based Access Control, Wallet.

1.INTRODUCTION

Blockchain allows for the decentralization of data distribution. Data are linked using pointers. New data will be collected. The blockchain requires new information. To keep the chain intact, no new data should be added. This solution maintains data integrity while avoiding the need for third-party trust.Web 3.0 uses blockchain to decentralize internet operations. Concerns about privacy plague Web 2.0. With the help of big data, application providers can target adverts based on user data. It is possible since they store user data. The Facebook data hack reveals how app developers use user data without their knowledge. Because of the benefits of blockchain technology, many firms are implementing it. The system's owner cannot change block data in blockchain. It enables businesses to store data without fear of changes. This data collection strategy is useful in healthcare, logistics, and smart cities. Blockchain technology has the potential to be applied in education. The application of blockchain technology to student records benefits education. Students' privacy is secured when they view their grades, personal information, and payment status. It can only be viewed by students who have access to college information. The certificate can grant digital degrees based on blockchain data as proof ofownership.

2.METHODOLOGY

In this study, the Prototyping Model is utilized to integrate blockchain into college information systems. The following steps are depicted in Figure 1: requirements collecting, analysis, rapid design, prototype production, initial user evaluation, prototype refining, product implementation, and maintenance. determining and evaluating requirements User requirements are collected and analyzed here. Users will appropriately designate software parameters. User software development expectations will be revealed during this phase. All user requirements will be assessed and integrated into the software. Quick thought. This phase shows how to use a requirement analysis to showcase software processes. A user will be able to confirm the results of segment design. Following user acceptance, design will lead software development.

.

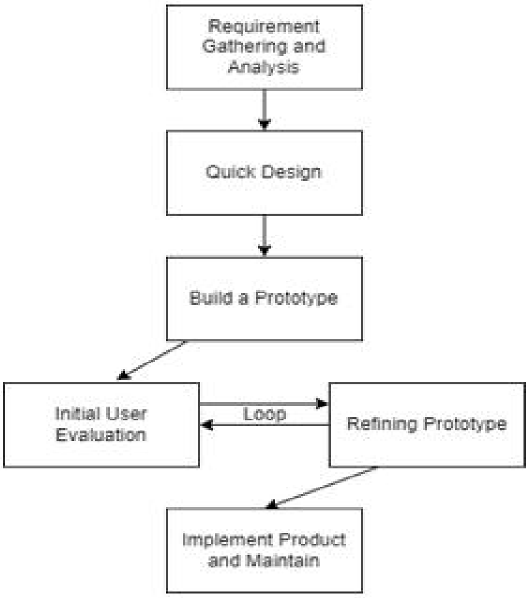

Figure 1. Modeling to create prototypes

Create a model. This phase involves developing software prototypes that are as user-friendly as possible. Users are given software prototypes that show how a feature will work in the final product.

Initial user evaluation. The goal of this stage is to get user input on the prototype. The prototype will illustrate the software's capabilities. Keeping software requirements in place during this time.

Development of prototypes. To guarantee that the software fits all requirements, the prototype is adjusted based on user feedback. This stage is done several times during the initial user review until the prototype meets the user criteria. The frequency of this operation is unknown because the user must authorize its termination.

Product development and maintenance. During this stage, software delivery and user compatibility take place. This stage entails software maintenance in order to extend its useful life.

3. RESULT AND DISCUSSION

The model's software development components are being adjusted because the system is not yet ready for blockchain-based authentication

Requirement Gathering and Analysis

According to user requirements and analytical findings, the program will meet the functional criteria listed in Table 1.

Table 1. Functional need

Code	Requirement
FR01	Students can log in to the system
FR02	Students can link their wallets to the system
FR03	The system can recognize students by their wallet address
FR04	Student can access their data based on their role
FR05	The system can show student information by their wallet address

We also conclude that data integrity is nonfunctional. Data that is precise, consistent, and system-compatible is required.Rapid Development

Quick Design

The research informs our use case diagram, which depicts how students might use the technology.

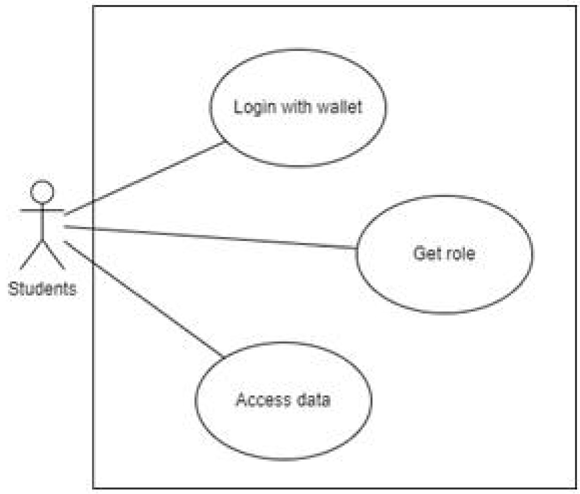

Figure 2 The utilization of.

Figure 2 displays the three basic ways in which students interact with the system.

Student accounts must be signed in electronically. This technique is distinct since user information is not saved on the system. Purses are required for students' work.Student obligations are manageable. When students log in, the system checks their wallet addresses against previously saved data.

The system allocates student positions when this is observed.

There are student records. Students with system responsibilities have access to their own data.

4. BUILDING A PROTOTYPE

Choosing Components

Software components are identified during prototyping.

BSC stands for Binance Smart Chain. This component generates a one-of-a-kind token. We can determine the system requirements for this token because it cannot be mined. Only the proprietor has the ability to change the number and ownership of tokens. The BSC provides free tokens. Tokens that have been delisted can still be used, but they cannot be seen. The BSC Evolution Proposal 20 is standard. The superhero mask. Students can enroll using their digital IDs and wallets. Metamask's integration with the BSC token and smart contract will offer students with crypto addresses. Addition for Web3. This module adds support for metamask. Applications can communicate with local and remote nodes using HTTP, IPC, and WebSocket libraries. Make your move. A UI library component. Decentralization necessitates the use of software that supports single-authentication.

Students must meet the following requirements before they can access their purses:

Students must use metamask identities.

Metamask must be installed and connected before students may use Binance Smart Chain.

As part of this campaign, students must register their handbags. Figure 3 shows how students can log into Metamask using their wallets. For student wallet information, Metamask will be queried. Metamask uses decentralized authentication to confirm student laptop credentials. Metamask requires wallet information after the student logs in. This enables the system to assign responsibilities and offer statistics to pupils. Figure 4 demonstrates the need for wallet and network databases for decentralized authentication. Students can have numerous accounts if they are on different networks. Metamask wallet addresses will be compared to student IDs. Following that, the system assigns database roles to pupils.

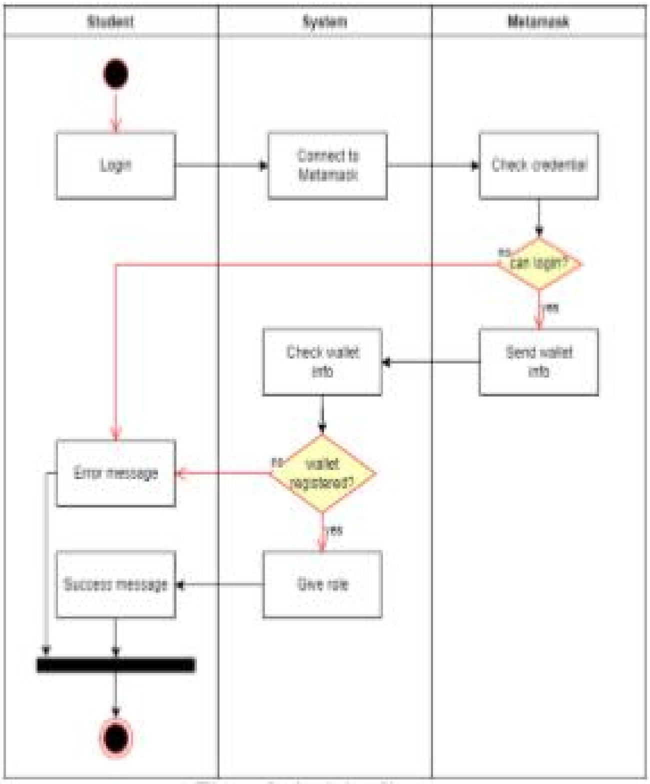

Figure 3. The flowchart of the method

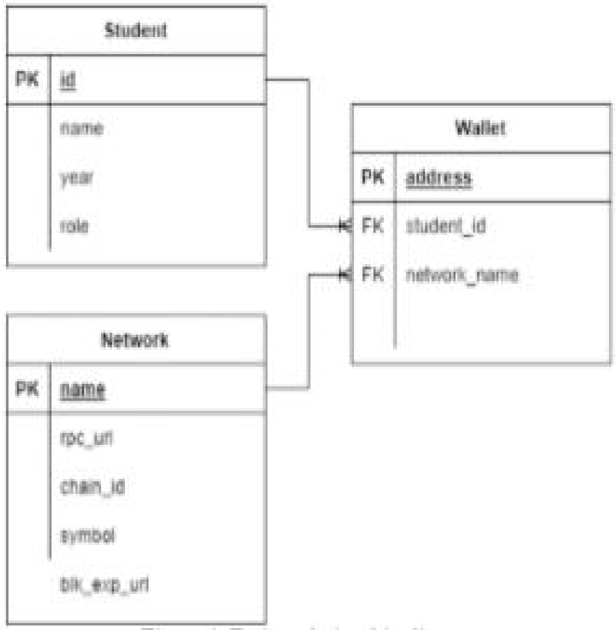

Figure 4An example of an entity relationshipApplication for Construction Software

Building Application

Ethereum is used in this module. To connect the module to BSC, which is based on Ethereum, we changed the chain ID and URL in the configuration file.

When the "Login with Metamask" button is clicked, our front-end application invokes Metamask, as seen in Figure 5. Because Metamask is only available locally, clients use Single Page Applications (SPA). Student

Metamask credentials are necessary to read the wallet address and transfer data to the backend in order to allocate roles.

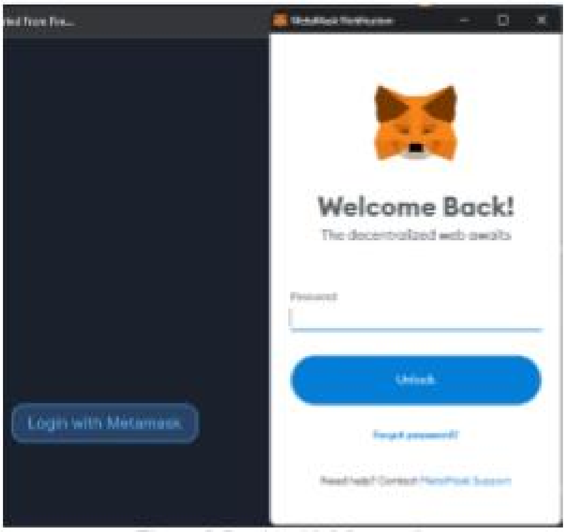

Figure 5 Authentication with Metamask.

Using the data provided by the frontend, the backend obtains pupil data from the database. Student data includes their ID number, name, wallet address, and duties. Session cookies hold all of this information for permanent credential management. Figure 6 shows a cookie that has been saved.

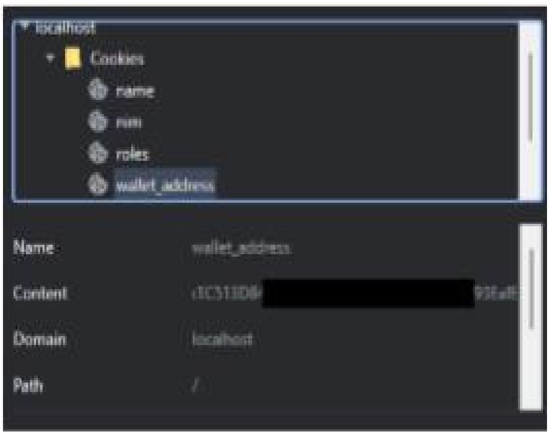

Figure 6. Student Statistics

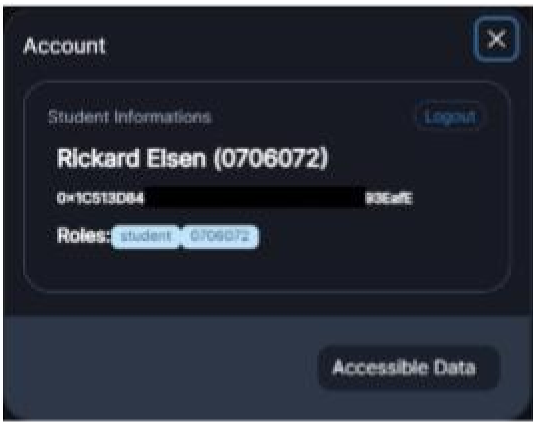

Figure 7. Student's Information

After validating pupil data and storing the session in cookies, the backend delivers a 200 status code to the frontend to signal success. Because student information is saved in cookies, the backend does not return student information. Figure 7 illustrates the pupil data interface.

After logging in, students can view their data by database role. Multiple roles might be allocated to students. Figure 8 depicts students' duties and responsibilities.

Figure 8. Student Role Information

We created software to register people online. Metamask wallet data can be requested and received by software. The software compares wallet addresses to database information to assign student roles.

Initial User Evaluation

- To demonstrate the product's operation to stakeholders, we mimic a student logon and solicit feedback from two users.
- We must reset student wallets and revoke data access because they may forget their credentials. Because humans generate the vast amount of data, software must limit data storage. System and student data must be reanalyzed.

Refining Prototype

Throughout this phase, feedback from stakeholders is used to inform program changes.

Application for resetting a student's wallet. Students' purses must be reset by the administration. Once authorized, administration will program the student's wallet address. Remove data access to the previous address and reset the pupil's wallet address. It is not possible to automate the prevention of unauthorized and irresponsible account access. Student information is removed from transaction records via software. All student information was replaced with wallet addresses. This technique reduces data storage by half. Additional inquiries have little or no impact on the system.

ISSN: 2366-1313

5.CONCLUSIONS

We created a Web 3.0 system to authenticate student logins and assign data access permissions. The BSC, Metamask, Web3 module, and React technologies were used in this system. To log in, use the student wallet addresses. Metamask allows for this strategy. The study shows how blockchain technology can be utilized for authentication, with wallets serving as user credentials and authorization duties. Our product is a working prototype. We do not use it because it demands college system improvements. We cannot monitor transactional dynamics using blockchain because we can only analyze data using a copy. We want it to grow and become more comprehensive so that it may be used at institutions. To improve BSC utilization, all college network transactions will be tokenized.

REFERENCES

1. U. Bodkhe et al., "Blockchain for Industry 4.0: A Comprehensive Review," IEEE Access, vol. 8, pp. 79764–79800, 2020, doi: 10.1109/ACCESS.2020.2988579.
2. S. Rouhani and R. Deters, "Blockchain based access control systems: State of the art and challenges," in IEEE/WIC/ACM International Conference on WebIntelligence, Oct. 2019, pp. 423–428. doi:10.1145/3350546.3352561.
3. S. Aghaei, "Evolution of the World Wide Web : From Web 1.0 to Web 4.0," International journal of Web & Semantic Technology, vol. 3, no. 1, pp. 1–10, Jan. 2012, doi: 10.5121/ijwest.2012.3101.
4. F. A. Alabdulwahhab, "Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation," in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Apr. 2018, pp. 1–4. doi: 10.1109/CAIS.2018.8441990.
5. P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," Future Generation Computer Systems, vol. 86, pp. 650–655, Sep. 2018, doi: 10.1016/j.future.2018.04.060.
6. V. Filimonau and E. Naumova, "The blockchain technology and the scope of its application in hospitality operations," International Journal of Hospitality Management, vol. 87, p. 102383, May 2020, doi: 10.1016/j.ijhm.2019.102383.
7. A. A. Monrat, O. Schelen, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," IEEE Access, vol. 7, pp. 117134–117151,2019,doi:10.1109/ACCESS.2019.2936094
8. D. di Francesco Maesa, P. Mori, and L. Ricci, "A blockchain based approach for the definition of auditable Access Control systems," Computers & Security, vol. 84, pp. 93–119, Jul. 2019, doi: 10.1016/J.COSE.2019.03.016.Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. K. Hung, "A Permissioned Blockchain-Based System for Verification of Academic Records," in 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Jun. 2019, pp. 1–5. doi: 10.1109/NTMS.2019.8763831.
9. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," Applied Sciences, vol. 9, no. 12, p. 2400, Jun. 2019, doi: 10.3390/app9122400.