Blockchain and Flutter-Based Quiz Mobile DApp Toward Decentralized Continuous Assessment

Priyanshu Kapadia, Megh Naik, Raaj Anand Mishra, and Anshuman Kalla

1 Introduction

Education is indispensable to our lives, and lately, we have experienced many new modes of acquiring it. Countries all around the globe are putting dedicated efforts, and building education reforms to educate people. For a given education system, irrespective of modes, assessment is an integral process. It provides insights at various levels such as students' performance, efficacy of the teaching learning methodologies used, efficacy of a course, and interest in a program. There are different types of assessment such as portfolio assessment, peer assessment, project-based assessment, and continuous assessment [1]. However, continuous assessment has been widely adopted.

Continuous assessment aims at measuring students' performance more frequently during a course of learning. Some of the ways to carry out continuous assessment are assignment, quizzes, oral presentation, and group tasks. The summative function of the continuous assessment is to prepare final transcripts and certificates which are issued to students at the end of a module, course, semester, or a program [2, 3]. One of the challenges is to make this functionality transparent and verifiable for not just teachers and school authorities, but also for students and their parents. This implies that various involved entities should be able see and verify anytime the computation of final grades from the continuous assessments. Any intentional or unintentional changes should be easily traceable.

Another issue is that a student shares only the final transcripts and certificates with entities such as companies (for recruitment) or other schools (for admission). However, these final transcripts do not presents the continuous learning logs of the

P. Kapadia · M. Naik · A. Kalla (✉)
Department of Computer Engineering, CGPIT, Uka Tarsadia University, Bardoli, Gujarat, India
e-mail: anshuman.kalla@ieee.org

R. A. Mishra
Dell EMC, Bangalore, India

J. K. Mandal et al. (eds.), *Proceedings of International Conference on Network Security and Blockchain Technology*, Lecture Notes in Networks and Systems 738,
https://doi.org/10.1007/978-981-99-4433-0_42

student. In other words, if someone wants to see how a student performed throughout the semester or program then that is either not possible or challenging with the use of state-of-the-art (centralized) technologies. Hence, the challenge is how to enable sharing of students' learning logs along with the final transcripts and certificates.

Furthermore, there has been increase in e-learning and blended learning which goes beyond the formal regular (face-to-face) mode of education [4]. Thus, students can acquire knowledge from various sources and using various modes (online, distance, regular). Many of these e-learning platforms have online quizzes as means of assessment. In this context, the challenge is how to ensure security and verifiability for the online quiz-based assessment to keep the trust intact.

In essence, there are numerous challenges associated with the continuous assessment such as transparent and secure conduction of assessment, verifiability of assessment process and computation of grades, and trusted sharing of learning or assessment logs along with final transcripts. The existing web or mobile applications are not right fit to overcome these challenges since they are centralized in nature. Thus, an interesting solution could be blockchain-based decentralized continuous assessment which allows transparency, security, verifiability, and trusted sharing.

The paper aims to contribute toward the development of decentralized continuous assessment by building a Blockchain and Flutter-based Quiz Mobile-Decentralized Application (BFQM-DApp). The front-end of the BFMQ-DApp is developed using flutter, while the back-end is made decentralized using blockchain technology along with smart contracts.

The main contributions of this paper are as follows.

- To propose a blockchain-based architecture for conduction of online quiz in an educational settings.
- To off-load the blockchain by securely storing the data in an off-chain distributed storage and pushing only the metadata on the blockchain.
- To implement the proposed architecture as a mobile application (BFMQ-DApp) using Flutter, Ganache (Ethereum) blockchain, smart contracts, and InterPlanetary File System (IPFS).
- To compute the cost of deploying various smart contracts designed to check the economic viability of the designed solution.

The demonstration video of the build BFMQ-DApp is available here[1].

Rest of the paper is organized as follows. Section 2 studies all the existing related works and distinguishes the current work. The proposed architecture and the overall flow is presented in Sect. 3. Section 4 provides the implementation details and discusses various smart contracts designed. The results are discussed in Sect. 5. Finally, Sect. 6 concludes this work.

[1] https://sites.google.com/view/blockchain-flutter-quiz-dapp/home.

2 Related Work

In recent years, blockchain has been considered an important technology for managing aspects of education ecosystem. Some of the applications of blockchain for education are (i) secure and privacy-protected sharing of degree and transcripts [5], (ii) secure and transparent admission process [6], (iii) scholarship management [7], (iv) prevention against degree certificate [8], and accreditation process [9]. One of the important aspects of the education is conduction of exams or quizzes toward continuous assessment. Some of the existing related works that make use of blockchain technology for secure, transparent, verifiable, and auditable conduction of examination are discussed below.

Shen et al. [10] emphasized on making the assessment process transparent and verifiable. More specifically, authors proposed the use of double-layer consortium blockchain for the conduction of quiz-based assessment. Here, students' answers for the questions rolled out during a quiz are stored of blockchain so that these can be publicly verified later. To overcome the issue of throughput and storage, authors used sharding technique where there is one main chain named as prime-chain and multiple sub-chains (shards) one sub-chain for each course. All the answer records are stored in prime-chain and sub-chains store only the summary. Moreover, use of group signature allows a teacher to completely trace any student inspite of pseudonymity. The paper not provides implementation details and experiment-based analysis.

Mitchell et al. [11] leveraged permissioned blockchain to make the examination reviewing process transparent and auditable. The examination reviewing process includes question paper creation, moderation, modification(s) if required, verification, and final submission. The authors proposed to shift this examination reviewing process on blockchain so that system can be secure, verifiable, and trustworthy. Authors used Hyperledger Fabric and Composer for implementation.

Tentea et al. [12] proposed a blockchain-enabled web application for online quiz that provides strong security against tampering of results. Authors used angular for front-end to develop interface. For back-end, they used firebase for real-time database and blockchain to store results. In addition to strong protection against result tampering, their web-based system provides single sign-in, quiz creation, and conduction. The work does not make use of any real blockchain platform and also does not provide cost estimation.

In [13], the authors aim at the issue of non-transparent and thus unreliable conduction of examinations. In particular, their focus is on making the assessment criteria (i.e., decision logic which is used to determine if the answer is correct or not) transparent with the use of blockchain. Authors implement their proposed solution using Bitcoin Core Testnet (public blockchain) and scoring server as back-end and web browser with a wallet enabled with ID and password as front-end.

Table 1 summarizes the related works and shows the clear distinction between these and our work. To the best of our knowledge, this is first work toward implementing blockchain and flutter-based mobile decentralized application for secure, transparent, and verifiable conduction of quiz.

Table 1 Comparison with the key related works

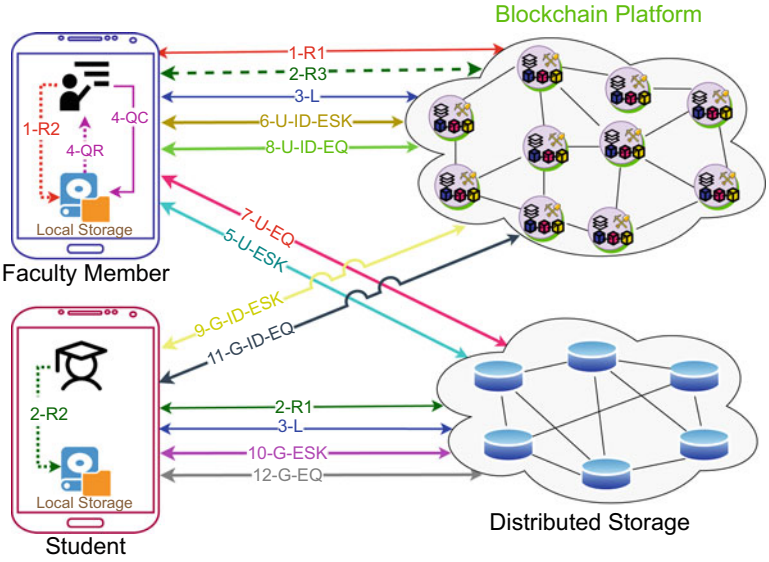
References	Aim	Implementation	Blockchain platform	Cost computed
[10]	Proposed use of double-layer sharding-based consortium blockchain for transparent and verifiable assessment process during conduction of quiz	No	–	No
[11]	Presented use of permissioned blockchain for secure, verifiable and auditable examination reviewing process	Yes	Hyperledger fabric and composer	No
[12]	Proposed a blockchain-enabled secure and tamper-proof web application for online quiz	Yes (web-based)	–	No
[13]	Proposed use of blockchain to make assessment criteria transparent and verifiable to avoid falsification of results and misjudgment	Yes (web-based)	Bitcoin core testnet	No
Our work	Propose and develop blockchain and flutter-based mobile quiz application for secure, transparent and verifiable conduction of quiz	Yes (mobile flutter-based)	Ganache (Ethereum)	Yes

3 Proposed Architecture

Figure 1 presents the proposed architecture for BFQM-DApp. There are four entities in the architecture: faculty member, student, blockchain platform, and distributed storage. Faculty members and students along with their mobile devices are the users and form the front-end of the DApp, whereas blockchain platform and distributed storage are at the back-end. Since storing all the quizzes directly on the blockchain would be expensive in terms of storage and transaction fee, thus the proposed architecture uses distributed storage. All the quiz-related data is stored in the distributed storage, and only the digital fingerprints are stored on the blockchain. In other words, we use distributed storage as off-chain storage to off-load the blockchain platform.

Faculty member, as a user, is allowed to perform following operations.

- **Approve Registration Request**: When a student registers for a course the request goes to the concerned faculty member (through blockchain platform). The faculty



1-R1: Registration (sign-up) of faculty member on blockchain platform.
1-R2: Encrypt the private key of faculty member with the password entered during previous step (1-R1) and store it in the local storage of phone. This private key is used to sign all the transactions.
2-R1: Registration (sign-up) of student on blockchain platform.
2-R2: Encrypt the private key of student with the password entered during previous step (2-R1) and store it in the local storage of phone.
2-R3: Send the registration request of student to the faculty member for approval.
3-L: Login of both type of users (faculty member and student).
4-QC: Quiz creation by faculty member (question-wise) and storing in the local storage of phone.
4-QR: Retrieve the quiz (JSON format) from the local storage.
5-U-ESK: Upload the Encrypted Session Key. A session key (created for every quiz) is encrypted using public keys of all the students and is uploaded on distributed file storage. An ID is returned from distributed file storage.
6-U-ID-ESK: Upload the ID received in previous step on blockchain.
7-U-EQ: Upload the Encrypted Quiz. The quiz is encrypted using the session key and then uploaded on distributed file storage. An ID is returned.
8-U-ID-EQ: Upload the ID received in the previous step on blockchain.
9-G-ID-ESK: Student (after login) gets ID of encrypted session key from blockchain.
10-G-ESK: Using ID received in previous step, get the encrypted session key from distributed file storage.
11-G-ID-EQ: Get ID of encrypted quiz from blockchain.
12-G-EQ: Using ID, get encrypted quiz from distributed file storage.

Fig. 1 Proposed architecture for BFQM-DApp

member after viewing the request and crosschecking the relevant details of the student can approve (or reject) the registration request. Rejection happens in case of fake registration request.
- **Create Quiz**: Faculty member can create a quiz by entering questions along with the correct answers and marking scheme (such as marks per question, time per question, negative marking).
- **Viewing of Results**: Once the students have attempted the quiz, the results can be viewed by the faculty members.

Student type user is allowed to perform following operations:

- **Request for Registration**: When a student wants to enroll for a course, s/he does the registration process. However, it is the concerned faculty member (delivering that course) who approves the registration request. On approval, a student gets successfully registered.
- **Attempt the Quiz**: At the time of assessment, faculty member rolls out the quiz and all the registered students are allowed to attempt the quiz.
- **Viewing of Results**: Like faculty members, students are also allowed to view the result. However, an individual can view only his/her marks and not of other students.

Note that faculty members also need to register and their registration can be approved by head of the department or institute. Furthermore, the registration of the head of the institute needs to be approved by some governmental apex body. However, the proposed architecture assumes that these steps are already in place.

The overall flow and brief explanation of all the steps involved is shown at the bottom of the same figure. The first number in the notation used for any step signifies the step number. Step 1 (1-R1 and 1-R2) is the registration of a faculty member. During this step, all the required details such as name, email address, and password (for login) are entered. Furthermore, the private key of the user is encrypted using the same password and stored in the local storage of the user's device. This private key is used to put digital signature every time a user performs a transaction. Step 2 is registration of student type user. Compared to the registration of a faculty member (i.e., step 1), there is one additional sub-step involved here (i.e., 2-R3). In this sub-step, the registration request of student is forwarded to the concerned faculty member for approval. Step 3 (i.e., 3-L) allows both faculty member and student type users to login by entering their password.

Step 4 is quiz creation by a faulty member. Since a faculty member may create a large pool of questions over a period of time, thus these questions are first stored in local storage of faculty member's device. Once the faculty member is done with all the questions, the final quiz is retrieved from the local storage as one single file. Now, if this quiz file is upload on distributed storage in plaintext, any attacker can apply brute-force attack and search entire distributed storage to retrieve the quiz. So in order to ensure strong security this quiz is first encrypted and then uploaded on distributed storage. To do so, a *unique session key* is created for every quiz. Upon creation of a session key, this session key is encrypted with every student's public

key and the final set of encrypted session keys are uploaded on the distributed storage (i.e., Step 5-U-ESK). On successful uploading, a unique ID is returned by distributed storage to faculty member, and this ID is then uploaded on the blockchain platform (i.e., Step 6-U-ID-ESK). In the step 7-U-EQ, the session key is used to encrypt the single quiz file and then upload the encrypted quiz on distributed storage. The ID returned is uploaded on the blockchain platform, i.e., step 8-U-ID-EQ.

In step 9-G-ID-ESK, student logins and gets the ID of encrypted session key from blockchain platform. Then in step 10-G-ESK, student retrieves the set of encrypted session keys and decrypts the session key using her/her private key. In step 11-G-ID-EQ and step 12-G-EQ, student gets the ID of encrypted quiz from blockchain and then retrieves the encrypted quiz from distributes storage, respectively. Finally, using the session key, student decrypts and attempts the quiz. The result of the quiz is uploaded on the blockchain by every student.

4 Implementation

To implement the proposed architecture, we have developed a decentralized application (BFQM-DApp) using different technologies and platforms. Table 2 summarized various technologies and platforms used. The back-end of BFQM-DApp consists of Ganache (Ethereum) blockchain plus InterPlanetary File System (IPFS). The former serves as blockchain platform, whereas the latter works as distributed storage. When any data or content is uploaded on IPFS in return the sender gets a Content Identifier (CID) which can be later used to retrieve the data. The front-end of the developed DApp comprises flutter-based mobile application which makes use of Web3 to interact with decentralized back-end.

IPFS is used for storing large quiz related data to reduce the cost. However, if we store the data on IPFS in plaintext, then attacker can apply brute-force attack to retrieve the quiz. Thus to ensure the overall security, BFQM-DApp encrypts all the data before storing on IPFS. To do so, our implementation generates an additional pair of public private keys since the encryption and decryption is not possible with key pair provided by Ganache blockchain. This additional key pair is generated at the time of registration using OpenPGP library. Thus, every user has two set of public private key pair, one provided by Ganache platform and second additionally generated. This second key pair is used for encryption and decryption of session key of every quiz.

4.1 Designed Smart Contracts

Four different smart contracts are designed for the developed BFMQ-DApp. Brief description of these smart contracts are as follows.

User Contract: This smart contract defines the structure of users' data and consists of member function for registering a new user. In particular, it has the logic

Table 2 Summary of technologies and platforms used

Technology/platform	Description
Flutter	Flutter [14] is a mobile app development framework that allows for the creation of apps for Android and iOS platforms. It was developed by Google and uses the Dart programming language
Ganache	Ganache [15] is a tool that allows developers to quickly set up a virtual blockchain for testing and development purposes
Web3	Web3 [16] is a library that allows developers to interact with the Ethereum blockchain from within a web application. It provides an API for reading and writing smart contract data, as well as for sending transactions on the network
IPFS	InterPlanetary File System [17] (IPFS) is a protocol and network designed to create a peer-to-peer method of storing and sharing hypermedia in a distributed file system. In IPFS, files are identified by their content, rather than by their location, which allows for a more robust and resilient file sharing system
Truffle	Truffle Suite [18] is a set of development tools for Ethereum blockchain development. It includes Truffle, a development environment, testing framework, and asset pipeline for Ethereum
OpenPGP library	OpenPGP [19] is a widely used library that provides cryptographic functions such as encryption and signing, to secure communication and data files. It is based on the OpenPGP standard and uses public key cryptography, allowing users to encrypt messages using the recipient's public key and decrypt them using their own private key

of (i) creating the student and faculty member user, (ii) retrieving the user details, (iii) updating the user details, and also the logic for verifying a student registration request by a faculty member.

Quiz Contract: As the name implies, this contract defines the structure used of quiz related data. The contract provides all the functionalities required for creating, encrypting, and uploading a quiz. More specifically, this contract consists of logic for (i) creating a quiz in JavaScript Object Notation (JSON) format, (ii) encrypting and uploading a quiz on IPFS, and (iii) pushing the CID (of the encrypted quiz) received from IPFS on the Ganache blockchain.

PublicKey Contract: This contract defines the structure of public key data which is mapped uniquely to user address. Various functionalities provided by this contract are (i) adding the public key to the blockchain according to each user enrollment address and (ii) retrieving the public key arrays for the encryption and decryption process of quiz data.

Result Contract: This contract maps each student's result for every quiz according to the quiz ID and user address. The mapping helps in easy retrieval of result data and verification as and when required.

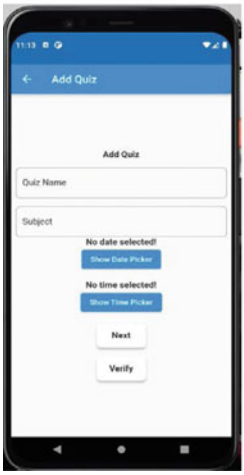
Further details of the smart contract can be found at[2].

[2] https://sites.google.com/view/blockchain-flutter-quiz-dapp/home.

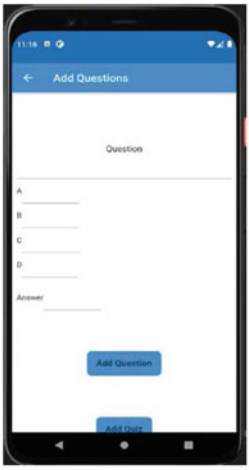
Landing Page

Signup (Registration)

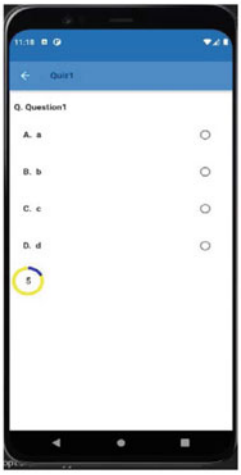
Sign-in



Quiz Creation



Add Question



Attempting Quiz

Fig. 2 Various snapshots of BFQM-DApp

Table 3 Various costs of smart contracts developed

Contract name	Cost (Gwei)	Cost (Ether)	Cost (USD)	Gas used	Gas limit
User contract	27,738,160	0.02773816	36.94	1386908	2,000,000
Quizzes contract	16,804,838	0.016804838	22.38	840242	2,000,000
PublicKeys contract	13,022,700	0.0130227	17.34	651135	2,000,000
Results contract	7,185,920	0.00718592	9.57	359296	2,000,000

1 Gwei = $1/10^9$ Ether, gas price = 20 Gwei, and 1 Ether = $ 1331.75 on Jan 10, 2023

5 Results and Discussion

The decentralized application (i.e., BFQM-DApp) has been successfully implemented and tested. Figure 2 shows snapshots of various steps such as landing page, sign-up, login, quiz creation, adding a question to quiz, and attempting a quiz.

Furthermore, the cost analysis of the smart contracts designed has been carried out to check the economic viability. Miners participating in Ethereum P2P network need to be incentivized for the resources they are offering. Thus, deployment of smart contracts on top of blockchain incurs some cost. Table 3 shows the cost (in Gwei, Ether, and USD), gas used, and gas limit set during computation for the four different smart contracts. These costs are computed using Ganache, and gas price is set equal to 20 Gwei.

6 Conclusion

The paper has proposed an architecture for a blockchain-enabled quiz mobile application named BFQM-DApp. The proposed architecture enables secure, transparent, and verifiable conduction of online quiz toward continuous assessment. For the proof of concept, we implemented the BFQM-DApp using Ganache blockchain which acts as a back-end. Flutter has been used to design the front-end, and Web3 has been leveraged to interact with decentralized back-end. Furthermore, IPFS has been used as decentralized (off-chain) storage. Four different smart contracts have been designed to encode various functionalities. The deployment cost of the smart contracts is also computed to check the economic viability. The future scope of the work includes latency computation, detailed cost computation of various functionalities (in addition to the costs of the designed smart contracts), and security analysis of overall applications. Since latency is an important factor, and it is also blockchain (type and) platform dependent, thus in the future we plan to implement the proposed architecture on hyperledger fabric blockchain as well and provide a comparative results.

References

1. Oli G, Olkaba T (2020) Practices and challenges of continuous assessment in colleges of teachers education in west Oromia region of Ethiopia. J Educ Teach Learn 5(1):8–20
2. Hernández R (2012) Does continuous assessment in higher education support student learning? Higher Educ 64(4):489–502
3. Peytcheva-Forsyth R, Saev S, Yovkova B (2021) Integrated continuing assessment in an online course as a mechanism for a smoother transition from face-to-face to distance learning. In: AIP conference proceedings, vol 2333. AIP Publishing LLC, p 050014
4. Commission UG (2023) Blended mode of teaching and learning: concept note. Available at https://www.ugc.ac.in/pdfnews/6100340_Concept-Note-Blended-Mode-of-Teaching-and-Learning.pdf. Accessed on 15 Jan 2023
5. Mishra RA, Kalla A, Braeken A, Liyanage M (2021) Privacy protected blockchain based architecture and implementation for sharing of students' credentials. Inf Proc Manag 58(3):102512
6. Kutty RJ, Javed N (2021) Secure blockchain for admission processing in educational institutions. In: 2021 international conference on computer communication and informatics (ICCCI). IEEE, pp 1–4
7. Tekguc U, Adalier A, Yurtkan K (2020) Scholarchain: the scholarship management platform with blockchain and smart contracts technology. Eurasia Proc Educ Soc Sci 18:86–91
8. Tariq A, Haq HB, Ali ST (2022) Cerberus: a blockchain-based accreditation and degree verification system. IEEE Trans Comput Soc Syst
9. Cahyadi D, Faturahman A, Haryani H, Dolan E, Millah S (2021) BCS: Blockchain smart curriculum system for verification student accreditation. Int J Cyber IT Service Manag 1(1):65–83
10. Shen H, Xiao Y (2018) Research on online quiz scheme based on double-layer consortium blockchain. In: 2018 9th international conference on information technology in medicine and education (ITME). IEEE, pp 956–960
11. Mitchell I, Hara S, Sheriff M (2019) Dapper: decentralised application for examination review. In: 2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3). IEEE, pp 1–14
12. Tentea EC, Ionescu VM (2019) Online quiz implementation using blockchain technology for result tampering prevention. In: 2019 11th international conference on electronics, computers and artificial intelligence (ECAI). IEEE, pp 1–6
13. Kaneko Y, Tanaka S, Kimura T, Okumura J, Azuchi S, Osada S (2021) Deexam: a decentralized exam administration model using public blockchain. In: 2021 3rd blockchain and internet of things conference. pp 1–7
14. Flutter. Available at https://flutter.dev/. Accessed on 15 Jan 2023
15. Ganache. Available at https://trufflesuite.com/ganache/. Accessed on 15 Jan 2023
16. Web3. Available at https://web3js.readthedocs.io/. Accessed on 15 Jan 2023
17. IPFS. Available at https://docs.ipfs.tech/. Accessed on 15 Jan 2023
18. Truffle. Available at https://trufflesuite.com/docs/truffle/. Accessed on 15 Jan 2023
19. Openpgp. Available at https://www.openpgp.org/software/developer/. Accessed on 15 Jan 2023