Smart Learning Environments

RESEARCH

Open Access

Zero-knowledge proofs in education: a pathway to disability inclusion and equitable learning opportunities

Xiao Xu[1*]

*Correspondence:
x.xu@unsw.edu.au

[1] UNSW Sydney Business School, University of New South Wales, Kensington, NSW 2052, Australia

Abstract

In the evolving landscape of global education, the significance of inclusivity and equity has never been more important. Emphasizing the United Nation Sustainable Development Goal 4, this paper explores the innovative application of blockchain-powered Zero-Knowledge Proofs (ZKPs) technology in education, with a particular focus on disability inclusion. This study introduces a novel disability management system powered by Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK). This advanced system enables educational institutions to verify the status of students with disabilities without compromising their personal information, thereby preserving their privacy and reinforcing their identity. This paper evaluates the potential operational efficiency of this prototype system against the existing costs incurred by higher education institutions in disability schemes. It also examines the system's potential to enhance self-disclosure among students with disability, which is pivotal for their academic success. By advocating for privacy and inclusivity, this study highlights the transformative potential of ZKP in creating an educational environment where students with disabilities can comfortably disclose their needs. This approach not only protects their confidentiality but also empowers them academically, aligning with the global commitment to accessible and inclusive education.

Keywords: Blockchain, Zero-knowledge proof, Disability inclusion

Introduction

The concept of Zero-Knowledge Proofs (ZKPs) originated in cryptography as a component of interactive proof systems. A ZKP allows one party, the prover, to demonstrate to another party, the verifier, that they possess certain knowledge without revealing the information itself (Goldwasser et al., 1985). In identification schemes, the proof of knowledge can be established using computational identification protocols, moving beyond certifying mere assertions. Recently, this concept has been adopted by blockchain platforms as a means to prove possession of sensitive data without revealing it, addressing growing privacy concerns. Some applications include data-minimized anonymous credentials in digital wallets (Babel & Sedlmeir, 2023) and the use of blockchain-based ZKP in city traffic management systems (Li et al., 2020). While the educational

sector has seen numerous applications of blockchain, the ZKP technology has yet to be fully studied. This paper explores the potential of ZKPs to support inclusive education, in line with the United Nations Sustainable Development Goal 4 (UN SDG 4), which aims to ensure inclusive and equitable quality education for all. This leads us to the central research question: 'How can the application of ZKP technology improve the confidentiality and protection of sensitive data for students with disabilities?' We will specifically examine how implementing ZKP systems can enhance self-disclosure among these students and contribute to their academic success, thereby aligning with UN SDG 4 objectives. Additionally, we will explore how ZKPs can improve efficiency in university administrative operations.

Literature review

Blockchain technology, through its distributed ledger system, offers a method for storing and sharing information among participants. Transaction records on the blockchain are permanent, transparent, and immutable. Once a block of transactions is verified and added to the blockchain, it cannot be altered. Over the past decade, blockchain technology has seen significant growth with applications such as InterPlanetary File System (IPFS), smart contracts, and decentralized finance (DeFi) among others.

In the realm of education, blockchain technology offers numerous potential applications due to its inherent trustworthiness, immutability, transparency, and self-sovereignty. One of its most widely recognized applications in recent years pertains to certificate management, the tracking of competencies, and the definition of learning objectives, all of which bolster the concept of lifelong learning. The capability of blockchain to maintain comprehensive lifelong learning logs allows learners to prioritize the storage of detailed data over merely possessing a diploma (Ocheja et al., 2019). University credits, which resemble some features of tokens in the blockchain world, can be authenticated by blockchain-powered higher education institutions. This capability enables universities to seamlessly issue degrees via the blockchain (Grech & Camilleri, 2017). Additionally, academic records can be securely shared and verified (Arenas & Fernandez, 2018), making credit transfers for students more efficient due to the immutable nature of records on a public ledger (Turkanović et al., 2018).

Raimundo and Rosário (2021) noted that in addition to supporting the accreditation of authentic certificates or academic data, blockchain technology promotes a decentralized learning infrastructure for all stakeholders on the network. This makes it a valuable tool for various educational processes. Furthermore, it can also provide feedback for teacher evaluations through carefully designed smart contracts (Chen et al., 2018). The details of smart contract-based learning system can be developed to fit different online learning purposes (H. Sun et al., 2018; X. Sun et al., 2021b). A peer-to-peer (P2P) network can be developed to bridge the gap between the academic theory and real-world practices (Lizcano et al., 2020). The prospect of low-cost blockchain accreditation for work-based learning achievements is particularly appealing (Williams, 2019).

Despite the advantages, Alammary et al. (2019) highlighted nine different challenges that blockchain may face, including scalability. As the number of blocks increases, transaction latency will also increase. Another significant challenge is privacy, which is further complicated by security concerns such as cyber risks and data leaks. Li et al. (2022)

emphasized that all transaction records in the blockchain must be disclosed to all nodes, which significantly increases the risk of privacy leakage. They also highlighted the potential use of ZKP as a solution to protect privacy and ensure calculation verification. The ZKP protocol enables the prover to confirm the accuracy of a statement to a verifier without revealing the underlying information. This not only enhances data privacy and confidentiality but also provides benefits such as reduced computations, since validators only need to verify the proofs (Berentsen et al., 2023). ZKP has been increasingly integrated into blockchain technology to improve scalability and address the issue of high transaction gas fees. Methods such as ZKP are recommended to safeguard the privacy of biometric data for identification, with an emphasis on intelligent proctoring systems and identification methods (Portugal et al., 2023). The ZKP computational structure can address issues related to personal data privacy when exchanging information between the educational agencies (Yin, 2023). However, to the best of the authors' knowledge, the potential of ZKP to support inclusive education especially in relation to disability has yet to be fully explored.

The United Nations has defined Sustainable Development Goal 4 (SDG 4) as ensuring inclusive and equitable quality education for all (United Nations, 2015). Kwok and Treiblmaier (2022) emphasize the potential of blockchain technology in fostering social inclusion and enhancing access to education. Alongside blockchain, the advent of mobile technologies, cloud computing, the Internet of Things (IoT), and artificial intelligence has seen Information and Communication Technologies (ICTs) increasingly support students with disabilities (Fichten et al., 2020). Successful implementation of these technologies can greatly benefit such students, fostering inclusion in the classroom (Fernández-Cerero et al., 2023; Perera-Rodríguez & Moriña Díez, 2019). However, the training of teaching staff becomes crucial when introducing new technologies. Without proper adaptation and training, there is a risk that these tools might inadvertently become obstacles, potentially leading to the marginalization of students with disabilities.

Due to technological advancements, the construction of self and identity processes are undergoing significant shifts. Maintaining anonymity and ensuring the privacy of certain information have become key concerns in the digital age (Muñoz-Rodríguez et al., 2022). L. Li and Ruppar (2021) highlight that an inclusive teacher identity is a foundational pillar in the conceptual framework for inclusive education, promoting equal status in collaborative teaching partnerships. While most disabilities do not prevent students from pursuing higher education, individual competencies can differ widely. Such differences necessitate various accommodations and require a case-by-case analysis for special considerations. This further elaborates on the challenges faced by the behavior intervention teams when addressing individuals with psychiatric disabilities, particularly in relation to potential overreporting and confidentiality issues.

In this paper, we explore the application of ZKPs in supporting students with disabilities through a three-fold approach. First, we analyze the structure of the ZKP algorithm, highlighting its inherent design for privacy protection. This analysis provides technical insights, positioning ZKP as a promising tool for safeguarding sensitive student data, especially for those with disabilities. Second, we evaluate the operational benefits of integrating a prototype ZKP system into administrative processes within educational institutions, focusing on efficiency gains and gas fees on the Ethereum network. Third,

Table 1 ZKP Four-Step Algorithm

Step	Purpose
Commit () → r	The algorithm provides a commitment r, which can verify the correctness of the proof about the secret s
Challenge () → e	The algorithm creates a random challenge e, which the verifier sends to the prover
Prove (e, ω, k) → s	The algorithm yields a proof s computed using the given e, the witness ω, and a random string k
Verify (r, e, s) → {1, 0}	The verification algorithm returns 1 if the verification result is accurate; if not, it returns 0

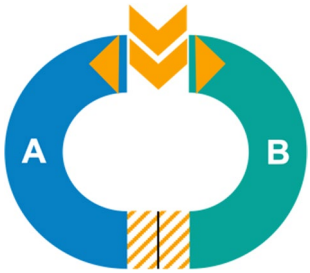

Fig. 1 Ali Baba Cave illustration

we examine how ZKPs can facilitate self-disclosure for students with disabilities, contributing to the establishment of their identities and enhancing academic outcomes. This study underscores the role of ZKP in promoting inclusive education.

Methods

ZKPs are a cutting-edge technology designed to enhance privacy by minimizing the amount of information shared between users in digital interactions. In addition, ZKPs expedite the verification process in open systems by omitting unnecessary details. In this section, we outline the algorithmic framework of ZKPs, presenting both the structural architecture and the specific pseudo-code for disability management design within the blockchain world. We also examine the implementation of a specific non-interactive ZKP type, known as Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs), which greatly enhances scalability on the Ethereum network.

Algorithmic structure for privacy

In the ZKP process, the primary parties involved are the prover, who aims to validate their knowledge of a secret without revealing it, and the verifier, who assesses the validity of the prover's claim without accessing sensitive information. This mechanism encompasses a four-stage procedure: commitment, challenge, proof, and validation, as outlined in Table 1 (Chi et al., 2023).

One of the commonly used illustrations to explain the ZKP protocol is the Ali Baba Cave example (Quisquater et al., 1990). In the city of Baghdad, Ali Baba, discovers a mysterious cave with two passages labeled A and B, each leading to what appears to be a dead-end door, as shown in Fig. 1. Each time he pursued a thief into the cave, the thief would vanish, no matter which passage Ali Baba chose to search.

After many failed attempts, Ali Baba discovers a hidden mechanism: by whispering a magic word "Open sesame," a hidden door opens as shown in Fig. 2, connecting the two passages. This secret allows the thieves to consistently evade Ali Baba by switching between the passages. The enigma of this cave emphasizes the theme of proving knowledge without revealing the secret.

In this example, the four-step algorithm can be analyzed as follows:

- Commit: After being robbed repeatedly, Ali Baba observes the thieves' pattern of escaping into the cave. Upon entering, each thief commits to a path, either A or B.
- Challenge: Seeking to catch the thief, Ali Baba enters the cave and must choose which path to search: A or B. His choice represents the challenge.
- Prove: In response to Ali Baba's challenge, the thief must prove their knowledge of the cave's secret. By using the magic words to open the secret door, the thief can escape depending on the path Ali Baba selected.
- Verify: Observing the consistent success of the thieves in evading him, Ali Baba concludes that they have knowledge of the cave's secret. Their consistent ability to escape through the opposite path serves as the confirmation of the knowledge.

Through probabilistic evaluations, Ali Baba's confidence in the thief's knowledge of the cave's secret grows. The more frequently the thief successfully disappears, the stronger Ali Baba's conviction becomes. However, this method does not provide definitive proof in the same way that disclosing all the information would.

The aforementioned algorithm can be generalized to a situation where a student with a disability needs to demonstrate to a university (symbolized by the cave) that their need for specific accommodations due to their condition. They aim to keep the exact nature of their disability confidential. Every time the student engages with the university, they commit to a particular path: either A (representing one type of proof) or B (indicating another type of proof). The university, in its pursuit of ensuring equitable treatment, challenges the student to prove their need for accommodations without revealing their exact disability.

The university can opt to challenge the student via path A or B, each representing different methods of verification. In response to the university's challenge, the student can use the magic words (akin to a digital signature) that validate their need without disclosing the specifics of their disability. This act of providing the correct proof in response to the university's challenge serves as evidence of their genuine need. By observing the

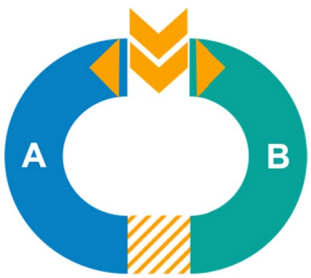

Fig. 2 Ali Baba Cave illustration with hidden door

consistent pattern of responses and the legitimacy of the proofs provided, the university can confirm the student's genuine need for accommodations. The student's consistent ability to provide the correct proof serves as confirmation of this knowledge.

It presents the blockchain-based ZKP network structure for students' disability management in Fig. 3. Each time the university sends a request to the prover (students with a disability), the students create proof using the ZKP algorithm. Upon successful verification, the university can confirm the students' needs through the verifier, without the need to disclose the confidential details of the students' conditions each time. With this structure, the university ensures that students receive the necessary support while maintaining the confidentiality of their specific disabilities, striking a balance between necessary verification and privacy.

Non-interactive ZKPs for scalability

Non-Interactive Zero-Knowledge Proofs (NIZKPs) allow the prover to confirm shared data with the verifier without the need for continuous back-and-forth exchanges between the parties (Ben-Sasson et al., 2014). In contrast, Interactive Zero-Knowledge Proofs (IZKPs) are achieved through an interactive exchange protocol, which involves a sequence of challenge-response interactions between the verifier and the prover. Unlike IZKPs, NIZKPs enable the prover to generate the proof in a single step, offering computational advantages. While Table 2 summarizes the key differences between IZKPs and NIZKPs, this discussion specifically focuses on NIZKPs.

A Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a cryptographic technique that allows an individual to demonstrate the authenticity of a claim without disclosing any detailed information about the claim and without any prior communication between the involved parties (Groth, 2010). A zk-SNARK method must satisfy the following four fundamental principles (ElSheikh & Youssef, 2023):

1. Perfect Completeness: For every valid statement paired with its corresponding valid witness, an honest prover will always convince an honest verifier.

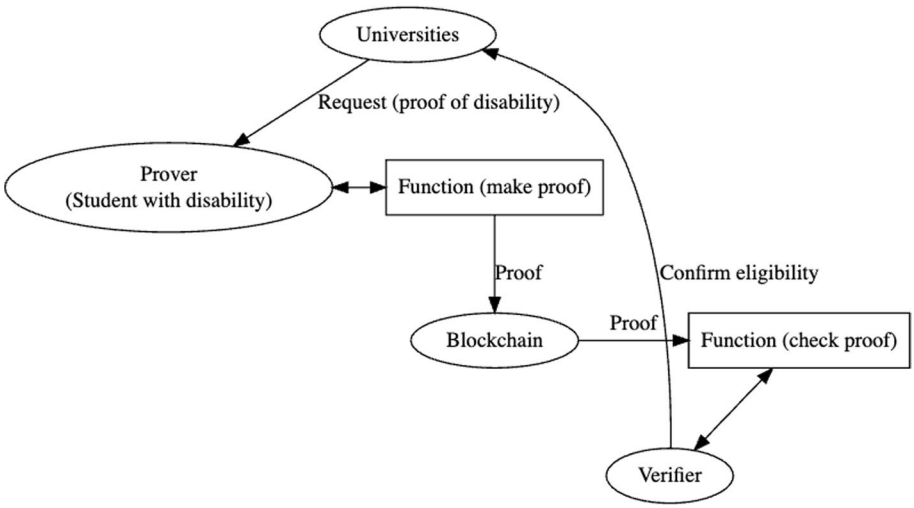

Fig. 3 Interactive workflow for student disability management using blockchain-based ZKPs

Table 2 Comparative Analysis of IZKPs and NIZKPs

Feature/type	IZKPs	NIZKPs
Interactivity	Involves back-and-forth communication between the prover and verifier	Relies on a single message from the prover to the verifier without further interactions
Proof Generation	Proof generation hinges on an interactive exchange protocol	Allows for one-step proof generation by the prover
Process	Characterized by a sequence of challenge-response interactions	Noted for offering computational advantages, minimizing interactive overhead
Versatility	Widely foundational, forming the basis for many cryptographic protocols	Often evolve from IZKPs via specific transformations
Security	Founded on diverse cryptographic assumptions and predicated on both parties adhering to the protocol during interaction	Built on certain assumptions, especially those pertaining to the non-interactive transformation. Some may also depend on trusted setups
Efficiency	Can be less efficient due to potential multiple rounds of communication	Highly efficient in contexts where ongoing interaction is impractical or resource intensive

2. Computational Soundness: A malicious prover, even with significant computational power, cannot convince the verifier of an incorrect statement.
3. Computational Zero-Knowledge: Even with an honestly generated proof, an adversary cannot extract any information about the witness.
4. Succinctness: The proof generated is concise and the verification process is efficient, running in polynomial time based on the security parameter.

The application of zk-SNARKs in a disability management system can be designed as shown in Fig. 4.

The system is designed to manage and support students with disabilities in a university setting using zk-SNARKs and smart contracts. Initially, an administrator and eligible students participate in a setup ceremony to generate cryptographic keys for various arithmetic circuits. The administrator then creates a list of eligible students and deploys a smart contract, setting the stage for the subsequent phases. Students provide cryptographic proof of their disability status to ensure that only eligible students can register and benefit from the system. Following registration, students document their required adjustments, which are cryptographically verified and stored securely on the blockchain. After gathering all the adjustment documents, the administrator proceeds to the support generation phase, where a comprehensive support plan is created based on the individual needs of the students. This plan is also cryptographically verified and stored on the blockchain. This entire process ensures transparency, security, and privacy, allowing universities to cater to the needs of students with disabilities efficiently and confidentially.

Results

The results section focuses on two main areas: evaluating the cost-effectiveness of implementing the ZKPs algorithm and assessing its impact on self-disclosure among students with disabilities.

Algorithm implementation and cost analysis

We deployed a zk-SNARKs-based smart contract for managing students' disabilities on the Ethereum network and analyzed the associated transaction cost. Our open-source

```
Initialize:
  - Create an empty list of students: `studentList = []`
  - Create an empty list of accommodations: `accommodationList = []`

Function ADD_STUDENT(studentID, studentName, disabilityProof):
  - Create a new student object: `student = {ID: studentID, Name: studentName, Proof:
disabilityProof, Accommodations: []}`
  - Add student to `studentList`

Function ADD_ACCOMMODATION(accommodationName, description):
  - Create a new accommodation object: `accommodation = {Name: accommodationName,
Description: description}`
  - Add accommodation to `accommodationList`

Function PROVE_DISABILITY(studentID, zkProof):
  - Find student with `studentID` in `studentList`
  - If zkProof validates the student's disability without revealing specifics:
    - Mark student as verified

Function ASSIGN_ACCOMMODATION(studentID, accommodationName):
  - Find verified student with `studentID` in `studentList`
  - If student found:
    - Find accommodation with `accommodationName` in `accommodationList`
    - If accommodation found:
      - Add accommodation to student's Accommodations list

Pre-defined zk-SNARK Functions:
  - Mux(s, P, Q): Returns P if selector s=0, and Q if s=1
  - LessThan(a, b): Returns 1 if a<b, and 0 otherwise
  - GreaterThan(a, b): Returns 1 if a>b, and 0 otherwise
  - CompC(a, c): Returns 1 if a>c, and 0 otherwise (where c is a constant)
  - Bits2Num(a0,...,ak-1): Returns integer number represented by bits a0,...,ak-1
  - IsPoint(x, y): Returns 1 if the pair (x, y) is a point on the elliptic curve, and 0 otherwise
  - IsEqual(P, Q): Returns 1 if the two points P and Q are equal, and 0 otherwise
  - eADD(P, Q): Point addition (P+Q) on the elliptic curve
  - eSUB(P, Q): Point subtraction (P-Q) on the elliptic curve
  - eScalarMUL(a, P): Scalar multiplication (aP) on the elliptic curve
```

Fig. 4 Disability management system pseudo-algorithm with zk-SNARKs

prototype provides a practical demonstration of the zk-SNARKs application. We measured the contract's execution cost at 660,478 gas units, indicating the computational effort required to process and integrate the transaction into the blockchain. Moreover, the on-chain verification transaction, which assures the validity and integrity of the zk-SNARKs proofs, consumed 1,195,474 gas units. It is noted that as the user base grows, we anticipate a linear increase in transaction costs, highlighting the scalable nature of the verification process.

We further assessed this technology's real-world feasibility by reviewing the costs associated with supporting individuals with disabilities in higher education settings. According to Pitman et al. (2022), the Australian government allocated approximately 7.6 million AUD to the Disability Support Fund (DSF) in 2019. A significant portion of this fund, 84.7%, was designated for the Additional Support for Students with Disabilities (ASSD), which was primarily dedicated to reimbursing the costs incurred in providing educational support and equipment for students with disabilities. From 2015 to 2019, universities claimed an annual average of 11,017,589 AUD for disability support, with only 58% typically reimbursed. Despite government assistance for an average of 3718 students per year, claims from educational institutions have outpaced the support

provided, averaging 1694 AUD in assistance per student each year. Recurrent costs, which include a wide range of operational expenses, account for 58% of the total expenditures, as detailed in Table 3.

In our cost analysis of the practical application of zk-SNARKs for managing recurrent expenses in disability support, the smart contract execution on the Ethereum network required 660,478 gas units. With the Ethereum price in September 2023 at 2518 AUD and a gas price of 7 gwei, this equates to a cost of approximately 11.64 AUD. Our analysis contrasts this transaction cost with the traditional disability support funding model, where the government's ASSD per-student aid is about 1694 AUD. The transaction cost for using the zk-SNARKs-based system represents roughly 0.6% of the ASSD per-student support.

Impact of ZKPs on student disclosure

Challenges in assessing the impact of ZKPs on students with disabilities arise from their general reluctance to disclose personal information. Among a cohort of 48,000 students with disabilities in Australia, only 253 responded to the survey conducted by Clark et al. (2018), indicating a response rate of less than 0.5%. This low participation highlights the considerable hesitancy among students with disabilities to share their personal information. To address this, our research uses hypothetical case studies to explore how the implementation of ZKPs might facilitate the disclosure process for students with disabilities, potentially leading to improved academic outcomes.

Clark et al. (2018) surveyed students with disabilities, asking them to rate their agreement with various key statements related to self-disclosure on a scale from one (strong disagreement) to five (strong agreement). Their analysis identified 'Disclosure benefits students' and 'Trust in the university' are positively associated with the likelihood of disclosure, whereas 'Fear of prejudice at university' and 'Data confidentiality concerns' were negatively associated. These significant variables, their logistic regression estimates and the average student ratings are presented in Table 4.

Building upon these insights, this study presents hypothetical case studies based on individual student profiles. We explore two distinct student groups in these case studies. Group A, which has shown hesitance in disclosing their disability status due to confidentiality concerns, often gives 'Data confidentiality concerns' a high rating of 4 out of 5. With the ZKP algorithm implementation, the disability status of these students can be verified without revealing specific details, potentially increasing their rate of disclosure and willingness to access university support services. For instance, if Group A's initial likelihood of disclosure is 20% with high confidentiality concerns, the implementation of ZKPs could reduce this rating to 2. According to logistic regression estimates, such a

Table 3 Annual expenditures allocation for disability support services

Expenditures	Percentage	Description
Recurrent	58	Salaries, software, hardware, training, projects, community outreach, consultancy, memberships, maintenance, exams
Non-recurrent	31	Unpredictable expenses like case-by-case adjustments, specialist equipment
Indirect	11	Curriculum design, staff training, infrastructure, tech, space allocation in libraries, web design

Table 4 Significant variables influencing disclosure and average student ratings

Variable	Logistic regression estimate	Average student rating
Disclosure benefits students	2.86	4
Trust in university	1.72	3.9
Fear prejudice at university	− 1.39	3.1
Data confidentiality concerns	− 1	2.8
University does not need the information	− 1.92	2.4
Do not know why should disclose	− 2.33	2
Do not know how to disclose	− 1.5	2
Academic GPA	0.08	N/A

reduction could enhance their odds of disclosing by 7.4 times, corresponding to a 65% probability—a significant improvement.

Group B, while recognizing the benefits of disclosure, is inhibited by the fear of stigmatization, often gives 'Fear of prejudice at university' a rating of 4. The introduction of ZKPs may change this dynamic, allowing these students to securely disclose their accommodation needs without the risk of exposing sensitive details. If Group B's initial disclosure rate is 50% with high fear of prejudice, reducing this rating to 2 could increase their odds by a factor of 16, resulting in a disclosure probability of 89%.

Discussions

This section outlines the prospective benefits of integrating blockchain-powered technology in education to support inclusive education and describes how the application of ZKP scan enhance the self-disclosure process for students with disabilities, contributing to their academic success and construction of their digital identity.

Blockchain-powered technology to support inclusive education

As we delve into transformative potential of blockchain technology in education, it is important to consider the cost and efficiency of implementing these systems on a larger scale. One of the challenges in employing zk-SNARKs-based smart contracts, especially on the Ethereum, is managing the variability of transaction costs. This variability could become significant when managing a large number of students with disabilities. For instance, domestic undergraduate enrollments with disabilities have steadily increased in Australia. The figure grew from 4.8% of total undergraduate students in 2011 to 9.4% in 2021, indicating an increase from 42,000 to over 100,000 more students (Australian Disability Clearinghouse on Education & Training, 2022).

To address this challenge, a promising approach is to shift zk-SNARK verification processes off-chain. Moving the verification off-chain can significantly reduce transaction costs and alleviate congestion on the Ethereum network, enhancing overall system efficiency. This strategy leverages more efficient computational resources and circumvents the high costs and storage limitations inherent in Ethereum's blockchain. Ensuring the off-chain verification processes to maintain the same level of security and reliability as on-chain verifications is also important. Strategies such as distributing the verifying key across multiple students or accommodation requests can further optimize the system.

The integration of the Ethereum network with file-sharing technologies like IPFS can democratize access and reduce reliance on traditional infrastructures, such as centralized universities and physical resources.

Aligning with UN SDG 4, which emphasizes the importance of inclusive education, blockchain technology can make higher education more accessible. As Kwok and Treiblmaier (2022) noted, reducing the transaction costs through blockchain can make higher education more reachable and potentially address broader issues such as poverty and social inequality. Advancements in blockchain technology can contribute to dismantling barriers within the educational system, addressing broader societal challenges.

Importance of privacy for students with disabilities

In the rapidly evolving technological landscape, where social interactions and community building predominantly occur online, privacy emerges as a critical concern, especially for students with disabilities. The post-COVID-19 era has accelerated technological integration in education, blurring the boundaries between Learning Management Systems and social media platforms. This shift raises concerns about data privacy as noted by Kumi-Yeboah et al. (2023). Students, particularly those from diverse backgrounds, often grapple with balancing technology use and maintaining control over their private information. Students with disabilities may face additional dilemmas, hesitating to use online services specifically designed for their needs due to privacy concerns. De Cesarei and Baldaro (2015) found that many such students exhibited significant reservations regarding their identity privacy when participating in online research. This cautious approach reflects a broader trend among the youth who, as Muñoz-Rodríguez et al. (2022) point out, adopt various methods to manage their online presence and safeguard their privacy.

ZKPs emerge as a promising technological solution to these privacy concerns. By facilitating the verification of information without revealing underlying data, ZKPs can significantly enhance privacy in digital communities. This technology empowers students with disabilities to engage in blockchain-powered communities with confidence, knowing their disability status or personal information remains confidential. It creates a secure environment for interaction, learning and growth without the fear of privacy invasion. The integration of ZKPs in digital communities, particularly in educational settings, marks a progressive step towards more inclusive and secure online spaces. While ZKPs offer a pathway to more inclusive and secure digital interactions, it is important for educational institutions and technology developers to navigate the ethical complexities and implement these solutions responsibly.

Impact of disclosure on academic success for students with disabilities

Students with disabilities have historically faced challenges in accessing quality, inclusive education worldwide. For example, in the European Union, within the 30–34 age group in 2019, only 33% of individuals with disabilities completed tertiary or equivalent education, compared to 44% of those without disabilities (Commission et al., 2021). Similarly, in the United States, the disability rate is higher among individuals with lower educational levels, and educational attainment is closely linked to lower employment percentages for persons with disabilities (McFarland et al., 2017). In Australia, data from

the Australian Disability Clearinghouse on Education and Training (2022) shows that students with disabilities typically have lower success and graduation rates compared to their non-disabled peers. Only 17% of students with disabilities aged over 20 hold a bachelor's degree or higher, compared to 35% of those without disabilities. In 2021, the success rate, defined as the pass ratio of all attempted courses, was 80.7% for students with disabilities, significantly lower than the 87.1% for those without disabilities. The notable disadvantage in educational outcomes for students with disabilities underscores the need for enhanced strategies to ensure equitable access and success for all students.

Our results section has demonstrated the potential effectiveness of adopting ZKPs to enhance self-disclosure, thereby increasing support for students with disabilities when needed. The ZKP algorithm, as a novel technology ensuring confidentiality, could also alleviate concerns related to general discrimination, distrust of universities, and negative experiences with previous disclosures, as highlighted by Clark et al. (2018). Furthermore, Clark et al. (2018) identified a strong correlation between a student's GPA and their propensity to disclose, suggesting that disclosure might not only lead to academic support and enhancing performance, but also that students with higher GPAs may be more inclined to disclose, perceiving an academic advantage.

Considering that academic GPAs are strong predictors of graduation rates, as suggested by Denning et al. (2022), maintaining good grades can have a causal effect on graduation and act as an indicator of learning ability. Therefore, enhancing disclosure rates could lead to a significant increase in academic GPAs, subsequently boosting the academic performance and outcomes for students with disabilities. Greater academic success among students with disabilities aligns with the aim of designing accessible and inclusive education, facilitating broader civic participation, employment opportunities and community life, as advocated by the UN SDG 4.

Limitations

ZKPs offer a transformative approach to privacy protection and secure authentication, but the implementation is not without challenges. This study recognizes these limitations, particularly the computational complexities of ZKPs and the challenges in interactional dynamics, given their prototype status and the absence of real-person interaction data for comprehensive evaluation.

Technological challenges with ZKPs

X. Sun et al. (2021a) highlighted several challenges associated with ZKPs:

1. Standardization issues: The diversity of ZKP models hinders universal adoption. As such, specific scenarios necessitate tailored applications.
2. Computational demands: ZKPs involve intricate mathematical computations. Certain models, especially zk-SNARKs in Zerocash, are computationally intensive and rely on third parties for setup.
3. Dependence on trusted setups: Some ZKP methodologies require a trusted establishment phase, underscoring the pivotal role of trusted entities.

Emerging technologies, such as Secure Multi-Party Computation (SMPC) and Differential Privacy, present advanced cryptographic solutions for secure data transformations and could supplement or even surpass the capabilities of ZKPs in certain contexts.

Interactional limitations

The integration of innovative technologies such as ZKPs often presents adoption challenges for various stakeholders, including students with disabilities, university support staff, registered service providers, and potentially caregivers. Since this technology is still at a prototype stage, its real-world adoption and effectiveness for students with disabilities have yet to be thoroughly tested.

For stakeholders to fully understand and utilize ZKPs, comprehensive training may be required for university staff and students. Chen et al. (2018) emphasized the potential pitfalls of applying blockchain technology in educational settings. The complexity can complicate the evaluation of subjective learning behaviors and outcomes such as essays and classroom presentations. Additionally, integrating students' educational data into blockchain ledgers presents another challenge. While blockchain's immutable nature bolsters data security, it simultaneously imposes limitations on modifying educational records, even when these changes may be justified.

Furthermore, numerous technical issues remain to be addressed for the effective application of blockchain in education. These issues include scalability, network congestion management, and the development of user-friendly interfaces that accommodate the diverse needs of all students, including those with disabilities. Addressing these challenges is crucial for the seamless adoption of blockchain and ZKPs in educational settings, which ensures that the benefits of these technologies are fully realized without compromising the learning experience or the rights of students.

Conclusions

In alignment with the UN Sustainable Development Goal 4, which emphasizes the importance of inclusive education, this paper explores the potential of integrating ZKPs via blockchain in the educational setting, particularly through blockchain technology. This approach provides an innovative approach of supporting students with disabilities, ensuring their privacy while enhancing administrative efficiency.

Our implementation of the zk-SNARK technology demonstrates how this advanced cryptographic solution can streamline accommodation verification processes for students with disabilities in higher education institutions. The disability management system not only significantly improves operational efficiencies but also ensures an enhanced self-disclosure process, providing robust support for the students. Our comparative cost analysis highlights the potential economic advantages of blockchain-backed ZKP systems over traditional disability support structures. Additionally, our hypothetical case studies suggest the disclosure rates would increase, presenting a promising strategy for managing student disability needs more effectively.

We further discuss the technological benefits from a cost–benefit perspective, highlighting how blockchain technology can promote inclusive education, enhance privacy to help establish individual identity in the digital era, and contribute to academic success for students through increased disclosure. Privacy is a crucial element of individual

identity in the digital age, especially for students with disabilities, who have long been disadvantaged in academic success and employment opportunities due to hesitancy in seeking help and concerns about confidentiality. Striking a balance between safeguarding student privacy and ensuring appropriate accommodations can be challenging; however, blockchain-integrated ZKP technology offers a promising solution. Beyond its technical innovations, ZKPs provide a means for students to protect sensitive information, ensuring it is not disclosed to unnecessary parties. The enhanced disclosure process facilitated by ZKPs can better address students' accommodation needs, helping them achieve greater academic success.

In conclusion, this study underscores the critical importance of embracing innovative technologies like ZKPs and zk-SNARKs. The ultimate shared goal is to the create sustainable, inclusive, and progressive educational environments. As blockchain and cryptography technologies continue to evolve, the apparent benefits will increasingly drive significant transformations in higher education. This research not only highlights these technologies' potential but also advocates for their strategic implementation to ensure equitable access and success for all students, particularly those with disabilities.

Abbreviations

ASSD	Additional support for students with disabilities
DSF	Disability support fund
ETH	Ethereum (a blockchain platform and cryptocurrency)
ICT	Information and Communication Technology
IPFS	InterPlanetary file system
IZKP	Interactive zero-knowledge proof
NIZKP	Non-interactive zero-knowledge proof
P2P	Peer-to-peer
SDG	Sustainable development goals
SMPC	Secure multi-party computation
UN	United Nations
zk-SNARK	Zero-knowledge succinct non-interactive argument of knowledge
ZKP	Zero-knowledge proof

Acknowledgements
Not applicable.

Author contributions
All aspects of the manuscript, including data analysis, interpretation, histological examinations, writing, and final approval, were carried out by XX.

Funding
Not applicable.

Availability of data and materials
All supplementary materials, including the prototype algorithm code, are available in the 'ZKP' directory of the repository: [LINK REMOVED FOR BLINDED REVIEW].

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 28 September 2023 Accepted: 1 February 2024
Published online: 06 February 2024

References

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences (switzerland)*. https://doi.org/10.3390/app9122400

Arenas, R., & Fernandez, P. (2018). CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 1–6. https://doi.org/10.1109/ICE.2018.8436324

Australian Disability Clearinghouse on Education and Training. (2022). *Higher Education Data Analysis*. https://www.adcet.edu.au/disability-practitioner/data-evaluation/higher-education-data/current-he-data-analysis

Babel, M., & Sedlmeir, J. (2023). *Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs*. http://arxiv.org/abs/2301.00823

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *Proceedings - IEEE Symposium on Security and Privacy* (pp. 459–474). https://doi.org/10.1109/SP.2014.36

Berentsen, A., Lenzi, J., & Nyffenegger, R. (2023). *An Introduction to Zero-Knowledge Proofs in Blockchains and Economics*. https://research.stlouisfed.org/publications/review/2023/05/12/an-introduction-to-zero-knowledge-proofs-in-blockchains-and-economics

Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*. https://doi.org/10.1186/s40561-017-0050-x

Chi, P. W., Lu, Y. H., & Guan, A. (2023). A privacy-preserving zero-knowledge proof for blockchain. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3302691

Clark, C., Wilkinson, M., & Kusevskis-Hayes, R. (2018). *Enhancing Self-Disclosure of Equity Group Membership*. https://www.ncsehe.edu.au/project/enhancing-self-disclosure-of-equity-group-membership

Commission, E., Directorate-General for Employment, S. A. and I., & Grammenos, S. (2021). *European comparative data on Europe 2020 and persons with disabilities – Labour market, education, poverty and health analysis and trends*. Publications Office of the European Union. https://doi.org/10.2767/745317

De Cesarei, A., & Baldaro, B. (2015). Doing online research involving university students with disabilities: Methodological issues. In *Computers in Human Behavior* (Vol. 53, pp. 374–380). Elsevier Ltd. https://doi.org/10.1016/j.chb.2015.07.028

Denning, J. T., Eide, E. R., Mumford, K. J., Patterson, R. W., & Warnick, M. (2022). Why have college completion rates increased? *American Economic Journal: Applied Economics, 14*(3), 1–29. https://doi.org/10.1257/app.20200525

ElSheikh, M., & Youssef, A. M. (2023). *Dispute-Free Scalable Open Vote Network Using zk-SNARKs* (pp. 499–515). https://doi.org/10.1007/978-3-031-32415-4_31

Fernández-Cerero, J., Montenegro-Rueda, M., & Fernández-Batanero, J. M. (2023). Impact of University Teachers' Technological Training on Educational Inclusion and Quality of Life of Students with Disabilities: A Systematic Review. In *International Journal of Environmental Research and Public Health* (Vol. 20, Issue 3). MDPI. https://doi.org/10.3390/ijerph20032576

Fichten, C., Olenik-Shemesh, D., Asuncion, J., Jorgensen, M., & Colwell, C. (2020). Higher education, information and communication technologies and students with disabilities: An overview of the current situation. In *Improving Accessible Digital Practices in Higher Education: Challenges and New Practices for Inclusion* (pp. 21–44). Springer International Publishing. https://doi.org/10.1007/978-3-030-37125-8_2

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85*, 291–304. https://doi.org/10.1145/22145.22178

Grech, Alexander., & Camilleri, A. F. (2017). *Blockchain in education*. https://doi.org/10.2760/60649

Groth, J. (2010). *Short Pairing-Based Non-interactive Zero-Knowledge Arguments* (pp. 321–340). https://doi.org/10.1007/978-3-642-17373-8_19

Kumi-Yeboah, A., Kim, Y., Yankson, B., Aikins, S., & Dadson, Y. A. (2023). Diverse students' perspectives on privacy and technology integration in higher education. *British Journal of Educational Technology, 54*(6), 1671–1692. https://doi.org/10.1111/bjet.13386

Kwok, A. O. J., & Treiblmaier, H. (2022). No one left behind in education: blockchain-based transformation and its potential for social inclusion. In *Asia Pacific Education Review* (Vol. 23, Issue 3, pp. 445–455). Springer Science and Business Media B.V. https://doi.org/10.1007/s12564-021-09735-4

Li, B., Qi, G., & Lu, W. (2022). Recent Advances in Privacy Protection Technologies in Blockchain. *International Conference on ICT Convergence, 2022-October*, 77–82. https://doi.org/10.1109/ICTC55196.2022.9952451

Li, L., & Ruppar, A. (2021). Conceptualizing teacher agency for inclusive education: A systematic and international review. *Teacher Education and Special Education, 44*(1), 42–59. https://doi.org/10.1177/0888406420926976

Li, W., Guo, H., Nejad, M., & Shen, C. C. (2020). Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. *IEEE Access, 8*, 181733–181743. https://doi.org/10.1109/ACCESS.2020.3028189

Lizcano, D., Lara, J. A., White, B., & Aljawarneh, S. (2020). Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *Journal of Computing in Higher Education, 32*(1), 109–134. https://doi.org/10.1007/s12528-019-09209-y

McFarland, J., Hussar, B., de Brey, C., Snyder, T., Wang, X., Wilkinson-Flicker, S., Gebrekristos, S., Zhang, J., Rathbun, A., Barmer, A., Bullock Mann, F., & Hinz, S. (2017). *The Condition of Education 2017 (NCES 2017144)*.

Muñoz-Rodríguez, J. M., Dacosta, A., & Martín-Lucas, J. (2022). Digital Natives or Digital Castaways? Processes of Constructing and Reconstructing Young People's Digital Identity and Their Educational Implications. In *Identity in a Hyperconnected Society: Risks and Educative Proposals* (pp. 15–32). Springer International Publishing. https://doi.org/10.1007/978-3-030-85788-2_2

Ocheja, P., Flanagan, B., Ueda, H., & Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*. https://doi.org/10.1186/s41039-019-0097-0

Perera-Rodríguez, V. H., & MoriñaDíez, A. (2019). Technological challenges and students with disabilities in higher education. *Exceptionality, 27*(1), 65–76. https://doi.org/10.1080/09362835.2017.1409117

Pitman, T., Ellis, K., Brett, M., Knight, E., McLennan, D., & ii, M. (2022). *Calculating the costs of supporting people with disability in Australian higher education 2022*. https://www.ncsehe.edu.au/publications/costs-supporting-disability-australian-higher-education/

Portugal, D., Faria, J. N., Belk, M., Martins, P., Constantinides, A., Pietron, A., Pitsillides, A., Avouris, N., & Fidas, C. A. (2023). Continuous user identification in distance learning: a recent technology perspective. In *Smart Learning Environments* (Vol. 10, Issue 1). Springer. https://doi.org/10.1186/s40561-023-00255-9

Quisquater, J.-J., Quisquater, M., Quisquater, M., Quisquater, M., Guillou, L., Guillou, M. A., Guillou, G., Guillou, A., Guillou, G., & Guillou, S. (1990). How to Explain Zero-Knowledge Protocols to Your Children. In *Advances in Cryptology—CRYPTO' 89 Proceedings* (Vol. 435, Issue 1, pp. 628–631). Springer New York. https://doi.org/10.1007/0-387-34805-0_60

Raimundo, R., & Rosário, A. (2021). Blockchain system in the higher education. In *European Journal of Investigation in Health, Psychology and Education* (Vol. 11, Issue 1, pp. 276–293). MDPI AG. https://doi.org/10.3390/ejihpe11010021

Sun, H., Wang, X., & Wang, X. (2018). Application of blockchain technology in online education. *International Journal of Emerging Technologies in Learning, 13*(10), 252–259. https://doi.org/10.3991/ijet.v13i10.9455

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021a). A survey on zero-knowledge proof in blockchain. *IEEE Network, 35*(4), 198–205. https://doi.org/10.1109/MNET.011.2000473

Sun, X., Zou, J., Li, L., & Luo, M. (2021b). A blockchain-based online language learning system. *Telecommunication Systems, 76*(2), 155–166. https://doi.org/10.1007/s11235-020-00699-1

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access, 6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929

United Nations. (n.d.). *Transforming our world: The 2030 agenda for sustainable development*. 2015. Retrieved September 23, 2023, from https://sdgs.un.org/2030agenda

Williams, P. (2019). Does competency-based education with blockchain signal a new mission for universities? *Journal of Higher Education Policy and Management, 41*(1), 104–117. https://doi.org/10.1080/1360080X.2018.1520491

Yin, W. (2023). Zero-knowledge proof intelligent recommendation system to protect students' data privacy in the digital age. *Applied Artificial Intelligence*. https://doi.org/10.1080/08839514.2023.2222495

Publisher's Note