Empowering Students with Blockchain: Rethinking Traditional Educational Record Systems

Abha Desai
Second year BSc student in Computer Science
School of Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
ad6g23@soton.ac.uk

Abstract

In the age of Big Data, maintaining the security and integrity of personal records has become increasingly important in educational institutions. Without implementing the necessary security measures, data stores become vulnerable to different forms of cyber-attacks. As the techniques used by cyber-attackers improve, so must the institute's system. Implementing a blockchain-based records system is a potential solution to this problem. Blockchain technologies produce a decentralized platform, increasing efficiency and speed for transactions as well as ensuring the authenticity of the records stored. This research demonstrates how blockchain can be incorporated to improve the safety of student records, whilst still considering the ethical and technical limitations this change could bring. It also suggests how blockchain's immutable feature would be adapted to GDPR legislation, preventing legal infringements.

ACM Reference Format:
Abha Desai. 2025. Empowering Students with Blockchain: Rethinking Traditional Educational Record Systems. In *Proceedings of 12th ACM Celebration of Women in Computing (womENcourage 2025).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction and motivation

Record management has always been a key feature of university administration. With the introduction of data protection laws such as the Data Protection Act 2018, the General Data Protection Regulation (GDPR), and the Privacy and Electronic Communications Regulations (PECR), protecting student data is a priority. Hence, organisations are being encouraged to look at their existing systems and improve them.

Research from multiple sectors, including healthcare and finance, highlights the benefits of hybrid approaches to resource management. However, Electronic Records Management Systems (ERMS) adoption remains inconsistent, and risks to data integrity persist.

womENcourage 2025, Braşov, Romania

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2 What is Blockchain?

Blockchain is a distributed digital ledger of events, where data items are linked and stored across all participating nodes. Each node performs "mining" operations, verifying transactions through consensus mechanisms. This architecture makes data tampering and unauthorised access exceedingly difficult. [5]. This would improve the integrity of student records drastically.

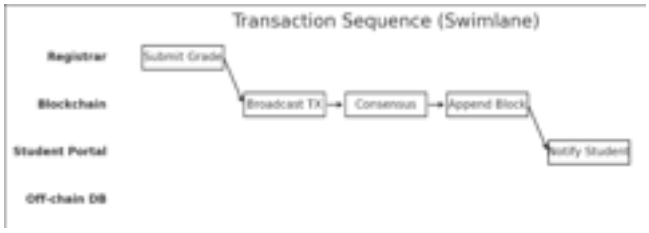

Figure 1: Transaction sequence swimlane.

3 Advantages of Using Blockchain

Blockchain can vastly improve interoperability between institutions (for example, sharing student records seamlessly across universities). [9]. By giving each institution its own node in a distributed ledger, blockchain eliminates tiresome admin-required data-transfer protocols and ensures that every node holds the same up-to-date information. Moreover, students today often lack visibility into which staff access their records; adapting MIT Media Lab's approach of public-key identity verification with off-chain data exchange [2], would let students grant or revoke access themselves, putting them firmly in control of their personal data.

Sharples and Domingue [11] identify key advantages:

- **Resilient, Distributed Storage**: Data remains intact even if individual nodes fail.
- **Authenticated Modifications**: Every change is tied to a verified identity, enabling trust and accountability in any changes.

4 Limitations

While blockchain boosts security and transparency, it also introduces challenges. For example, system performance can decrease due to the consensus protocol, which consumes large computing resources and energy, causing long system latency [1]. A fully decentralised network depends on trustworthy nodes. Malicious actors or "selfish miners" can exploit mining forks to gain unfair

advantage and threaten the chain's integrity [8]. Further, the cost of maintaining anonymous, trustless consensus may exceed the value of protection, posing a higher risk from blockchain compared to the advantages it provides [3]. A possible mitigation is to select primary nodes from a limited number of trusted nodes, and to prevent high system latency: choosing a consensus algorithm to decrease network broadcasting [1].

The concept of selfish mining can also 'fork' the whole chain within the system [8]. This is due to malicious miners selectively revealing mined blocks instead of immediately showing them. This allows them to command a relatively small portion of the total mining power while collecting higher revenues than honest miners, gaining an unfair advantage in a supposedly fair, decentralised network.

A key concept of blockchain is the anonymous, decentralised trust within the system. However, this is a lot more expensive and possibly dangerous than expected [3]. The flow cost of running the blockchain must be compared to the one-shot value of attacking it. If the value of attack is higher, the entire system is jeopardised and vulnerable to sabotage. This is a precarious position for a university management system to be in, as one would be held accountable for the possible data leakage of tens of thousands of students' sensitive information.

5 Ethics of using Blockchain for Student Data

Many authors have stated that there is a large gap in the literature available in regards to the ethics of blockchain within various fields [7, 12]. GDPR mandates data erasure upon request, which conflicts with blockchain's immutability [4]. Lemieux et al. [10] argue that blockchain could improve transparency by logging data access, but practical implementation remains uncertain. Due to blockchain's decentralised levels, managing access rights would also be challenging - this must be taken into consideration during designing and implementation.

A significant ethical issue arises from the lack of a centralised service provider: all participants in a blockchain network may be able to view all stored data [12]. In an educational context, this could result in students being able to see each other's personal data, which is unacceptable.

Fortunately, different types of blockchain networks can be implemented: **Public**, for permissionless access; **private**, controlled by a single central authority; and by **consortium**, governed by a group with controlled permissions. In general, consortium blockchains are recommended. Using a private blockchain places too much power in one authority, increasing the risk of a single point of failure or vulnerability [13]. This is shown further in Figure 2.

6 Privacy and GDPR

Despite growing interest in blockchain for record management, scholars warn that its ethical implications remain under-explored [7, 12]. In a permissionless public ledger, any node can view all entries. This raises serious privacy concerns in education, where students must not access one another's grades or personal data. A consortium blockchain (where a vetted group of institutions governs permissions) strikes a balance between transparency and confidentiality, avoiding both single-authority vulnerabilities and

Figure 2: Performance across various Blockchain types.

unrestricted data visibility. Its performance is shown in Figure 2 above.

7 Conclusion

Consortium blockchain presents a promising solution for managing student records securely. Yet its heavy consensus processes can introduce performance and latency challenges. In addition, concerns about ethics, and legal compliance, especially regarding GDPR, must be addressed. Further research is essential before full-scale deployment. VerifyB [6] is a notable example of a blockchain-based student records system worth exploring before any large scale adoption.

References

[1] A. et al. Abdelmaboud. 2022. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* 11, 4 (2022), 630.
[2] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. 2016. MedRec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 25–30.
[3] E. Budish. 2018. The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper* 24717 (2018).
[4] A. Calder. 2017. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Publishing.
[5] A. Capetillo, D. Camacho, and M. Alanis. 2022. Blockchained education: challenging the longstanding model of academic institutions. *International Journal on Interactive Design and Manufacturing* 16, 2 (2022), 791–802.
[6] A. Desai, P. Shah, and D.D. Ambawade. 2021. VerifyB: Students' record management and verification system. In *2021 International Conference on Communication Information and Computing Technology (ICCICT)*. IEEE, 1–6.
[7] C. Dierksmeier and P. Seele. 2019. Blockchain and business ethics. *Business Ethics: A European Review* 29, 2 (2019).
[8] I. Eyal and E.G. Sirer. 2018. Majority is not enough: Bitcoin mining is vulnerable. *Commun. ACM* 61, 7 (2018), 95–102.
[9] M. Kataev and L. Bulysheva. 2022. Blockchain system in the higher education: Storing academical students' records and achievements. *Systems Research and Behavioral Science* 39, 3 (2022), 589–596.
[10] V. et al. Lemieux. 2019. Blockchain technology & recordkeeping. *ARMA International Educational Foundation* (2019).
[11] M. Sharples and J. Domingue. 2016. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In *Adaptive and Adaptable Learning*. Springer, 490–496.
[12] Y. et al. Tang. 2020. Ethics of blockchain. *Information Technology & People* 33, 2 (2020), 602–632.
[13] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 557–564.