Certificate Generator using Blockchain Technology(BlockCert)

Sohaila Ismail Mohamed
Department of Computer Science
College of Information Technology,
Misr University for Science and Technology (MUST), 6th of October city, Egypt
89570 @must.edu.eg

Mohamed S.Abdiwahab
Department of Computer Science
College of Information Technology,
Misr University for Science and Technology (MUST), 6th of October city, Egypt

Rania Elgohary
Department of Artificial Intelligence
College of Information Technology,
Misr University for Science and Technology (MUST), 6th of October city, Egypt
rania.elgohary@must.edu.eg

***Abstract*— In recent times, various technologies have become pervasive in our surroundings, contributing to the dynamism of everyday life and time efficiency. Globally, there is a prevailing trend toward embracing technology, with countries striving to digitize various aspects of their operations. Notably, Egypt has played a significant role in this digital transformation. Several years ago, Egypt initiated a comprehensive digitization effort, such as converting employee signatures into fingerprints, scanning IDs to track attendance, and utilizing drone planes for various applications, including capturing sports events.**

Furthermore, a noteworthy development occurred approximately three years ago when Egypt transitioned from using paper currency to adopting a card payment system for transportation. The nation has also embarked on constructing smart cities, exemplified by New Alamein, with the goal of enhancing operational efficiency and elevating the quality of government services and citizen well-being. This initiative addresses issues like waiting in queues at the Student Affairs Office, where:

individuals would traditionally wait for their turn, dealing with paperwork, and waiting for signatures. Our project is designed to tackle these challenges, aiming to eliminate the inefficiencies of spending an entire day at a single location for administrative processes. Ultimately, our objective is to contribute to the realization of a digital Egypt, equipped with advanced technology that aligns with global standards.

Keywords*— *Technology, Smart Cities, Certified Certificate.

I. INTRODUCTION

Technology involves applying knowledge to achieve practical goals in a specified and reproducible manner. Its widespread use is evident in various sectors, including medicine, science, industry, communication, transportation, and daily life. Technologies encompass tangible items such as tools or machines, as well as intangible tools like software. Given the extensive array of technology, numerous technological fields have emerged, such as the Internet of Things (IoT) and the web, each requiring databases.

As the utilization of social networks and systems rapidly grows, and governments strive to digitize every aspect of their agencies, this project aims to streamline the collection of student information to facilitate the certificate issuance process. This involves using the student's ID number, password, and website, where the certificate is displayed on a screen and subsequently printed. This approach reduces reliance on printed papers and minimizes human efforts, alleviating crowd in the student affairs office and preventing the risk of certificate falsification.

The project actively supports the Sustainable Development Goals (SDGs), particularly focusing on SDG#9: Industry, Innovation, and Infrastructure. The integration of blockchain technology within our project is a testament to our commitment to innovation, thereby contributing to the advancement of infrastructure in Egypt. Digitalizing the certification generation process aligns seamlessly with the goals of fostering technological innovation within industries and building robust infrastructure.

Furthermore, our initiative resonates with SDG#11: Sustainable Cities and Communities. By enhancing government services through the implementation of technology, we are actively contributing to the creation of sustainable cities that prioritize technological advancements. The utilization of blockchain not only streamlines certification processes but also lays the foundation for building smart cities, fostering a technology-oriented environment conducive to long-term sustainability. In aligning with SDGs, our project serves as a catalyst for positive change, propelling advancements in both innovation and urban sustainability.

II. PROBLEM DEFINITION

Local government institutions are increasingly under pressure to deliver high-quality services to citizens. Governments and governmental bodies are striving to meet customer expectations while ensuring efficiency and accountability. In our country, there are numerous challenges, including the considerable time wasted waiting in queues at hospitals or government offices to obtain necessary paperwork, whether for job applications or other administrative processes. If you ask any Egyptian citizen about interacting with governmental institutions to obtain, create, or modify any data, the common response would highlight the difficulty, time consumption, and financial expenses involved in achieving these objectives. Given the widespread nature of this issue across all state institutions, efforts are being made to address the problem on a smaller scale, focusing on the educational institution as a miniature model. Specifically, the project targets the issue of certificates in universities, aiming to eliminate the risk of certificate loss or forgery. The ultimate goal is to provide students with a reliable certificate without unnecessary hassle or wasted time.

III. PROBLEM DESCRIPTION

When a senior student seeks to apply for a job, the initial step involves requesting the university to issue a graduation certificate. To initiate this process, the student must first complete their personal data or information, ensuring they meet specific criteria such as fulfilling a particular number of

hours and maintaining a GPA that qualifies them for the certificate. Additionally, fees are required for the issuance of the certificate.

Upon the university receiving a certificate request, a preliminary verification phase is conducted before the student formally submits the request. This involves confirming the student's affiliation with the university by entering their ID number and password. If the student profile is found, the system allows the student to proceed with the certificate request. Subsequently, the system conducts a two-step verification process: first, checking the finance account to confirm the completion of the financial transaction, and second, verifying the student's academic account to ensure eligibility for the certificate. If both verifications are successful, the system proceeds to generate the digital certificate. If any of the verifications fail, the system cancels the request.

The entire process of obtaining the digital certificate necessitates thorough checks of all transactions involved in generating the certificate. When the student presents the certificate to a prospective employer, such as a company, only the student's ID number and password are required for the employer to view the digital certificate.

IV. Problem Definition

In our exploration of blockchain, we discovered various applications, one of which is Bitcoin—a peer-to-peer electronic payment system that has gained rapid popularity in recent years. The challenge arises when attempting to extract meaningful economic variables from the extensive history of Bitcoin blockchain data, now exceeding 1.6 billion historical transactions. Querying this data efficiently has become increasingly complex.

To address this challenge, cohort analysis, a methodology developed for population data in the social sciences, is employed to interpret Bitcoin blockchain data. Specifically, the approach involves querying and processing the Bitcoin transaction input and output data within daily cohorts. This allows to generate datasets and visualizations pertaining to key Bitcoin transaction indicators, such as the daily lifespan distributions of spent transaction output (STXO) and the daily age distributions of the cumulative unspent transaction output (UTXO).

Through this method, a computationally feasible approach for characterizing Bitcoin transactions is presented, opening avenues for future economic studies of Bitcoin [1].

V. Comparative Study

Upon conducting an in-depth examination of our system and other systems related to ours, it became apparent that the projects discussed in Chapter 2 (related work) are not only the ones closely related to ours; there are additional projects such as Udemy, Coursera, Udacity, and more. While these platforms do not share a technological connection with our project, such as blockchain or specific techniques, they align with our project in terms of the overarching idea: generating certificates based on predefined criteria, such as completing courses and achieving a minimum score, resembling the concept of a contract in our case.

In contrast to these platforms, our project distinguishes itself in several aspects, as previously outlined in earlier chapters. One significant difference lies in the utilization of a distributed database for our project, whereas these platforms rely on centralized databases.

For instance, Udacity operates as an online education provider, offering courses developed in collaboration with notable companies like Google, Facebook, and Intel, as well as other global organizations. Udacity's courses feature pre-recorded video lectures that learners can access at their convenience. Free courses on Udacity include video lessons and auto-graded quizzes. The platform also offers a paid micro-credential called a Nanodegree, comprising Udacity courses, human-graded projects, mentor support, and a certificate, available through either a monthly subscription or a single discounted payment for the entire nanodegree.

On the other hand, Udemy allows instructors to create, own, and manage their courses, incorporating various elements such as videos, slides, text, resources, and practice activities to enhance the learning experience for students. Each Udemy course is independent and reflects the instructor's approach to teaching.

In summary, while these online education platforms share a common goal of providing certificates based on course completion, the technological infrastructure, database architecture, and operational models significantly differ between our distributed database-dependent project and the centralized database-oriented platforms like Udacity and Udemy.

VI. Methedology

In the course of our research, we explored numerous algorithms for implementing blockchain in our project, and after careful consideration, we identified the Hashing Algorithm as the most suitable for our concept.

A hashing algorithm, in essence, is a mathematical function designed to scramble data, rendering it unreadable. One of the key characteristics of hashing algorithms is their one-way nature, preventing the unscrambling and decoding of the text by any external entity. This property ensures that data at rest remains secure, even if unauthorized access to the server is gained.

Furthermore, hashing serves to verify the integrity of data, providing assurance that it hasn't been tampered with after its initial creation. Additionally, some utilize hashing to facilitate the analysis of extensive datasets.

The typical process followed by most hashing algorithms involves several steps:

1. Create the message: A user determines the content that needs to be hashed.
2. Choose the type: Given the variety of hashing algorithms available, the user selects the one that best suits the specific message.
3. Enter the message: The user inputs the message into a computer running the chosen hashing algorithm.

4. Start the hash: The system transforms the message, regardless of its length, into a predetermined bit size. Typically, the message is broken into equal-sized blocks, each compressed in sequence.
5. Store or share: The user then sends the resulting hash, also known as the "message digest," to the intended recipient, or stores the hashed data in that form.
While the hashing process may seem complex, it operates rapidly, completing the hash in a matter of seconds. This efficiency, combined with its security features, makes Hashing Algorithm the optimal choice for implementing blockchain in our project.

VII. Methodology & Techniques

The Agile methodology is employed in the execution of this project, facilitating a swift progression towards our mission. Initially, we conducted an analysis of the required system [1]. Subsequently, we identified the tools required to translate our conceptual idea into reality. Following this, we commenced the creation of diagrams to provide visual clarity during implementation. Concurrently, we engaged in designing the User Interface/User Experience (UI/UX) for the application. The implementation phase involved the simultaneous development of the database, web pages, and contract.

VIII. System Design

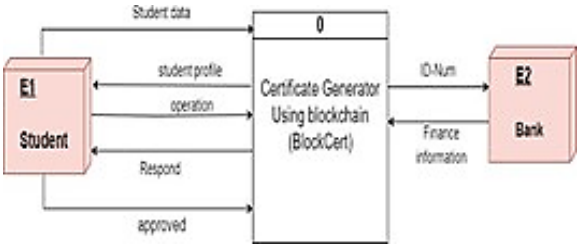

Fig.1 System Architecture

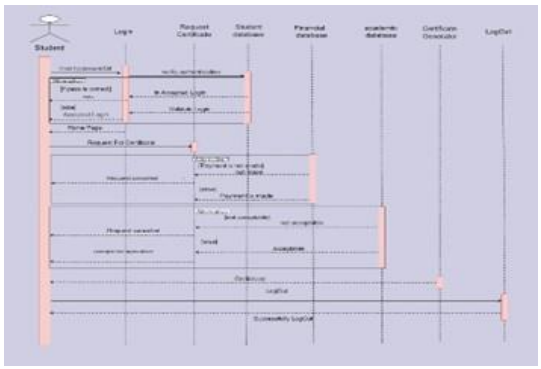

Fig. 2 Sequence Diagram

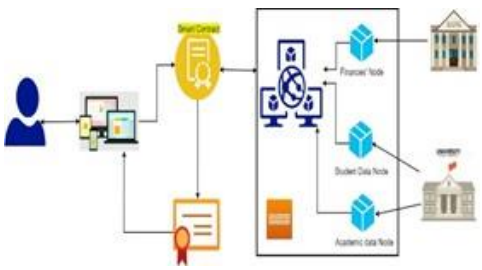

Fig. 3 Class Diagram

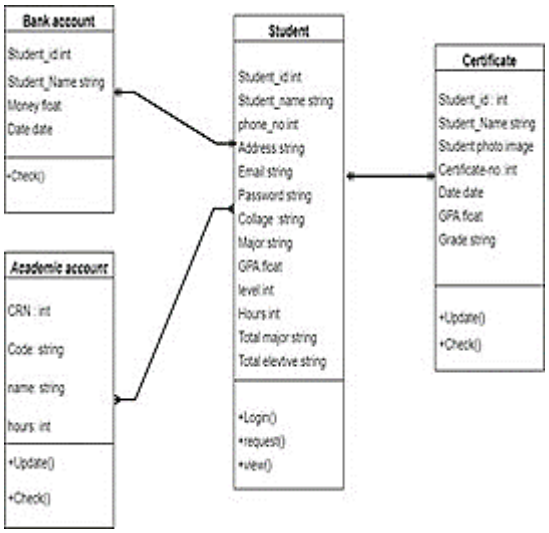

Fig. 4 Data Flow Diagram

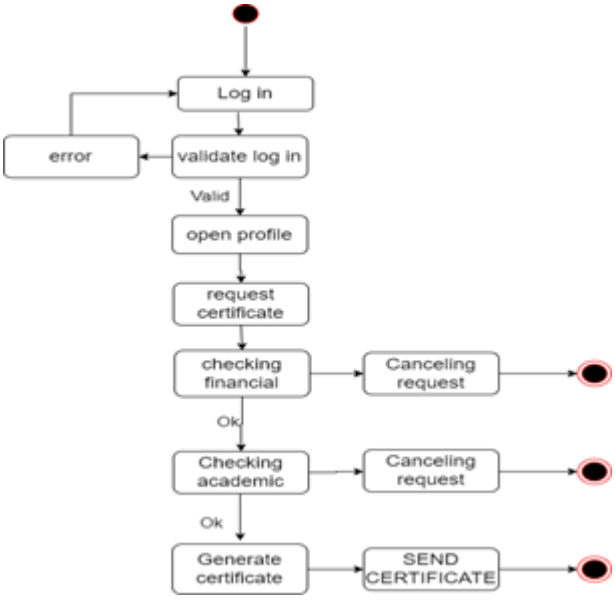

Fig. 5 Activity Diagram

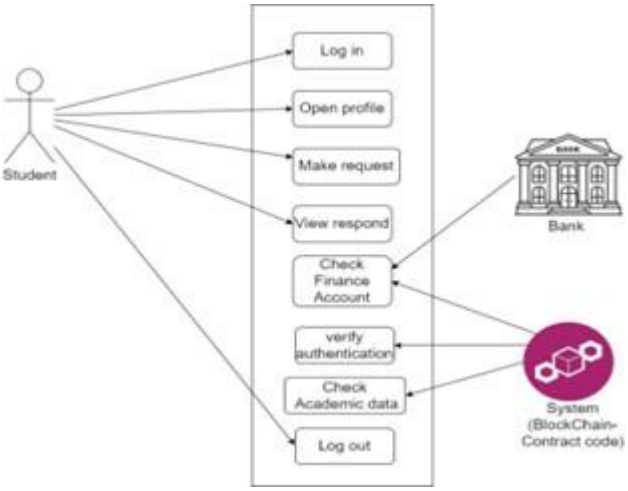

Fig. 6 Use Case Diagram

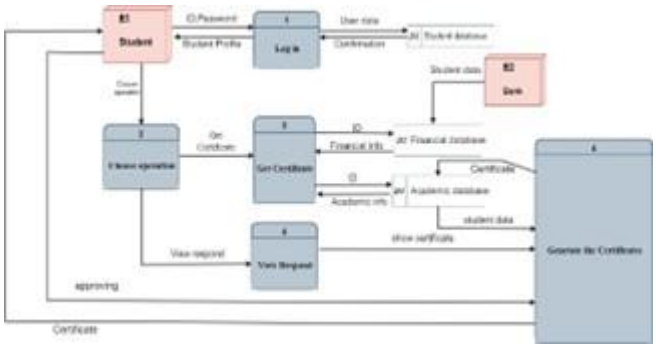

Fig. 7 Context Diagram

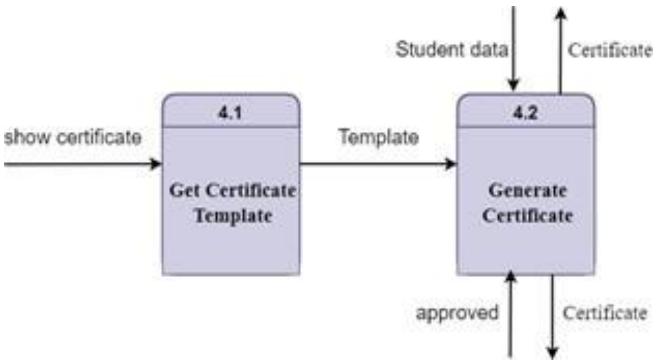

Fig. 8 Context Diagram Level 1 (Child)

IX. TOOLS

User Interface

For the front-end implementation, we utilized the power of Html, CSS, and JavaScript. Prior to the actual development, we utilized Figma to craft a comprehensive design for our website. Figma served as a crucial tool in visualizing and planning the user interface before diving into the coding phase.

Django

In the backend architecture, Django, a free and open-source web framework based on Python, played a pivotal role. Following the model–template–views (MTV) architectural pattern, Django is renowned for its emphasis on ease of creation for complex, database-driven websites. Maintained by the Django Software Foundation (DSF), it promotes reusability, "pluggability" of components, minimal code, low coupling, and rapid development. Notable websites such as Instagram, Mozilla, Disqus, Bitbucket, Nextdoor, and Clubhouse have successfully utilized Django for their platforms.

The Smart Contract

Smart contracts, integral to our project, are programs stored on a blockchain that execute when predetermined conditions are met. These contracts automate agreements, ensuring immediate certainty of outcomes without intermediary involvement or time loss. Additionally, they facilitate workflow automation, triggering subsequent actions when specific conditions are satisfied.

Programs

• Visual Studio Code

Visual Studio Code is a source-code editor that we used to run html, CSS, and Django code, then we connected it which the contract using JavaScript.

REMIX IDE

REMIX IDE, a user-friendly tool with a graphical user interface, was employed for developing smart contracts. Suitable for both experts and beginners, Remix offers a no-setup environment that expedites the development process. Known for its visual debugger, Remix integrates well with other tools and facilitates a straightforward deployment process to the Ethereum blockchain. It has become a go-to platform for individuals seeking to learn and develop on the Ethereum network.

X. RESULTS

The outcomes of our efforts culminated in the successful implementation of a website designed to generate certificates, providing valuable assistance to both Student Affairs (student services) and students. This achievement not only translates into time, money, and effort savings but also ensures the generation of certified certificates.

The overarching mission of our project is to address the challenge of individuals spending entire days in unproductive queues and waiting areas. Our goal is to contribute to the digitization of Egypt, infusing it with cutting-edge technology that aligns with global standards.

XI. CONCLUSION

Information technology has been an integral part of human existence for an extensive period. Its evolution has been closely intertwined with our quest for improved and rapid communication. The interplay between technology, community, and citizens forms the bedrock of a country's development. With the ever-growing influence of Internet applications, digital governance is continually advancing, emerging as a fundamental pillar of national progress.

As technology facilitates our daily lives, offering solutions to dynamic challenges and saving us time, its centrality is becoming increasingly evident. The global technological era is underway, marked by the development of "smart cities" worldwide. These cities leverage information and communication technologies (ICT) to enhance operational efficiency, disseminate information, and elevate the quality of government services and citizen welfare.

To propel Egypt into the digital age, the realization of a comprehensive vision and plan known as "Digital Egypt" is imperative. This initiative, grounded in a robust digital infrastructure, aims to collectively save time, money, and effort for the benefit of all.

Among the many positive impacts of technology, efficient management of time and resources stands out prominently. The influence of technology extends across various facets of 21st-century life, from enhancing transportation efficiency and safety to facilitating access to food, healthcare, socialization, and productivity. The internet's power has fostered the formation of global communities, facilitating the sharing of ideas and resources on a broader scale.

XII. ACKNOWLEDGEMENTS

Foremost, our sincere gratitude is extended to Almighty Allah for guiding and overseeing the successful completion of this project. Our heartfelt appreciation goes to our dedicated supervisors whose unwavering belief in our capabilities and guidance played an instrumental role throughout the project.

Achieving this significant milestone in our project was made possible with invaluable guidance and assistance from numerous individuals.

Furthermore, we express our heartfelt thanks to our parents and friends whose constant presence and unwavering support have been a source of encouragement throughout this journey. Their support has been instrumental in overcoming challenges and reaching the successful outcome of our project.

REFERENCES

1. Deciphering Bitcoin Blockchain Data by Cohort Analysis(paper).
2. J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey", IEEE Access, vol. 7, pp. 36500-36515, 2019.
3. Casino, T. K. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status classification and open issues", Telematics Inform., vol. 36, pp. 55- 81, Mar. 2019.
4. Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey", Int. J. Web Grid Services, vol. 14, no. 4, pp. 352-375, 2016.
5. S. Bano, M. Al-Bassam and G. Danezis, "The road to scalable blockchain designs", USENIX Login Mag., pp. 1-6, Dec. 2017.
6. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, A. Ritzdorf and S. Capkun, "On the security and performance of proof of work blockchains", Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 3-16, Oct. 2016.
7. Gervais, G. O. Karame, V. Capkun and S. Capkun, "Is bitcoin a decentralized currency?", IEEE Security Privacy, vol. 12, no. 3, pp. 54-60, May/Jun. 2014.
8. Blundell-Wignall, The Bitcoin Question, no. 37, 2014.