Computer Science and Information Technologies
Vol. 7, No. 2, July 2026, pp. 131~140
ISSN: 2722-3221, DOI: 10.11591/csit.v7i2.p131-140

Fuzzy logic–based consensus protocol for educational blockchain networks

Igor Ivanov[1], Svetlana Zhdanova[2]
[1]Faculty of Science and Engineering, Milagro State University, Milagro, Ecuador
[2]Faculty of Information Technology and Control Systems, Belgorod State Technological University, Belgorod, Russia

Article Info

Article history:

Received Oct 24, 2025
Revised Nov 28, 2025
Accepted Jan 1, 2026

Keywords:

Consensus mechanism
Educational blockchain
Educational data security
Fuzzy sets
Node reputation
Protocol trust
Reliable data storage

ABSTRACT

This paper addresses the growing challenge of ensuring trust, authenticity, and transparency in the management and verification of educational credentials within modern, digitally oriented learning ecosystems. Rapid expansion of e-learning, lifelong learning, and global mobility has intensified document fraud, revealing the limitations of traditional verification mechanisms. To respond to these systemic risks, the study proposes a socially oriented block-validation protocol integrated into a distributed blockchain environment designed specifically for educational data security. The protocol forms the core of the EduBLOCK system, developed by the authors, and introduces an innovative consensus mechanism that incorporates human-centered reputation assessments rather than computational or financial power. The approach employs fuzzy-set theory to evaluate user activity, institutional credibility, and delegate reputation, enabling a more nuanced and context-sensitive model of trust. Delegates responsible for validating blocks are selected through a dynamic, reputation-driven procedure that excludes financial contributions and subjective parameter tuning. The proposed algorithm combines cryptographic guarantees, peer-to-peer (P2P) communication, and soft-computing methods to ensure fairness, prevent manipulation, and maintain stable system functioning. Block validity is determined through open voting, requiring approval by more than two-thirds of elected delegates.

Corresponding Author:

Igor Ivanov
Faculty of Science and Engineering, Milagro State University
091050 UNEMI, Milagro, Ecuador
Email: i.v.ivanov1960@gmail.com

1. INTRODUCTION

In the contemporary knowledge-based society, where information has become a central economic and social resource, education systems undergo continuous transformation in response to the rapid evolution of digital technologies. Institutions of higher learning across the world are adapting to these changes by expanding technology-enhanced learning opportunities, integrating advanced digital tools into traditional pedagogical frameworks, and developing new models capable of meeting the expectations of increasingly diverse learner populations. Among these transformations, e-learning has emerged as one of the most influential innovations, enabling access to education independent of time and place while enhancing the quality, flexibility, and diversity of instructional resources [1], [2]. Digital platforms extend the learner's "zone of proximal development (ZPD)" [3], support individualized pacing, and facilitate autonomous study, communication, and collaborative inquiry—thus embodying the broader shift toward flexible and technology-mediated learning environments characteristic of modern information societies.

Parallel to the expansion of electronic education, the paradigm of lifelong learning has become a defining feature of contemporary educational landscapes. Rather than representing a temporary trend, it reflects a profound structural reconfiguration in which ongoing learning is increasingly viewed as a prerequisite for social mobility and professional advancement. Individuals accumulate multiple credentials—degrees, certificates, badges, and micro-qualifications—to demonstrate skills and competencies relevant to dynamic labor markets. The growing demand for accessible educational opportunities is matched by the rise of global online platforms such as Coursera, EdX, and Udacity, which provide mass, scalable learning and create new forms of educational capital. As a result, the digital learning portfolio becomes an important asset: it aggregates information about learners' goals, achievements, strategies, and decisions, and supports personalized trajectories within information-rich environments [1], [2], [4].

However, the rapid expansion of lifelong, electronic, and mass learning brings with it a critical systemic challenge: the unprecedented growth of document fraud and credential falsification. Traditional verification and control mechanisms—designed for classical, in-person education—are increasingly unable to respond effectively to the scale, variety, and sophistication of fraudulent practices. Educational institutions frequently face difficulties in confirming the identity of distance-learning participants, ensuring that the person completing coursework is indeed the one receiving the certificate. At the same time, evidence from multiple regions indicates an alarming increase in forged documents: for example, the UK degree verification service (HDD) warned graduates not to post diploma images online due to the risk of fueling a multimillion-dollar black market for falsified credentials [5]. Research shows that up to 90% of recommendation letters submitted by some international applicants to US universities may be fabricated, 70% of personal essays are written by third parties, and 50% of academic transcripts contain falsifications [6]. Moreover, the global mobility of professionals requires cross-border recognition of credentials, making verification processes even more complex. In many cases, intermediary organizations must assess authenticity and determine equivalency with national training standards, further increasing the burden on verification systems.

In response to these challenges, international and national institutions have intensified efforts to detect and prevent document falsification. The European FRAUDOC project has developed methodological guidelines for identifying forged educational records. The Russian Federation introduced a federal information system through the Government Resolution of 26 August 2013, modernizing the national register of educational documents and implementing the "contingent" system, which accumulates electronic diplomas and certificates issued across the country [7]. In Ecuador, the Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) maintains an official registry responsible for storing, verifying, and certifying educational records [8]. These initiatives reflect a global acknowledgment that the integrity of educational credentials is a matter of societal importance.

Amid these efforts, blockchain technologies [9] have been widely discussed as a promising solution for secure, tamper-resistant, and decentralized verification of educational documents [10]. Their distributed nature, immutability, and cryptographic guarantees theoretically make them well-suited for combating falsification [11]. Yet practical implementations have revealed notable shortcomings. Existing blockchain-based verification protocols [12] often remain overly technocratic and insufficiently transparent to educators, employers, and regulatory bodies. Furthermore, they may allow circumvention when formal requirements are technically satisfied but socially dubious—for instance, when credentials originate from low-credibility educational agencies or short-lived organizations created solely to legitimize questionable documents. These limitations underscore the need not merely for technological enhancement but for a fundamental humanization of verification processes.

In the field of education, the institution of reputation plays a decisive role. The credibility of learners, educators, issuing organizations, and intermediaries shapes trust relationships and affects the perceived value of credentials. Therefore, a socially oriented verification system must incorporate reputation as a core analytical dimension rather than treating it as an external factor. Reputation-aware verification extends beyond cryptographic validity and includes social signals, historical performance, institutional standing, and collective assessments of trustworthiness. The paper by Hu *et al.* [13] proposes an educational blockchain system for knowledge distribution, the key element of which is an algorithm for assessing the reputation of educational agents. This algorithm that assigns a reputation score to users based on their contributions and interactions. This score is a key factor in the incentive mechanism, and can be combined with proof-of-stake (PoS) algorithm to form a hybrid system. The reputation assessment algorithm is a weighted sum of various factors, with the sum then normalized to one. The weights of the factors are set subjectively based on an intuitive understanding of their importance. The presented system is commercial in nature and operates on the basis of contributions from participants. One of the important factors of reputation is the amount of the monetary contribution, which is not always acceptable for public education systems.

Against this background, this article proposes a block verification protocol within a distributed blockchain system that incorporates reputation assessment mechanisms into the credential verification

process. The protocol does not contain subjective numerical parameters or parameters related to the monetary level of network participants, which distinguishes it from its counterparts. By integrating social assessments with technical verification rules, the proposed approach aims to create a more human-centered, transparent, and reliable model capable of responding to the challenges associated with lifelong, electronic, and mass education. The protocol has been implemented in the EduBLOCK blockchain system for verifying educational documents, developed with the participation of the authors.

2. DEVELOPMENT OF A PROTOTYPE OF A SECURE BLOCK VALIDATION PROTOCOL IN A SOCIALLY ORIENTED (HUMANISTIC) SYSTEM

2.1. General information

From the aforementioned discussion, it can be deduced that there exists an urgent global demand for a technological solution to address the issue of trust deficiency and to facilitate reliable and secure electronic data storage. We posit that such a technology could manifest as a multifunctional and multi-tiered information system, known as a distributed ledger. Distributed ledger technology represents an innovative approach to the exchange and preservation of information, possessing certain irrefutable advantages, including the ownership of a comprehensive copy of the ledger, real-time data synchronization, and immediate access to transaction histories [14]. The primary catalyst for the heightened interest in this technology is the anticipation that it will rectify the current challenges and constraints associated with contemporary methodologies of storing, accumulating, and transmitting information. Distributed ledger technology employs blockchain mechanisms to circumvent these impediments.

A blockchain can be characterized as the storage framework meticulously designed to maintain a permanent and verifiable record of transactions that transpire between two parties. Furthermore, blockchain functions as an open, distributed peer-to-peer (P2P) framework for data storage [15]. Each block establishes a connection to its immediately preceding block through a reference that constitutes a hash value of the prior block, referred to as the parent block. It is important to highlight that the hashes of uncle blocks (descendants of the block's ancestors) are also retained within the blockchain. The inaugural block of a blockchain is designated as the genesis block, which lacks a parent block [16].

The blocks themselves, along with the data encapsulated within them, are safeguarded through the mechanism of chain linking. Each record encompasses a connection to the prior source record, in addition to a blocking condition and an unblocking stipulation. To articulate the rules and conditions, a programming language is employed, which permits the establishment of intricate logic and regulations governing the interactions of participants. It is feasible for each record to have multiple sources and results; thus, a record can transmute several source records into multiple outcome records. Consequently, blockchain possesses the capability to engender trust among independent, unfamiliar actors, thereby affording them the opportunity to collaborate without necessitating any form of central authority [17].

The overarching structure of the blockchain is predicated upon the Merkle tree framework. A Merkle tree constitutes a data architecture characterized by a hierarchy of cryptographic hashes. Its configuration exhibits minimal divergence from conventional tree-like data structures. It fundamentally relies on the computation of hash values derived from the hash values of all its subordinate nodes. The root hash is inscribed within the block header, thereby rendering the deletion or substitution of transaction blocks infeasible. Considering that block headers are sufficiently safeguarded against alterations, it follows that an adversary would be compelled to replace all subsequent blocks across the entire blockchain to amend a solitary block. An effective strategy for the protection of block headers consequently renders the eradication of transactions from the blockchain, which were documented a considerable time ago, impracticable. Hence, the blockchain fulfills the criterion of transaction finality [18]. The composition of each transaction block is uniform and comprises the following components [19]:

- Block version: encompasses all the stipulations (hashing protocols) that a block must adhere to in order to attain validation.
- Parent block hash: retains the values utilized to signify the connection to the preceding record block.
- Merkle tree root hash: contains the hash value representing all the transactions within the block.
- Timestamp: serves as a temporal reference.
- N-bits: pertains to the current hashing objective within the enumeration.
- Nonce: a four-byte field that increments its value following each successive transaction or computational operation.

The inherent block structure obviates the necessity of storing the entire document. Instead, the data is retained by the user, with only the hash value of a particular document being integrated into the distributed system. By maintaining the confidentiality of their private key, users are empowered to consistently regenerate the document's hash value for verification. A successful match between the document's hash and

the hash recorded in the transaction, provided the transaction is validated, unequivocally establishes the document's authenticity. In contrast to traditional databases like MySQL and MongoDB, whose security relies on centralized data validation conducted by system operators, the human element in management processes renders these conventional systems susceptible to vulnerabilities. A pertinent illustration of this vulnerability is the compromise of the biometric database managed by the Indian agency Unique Identification Authority of India (UIDAI). Although UIDAI stated in November 2017 that "Aadhaar data is fully safe and secure and there has been no data leak or breach at UIDAI," investigative journalists from "The Tribune" [20] newspaper reported acquiring access, via anonymous sellers on WhatsApp, to comprehensive details for a substantial portion of India's Aadhaar numbers, numbering over one billion. The blockchain protocol and its structure, which is based on secure data storage, creates an automated system of registries in a form of interconnected system and mitigate external threats.

Smart contracts are unprecedented methods of ensuring contractual compliance, including social contracts. "If you have a big transaction with a specific control structure, you can predict the outcome at any period in time," said Antonopoulos [21]. According to Tapscott and Tapscott [9], it is stated that when a fully verified and signed transaction contains multiple signatures within a multisignature account, the verifiability of that transaction by the network can be predicted. If the transaction is verified by the network, it is regarded as redeemable and irrevocable. Tapscott and Tapscott [9] emphasizes that no central authority or third party is able to revoke it, and that the consensus of the network cannot be overridden by anyone. This is described by him as a new concept in both law and finance. It is further asserted that the Bitcoin system provides a very high degree of certainty regarding the outcome of a contract. The integration of smart contracts with blockchain technology principles facilitates the establishment of a system for meticulously recording an individual's academic credentials and certifications. This synergistic approach addresses the challenges associated with the accessible, dependable, and transparent preservation of digital documentation, as illustrated in Figure 1.

Contemporary European universities and educational bodies are increasingly integrating blockchain technology, primarily for the administration of academic credentials and the comprehensive evaluation of educational achievements [22]. Notably, the University of Nicosia pioneered the application of blockchain for managing certificates issued through massive online open courses (MOOCs) [23]. Sony Global Education has also harnessed this technology to develop a worldwide assessment platform designed for the secure storage and management of academic degree data. Furthermore, the Massachusetts Institute of Technology (MIT) is issuing digital academic degrees, with participants in MIT Media Lab projects who successfully complete assessments receiving blockchain-supported certificates [24]. An additional significant initiative is the development of BlockTac [25], a blockchain-based framework intended for collaboration with Spanish universities, business schools, and professional organizations, as well as international educational establishments across Europe and Latin America. This system enables students to upload their certificates, which are then digitally endorsed by educational institutions. Consequently, students can present these verified certificates at other academic institutions, with their authenticity verifiable directly through the system, obviating the need to contact the original issuer.

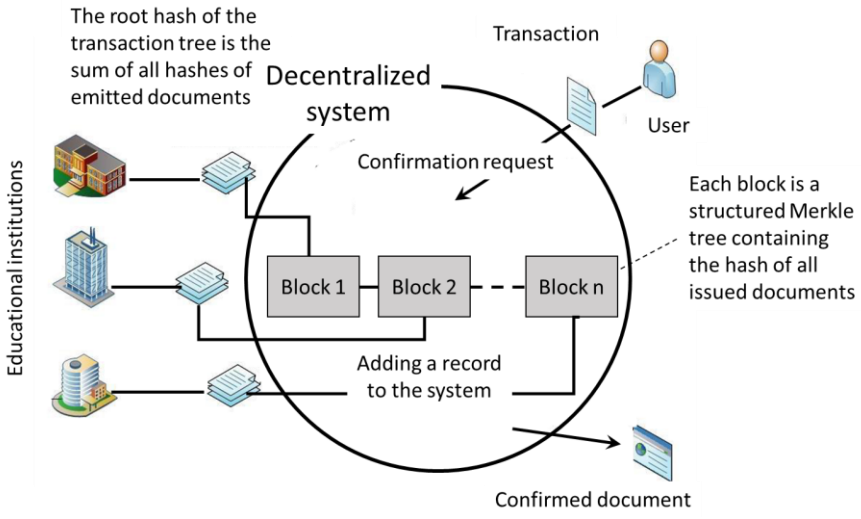

Figure 1. Communications between user and educational organizations using decentralized system

2.2. The structural design of the secure repository solution

The global relevance and demand for systems utilizing distributed ledger technology are evident. Nevertheless, it is noteworthy that comprehensive architectural and software implementations, along with their detailed specifications, are exceedingly scarce. Furthermore, existing systems often fall short of specific user requirements, necessitating further modification for organizational applications. The EDBlock informational system, a project initiated by an international group of researchers and engineers, was conceived precisely to address these challenges. To design the subject area model was used a functional approach based on the IDEF0 methodology [26]. The IDEF0 context diagram in Figure 2, reflects the general description of activities of informational system EDBlock.

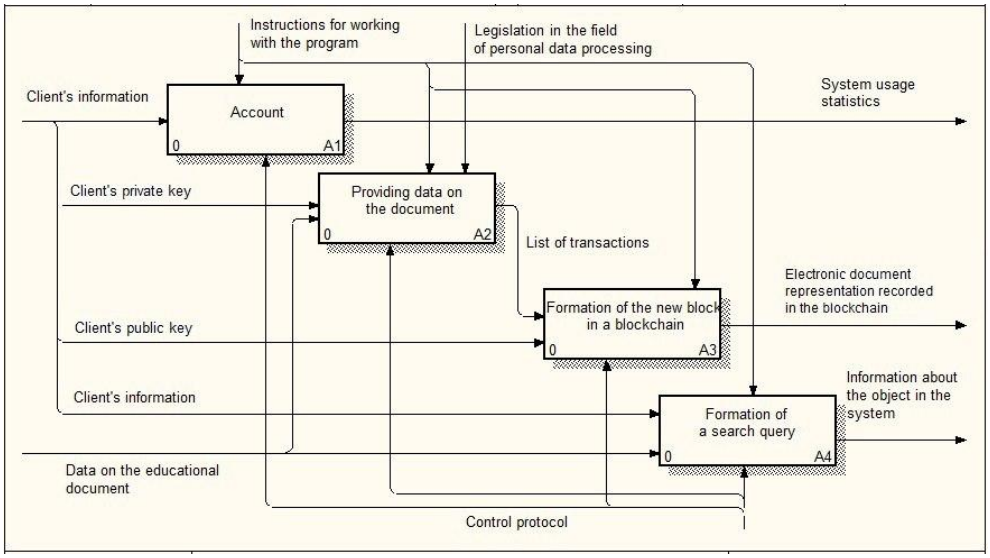

Figure 2. Structure of EDBlock system

The system processes customer data and information pertaining to educational documents. The output comprises blockchain records representing electronic versions of these documents, system usage statistics, and search query outcomes. As depicted in the diagram, the system's overall functionality is segmented into four principal components.

The initial block utilizes user data as input, yielding either a request for educational document information or system usage statistics. The second block is responsible for generating new transactions, which encapsulate details regarding the submitted document and the associated user creating the transaction. Subsequently, the third block constructs the blockchain, incorporating all transactions generated in the preceding stage. The fourth block leverages the provided document information to formulate a search query. The resolution of this query delivers relevant document information present within the system to the user.

Analysis of these information flows has led to the identification of the following subsystems (modules) within the information system: a cryptographic module, an interconnection module, a blockchain module, and an application facilitating user interaction with the system. The cryptographic module must be able to generate cryptographically strong keys based on the RSA-2048 standard. The hash of personal data is being created using the SHA-512 algorithm, and then user uses their private key to construct the transaction signature.

The interworking module is built on the basis of P2P technology. P2P technology differs from standard approaches to scaling network infrastructures. When a P2P approach is applied, the main focus is not communication between the client-server, but the ways and methods of finding other clients on the network, according to the information they are able to exchange information with each other. Blockchain (control) module is used to create transactions, transactional and authorization blocks. In addition, this module describes algorithms for checking received information, checking the local data circuit, storing data in the local circuit, verifications using confirmation protocol.

The core of distributed registry technology is the consensus protocol [27]. Roughly defined, consensus is an agreement that satisfies each of involved parties. Consensus itself is the key to democracy and decentralization in general, and distributed registry technology in particular.

In the most of cryptocurrencies, network security relies on a proof of work (PoW) algorithm in the form of block mining. Each node which would like to participate in the mining, must solve a computationally difficult problem to construct new valid block. If we define as B the header of the last block of a valid block chain, then this complexity should not exceed the following threshold:

$$hash(B) \leq H/D \quad (1)$$

where D ∈ [1; H] is the target complexity, and H is the upper bound of the value of the hash function used in the system. There is no algorithm to find B that satisfies this inequality, other than iterating over all possible values of the block header. Larger value of D causes more iterations to find a valid block; the expected number of operations is D.

The protocol is fair in the sense that a miner with a computing power n can create a block and receive a reward with probability p=n/N, where N is the total computing power of the entire system. The attacker must solve the same problems as each of miners of the entire system, thus, the attack could be successful if only the attacker had the amount of computing resources nearly equal as resources of the whole system. PoW-like protocols operate in a way that the security of the network is supported by physical resources, such as specialized equipment for computing, or the electricity required to operate this equipment. This makes protocols inefficient in terms of resource consumption and inapplicable in systems focused on social motivation.

One possible implementation of a distributed database that does not rely on expensive computations and is based on PoS algorithms. The idea of proof of stake is simple: instead of computing power, the probability of creation a new block and receiving the appropriate reward is proportional to the user's share in the system. In the classic interpretation of PoS algorithms, inequality (1) is modified in a way of getting rid of block properties and switch into the system parameters owned by a user:

$$hash(hash(B), A, t) \leq bal(A)/N \quad (2)$$

where A is the user account in the system, t is the current moment in time, bal(A) is the numeric value of the system key parameter, which is owned by the user A at the moment t, N is the maximum value of the key indicator of the system.

The choice of a key indicator of system and of a logic relationship between the current balance and total capacity of the distributed system generates a variety of algorithms of the PoS family. The outcome of the research of the specifics of given PoW algorithms is the understanding of the inapplicability of the PoW algorithms family for solving a class of social problems. The motivation for the developing information system "EDBlock" is the desire to create a unified register of legal educational documents confirming the competence and knowledge of students. The consensus algorithm of the system needs an alternative reward for users. To achieve this, it is proposed to use concepts of "activity" and "reputation". One type of PoS algorithm is chosen as a basis - delegated proof-of-stake (DpoS). In this protocol, blocks are generated by a predefined set of system users (delegates) who are rewarded for their duty and punished for malicious behavior (for example, for recognizing a deliberately invalid block). Delegates have two roles simultaneously. They participate in the construction of the block of transactions and verify generated block by means of cryptographic methods. A generated block supposed to be recognized as valid, if it is verified by a specified number of users from a set of delegates. The list of users eligible for block signing is periodically changed in accordance with agreed rules.

The developed system exhibits a fundamentally humanistic characteristic. A humanistic system is defined as one whose operations are significantly shaped by human discretion or interpretation. Conventional approaches to systems analysis and computational modeling, which rely on exact quantitative methodologies, fall short in capturing the intricate nature of human cognition and the underlying principles governing decision-making. Embracing this proposition implies the imperative to forgo conventional standards of rigor and precision in favor of alternative methodologies for system investigation [28]. That is why the logic of the algorithm is based on the concept of fuzzy sets and uses fuzzy logic.

The selection of delegates is predicated on the assumption of a system user base, denoted as set X. This set encompasses all individuals utilizing the system. Voting eligibility for delegate elections is contingent upon an individual's vote count, a metric derived from several factors: sustained engagement duration within the system, the aggregate number of educational materials acquired, the quantity of educational documents validated by the educational institution, and the user's account balance, quantified in the system's internal currency. Users exhibiting sustained engagement are recognized with a voting privilege, thereby constituting the fuzzy set A, designated as "active voters". Fuzzy set A "active voter" is represented by a set of pairs $A=\{(f_A(x), x)\}$, where x represents the user of the system, $f_A(x)$ is the membership function that determines the activity of the participant. In our opinion, $f_A(x)$ is a global fuzzy criterion of the system,

which is a composition of four local fuzzy criteria. According to theory of fuzzy sets, each of criteria could have a value from 0 to 1. They are:

- t(x) represents the duration of a user's uninterrupted engagement within the system.
- d(x) denotes the cumulative quantity of educational documents acquired.
- d*(x) signifies the count of educational documents that have received validation from the relevant educational institution.
- m(x) indicates the financial standing of the user's account, expressed in the system's proprietary currency.

The voter can regulate the level of their activity by increasing any of the local fuzzy criteria listed above. The evaluation of the values of these criteria has led to the understanding of the impossibility of use the "hard" mathematical tools of interval fuzzy arithmetic. To obtain a quantitative value of the global criterion $f_A(x)$, Zadeh [29] proposed a system of "soft relations". The essence of soft computing is that, unlike traditional and hard computing, it aims to adapt to the general uncertainty of the real world. Therefore, the guiding principle of soft computing is tolerance for inaccuracy, uncertainty, and partial truth in order to achieve manageability, reliability, low cost of solutions, and better alignment with reality [29]. The final quantitative value is determined as way:

$$f_A(x) = m(x) + d^*(x) + d(x) + t(x) - m(x)d^*(x) - m(x)d(x) - m(x)t(x) - d^*(x)d(x) - d^*(x)t(x) - d(x)t(x) + m(x)d(x)d^*(x) + m(x)d^*(x)t(x) + m(x)d(x)t(x) + d^*(x)d(x)t(x) - m(x)d(x)d^*(x)t(x) \quad (3)$$

Set Y "delegates" is formed by choosing representatives. Inside the set Y a fuzzy set V is formed by "voting delegates". The main task representatives of this set solve, is the regulation of the system by generating blocks. As a fuzzy criteria $r_V(y)$ has been chosen a "reputation" concept. The correctness of proposed judgments is confirmed by studies by other authors in this area.

It is observed that reputation serves as a foundation of the new digital economy [22], with companies like Airbnb and Uber establishing trust through ratings and reviews. In the academic sphere, reputation already functions as a tradeable commodity, since promotion and recruitment are partly determined by indicators such as citation counts and the H-index, which reflects publication impact. It is further suggested that the trading of scholarly reputation could be extended beyond academia and used as the basis for a broader educational economy. The delegate's reputation metric, denoted as $r_V(y)$, along with evidence of initial share, is assessed through the application of the following five fuzzy criteria:

- l(y), which signifies the possession of a license authorizing educational activities;
- d(y), representing the quantity of educational credentials conferred by the institution;
- v(y), indicating the aggregate user votes garnered from the system;
- p(y), referring to the ratio of validly signed metadata to the entirety of signed metadata, inclusive of invalid entries;
- s(y), which denotes the total count of engagements as a delegate.

The final value of the reputation criteria $r_V(y)$ is being calculated similar to the fuzzy "active voter" set (3) and can be represented using (4):

$$r_V(y) = l(y) + d(y) + v(y) + p(y) - l(y)d(y) - l(y)v(y) - l(y)p(y) - d(y)v(y) - d(y)p(y) - v(y)p(y) + l(y)d(y)v(y) + l(y)d(y)p(y) + l(y)v(y)p(y) + d(y)v(y)p(y) - l(y)d(y)v(y)p(y)\big(1 - s(y)\big) + s(y) \quad (4)$$

Requirements for elected delegates are: i) last two delegates who signed the last block in the current round are excluded from the list of candidates of the next round of voting; ii) delegates with the same reputation rating are being mutually excluded; and iii) there cannot be two identical node identifiers in the sequence of delegates.

The formatting algorithm for a valid block is represented by the following sequence of actions. Each of the selected delegates sequentially forms a valid block from user transactions. Each delegate has a fixed amount of time for one round of voting to release blocks of the chain. Each delegate within 10 seconds receives transactions for the creation of blocks, or an information about the creation error which is sent by other nodes. A decision whether to sign or not the block sent by an active delegate is being made by the processing an open voting to determine the validity of the generated block. A block is considered valid if more than 2/3 of the elected delegates quorum accepts it. The generated block is signed with the digital signature of the delegate who created it. This mechanism is needed to reduce the reputation rating in a case it turns out that the block is falsified. After completing the entire voting circle, an auction is organized again to select new delegates. The order in which delegates are selected is represented by the following algorithm, as in Figure 3: i) within 5 seconds, each user node that has the opportunity to vote, must distribute its votes

among participants-delegates; ii) then it is necessary to rank candidates from *1* to *n* among nominated delegates with a reputation score above or below the established boundary; iii) broadcast the hash of the resulting list to all system nodes; and vi) the list of the most significant members is being selected as a quorum of active delegates.

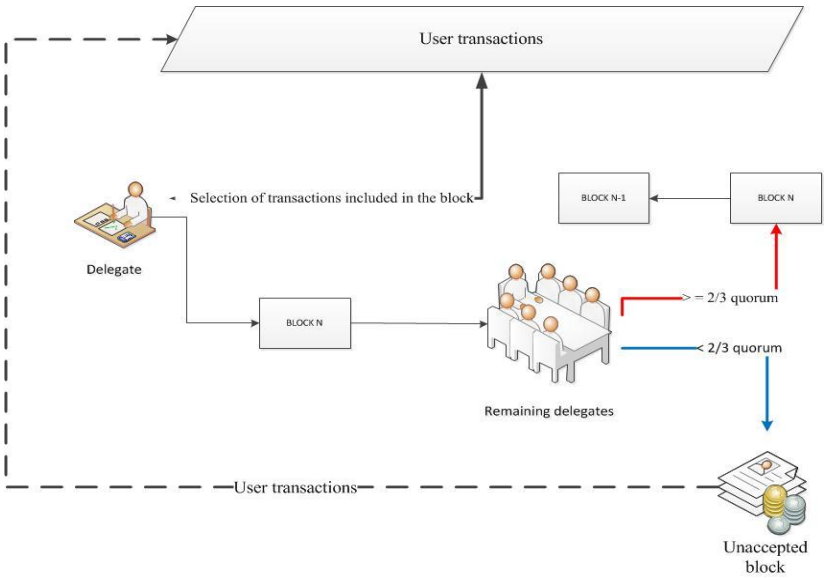

Figure 3. Voting process

3. CONCLUSION

The development of educational blockchain networks calls for a coordinated set of measures that ensure their stable, efficient, and trustworthy functioning. These measures include creating mechanisms for the automatic allocation of miner shares in the form of reputation-based rewards to maintain fairness, establishing node-rating practices that discourage improper behavior and reinforce positive actions, and advancing P2P protocols to secure and streamline communication across the system. This paper proposes an algorithm for achieving consensus in decentralized block verification by nodes in an educational network based on the formation of a reputation rating for participants. The parameters of reputation are indicators of the professional activity of educational institutions and their informational contribution to the functioning of the network. Financial investments are not taken into account. To reconcile reputation indicators with different semantic content, fuzzy sets are used. Collectively, these efforts aim to build an educational blockchain infrastructure that is both effective and reliable.

FUNDING INFORMATION

The authors declare that no funding was received for this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Igor Ivanov	✓	✓		✓	✓	✓			✓	✓		✓	✓	
Svetlana Zhdanova		✓	✓			✓	✓	✓	✓		✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

REFERENCES

[1] H. Yongqiang and Y. Jinwu, "Study on the evaluation system of e-learning based on e-learning portfolio," in *International Conference on Information and Management Engineering*, 2011, pp. 420–426, doi: 10.1007/978-3-642-24010-2_57.

[2] L. S. Yanthan *et al*., "Unlocking the potential of e-learning platforms in education," *International Journal of Science and Research Archive*, vol. 15, no. 3, pp. 1154–1164, Jun. 2025, doi: 10.30574/ijsra.2025.15.3.1836.

[3] M. Ponmani and R. Geetha, "Integration of zone of proximal development (ZPD) and ICTs in language learning," in *Contemporary ELT Strategies in Engineering Pedagogy: Theory and Practice*, 1st ed., S. Mekala and R. Geetha, Eds., New Delhi: Routledge India, 2022, pp. 237–251, doi: 10.4324/9781003268529-20.

[4] A. Allman, A. Kocnevaite, and F. Nightingale, "The effectiveness of online portfolios for assessment in higher education," in *The IAFOR International Conference on Education*, Mar. 2021, pp. 469–480, doi: 10.22492/issn.2189-1036.2021.35.

[5] L. J. Børresen and S. A. Skjerven, "Detecting fake university degrees in a digital world," University World News. Accessed: Jul. 24, 2025. [Online]. Available: https://www.universityworldnews.com/post.php?story=20180911120249317

[6] A. Hesselbäck, "The modern counterfeit industry and higher education," 2016, [Online]. Available: http://www.skvc.lt/uploads/documents/files/Naujienos/Andre_Hesselback_Vilnius_November_2016.pdf

[7] Government of the Russian Federation, "Resolution of the Government of the Russian Federation of August 26, 2013 No. 729 "On the Federal Information System 'Federal Register of Information on Education Documents and (or) Qualifications, and Training Documents,'" (in Russian) Base.garant.ru. Accessed: Jul. 24, 2025. [Online]. Available: https://base.garant.ru/70441478/

[8] Viceministerio de Educación Superior – SENESCYT Ecuador, "Central Registry, Scholarships, Research, and Innovation," (in Spanish), Siau.senescyt.gob.ec. Accessed: Jul. 24, 2025. [Online]. Available: https://www.educacionsuperior.gob.ec/

[9] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world*. New York: Penguin, 2016.

[10] X. Wang, M. Younas, Y. Jiang, M. Imran, and N. Almusharraf, "Transforming education through blockchain: a systematic review of applications, projects, and challenges," *IEEE Access*, vol. 13, pp. 13264–13284, 2025, doi: 10.1109/ACCESS.2024.3519350.

[11] C. Banga and F. S. Ujager, "Blockchain revolution in education and lifelong learning," in *Frameworks for Blockchain Standards, Tools, Testbeds, and Platforms*, Y. Ramakrishna and P. K. Keer, Eds., Hershey, PA: IGI Global Scientific Publishing, 2024, pp. 131–154, doi: 10.4018/979-8-3693-0405-1.ch006.

[12] T. K. Vashishth, V. Sharma, K. K. Sharma, and B. Kumar, "A novel approach for implementing blockchain technology in the education sector," in *Disruptive Technologies in Education and Workforce Development*, J. A. Delello and R. R. McWhorter, Eds., Hershey, PA: IGI Global Scientific Publishing, 2024, pp. 27–50, doi: 10.4018/979-8-3693-3003-6.ch002.

[13] S. Hu, L. Hou, G. Chen, J. Weng, and J. Li, "Reputation-based distributed knowledge sharing system in blockchain," in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, Nov. 2018, pp. 476–481, doi: 10.1145/3286978.3286981.

[14] Central Bank of the Russian Federation, "Report on public consultations on distributed ledger technologies," (in Russian), 2017. [Online]. Available: https://www.cbr.ru/content/document/file/36007/reestr_survey.pdf

[15] A. H. Mohsin *et al*., "Blockchain authentication of network applications: taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Computer Standards & Interfaces*, vol. 64, pp. 41–60, May 2019, doi: 10.1016/j.csi.2018.12.002.

[16] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.

[17] L. Mercenne, K.-L. Brousmiche, and E. B. Hamida, "Blockchain studio: a role-based business workflows management system," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Nov. 2018, pp. 1215–1220, doi: 10.1109/IEMCON.2018.8614879.

[18] Monika and R. Bhatia, "Cross-blockchain decentralized asset transfer protocol for public blockchains," *International Journal of Communication Systems*, vol. 37, no. 6, p. e5709, Apr. 2024, doi: 10.1002/dac.5709.

[19] M. Nassar, O. Rottenstreich, and A. Orda, "CFTO: communication-aware fairness in blockchain transaction ordering," *IEEE Transactions on Network and Service Management*, vol. 21, no. 1, pp. 490–506, Feb. 2024, doi: 10.1109/TNSM.2023.3298201.

[20] R. Khaira, "Rs 500, 10 minutes, and you have access to billion Aadhaar details," The Tribune India. Accessed: Jul. 24, 2025. [Online]. Available: https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361/

[21] A. M. Antonopoulos, *Mastering Bitcoin: programming the open blockchain*. Sebastopol, CA: O'Reilly Media, Inc., 2017.

[22] M. Sharples and J. Domingue, "The blockchain and kudos: a distributed system for educational record, reputation and reward," in *European Conference on Technology Enhanced Learning*, 2016, pp. 490–496, doi: 10.1007/978-3-319-45153-4_48.

[23] E. V. Cano, E. L. Meneses, and J. L. S. Sánchez-Serrano, *The expansion of open knowledge: MOOCs*. Barcelona: Editorial Octaedro, (in Spanish), 2013. [Online]. Available: https://diposit.ub.edu/items/23cd9957-bc25-464e-9579-168e49ad2332

[24] A. Meier and H. Stormer, "Blockchain = distributed ledger + consensus," *HMD Praxis der Wirtschaftsinformatik*, vol. 55, no. 6, pp. 1139–1154, Dec. 2018, doi: 10.1365/s40702-018-00457-7.

[25] BlockTac, "Acerca de BlockTac," Blocktac.com. Accessed: Jul. 24, 2025. [Online]. Available: https://www.blocktac.com/acerca-de/

[26] IDEFØ, "IDEFØ – function modeling method," Idef.com. Accessed: Jul. 24, 2025. [Online]. Available: https://www.idef.com/idefo-function_modeling_method/

[27] I. Ivanova, S. Zhdanova, and E. Ivanov, "Block validation protocol in a distributed blockchain system with social orientation," in *International Conference on Health and Social Care Information Systems and Technologies (HCist)*, 2024, pp. 369–373. [Online]. Available: https://scika.org/projman/2024/CONTENTS/downloads/boa2024.pdf

[28] L. A. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning—I," *Information Sciences*, vol. 8, no. 3, pp. 199–249, 1975, doi: 10.1016/0020-0255(75)90036-5.

[29] L. A. Zadeh, "Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems," in *Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications*, 1998, pp. 1–9, doi: 10.1007/978-3-642-58930-0_1.

BIOGRAPHIES OF AUTHORS

Igor Ivanov is professor at Faculty of Science and Engineering, Milagro State University, Ecuador. He received an engineer degree in Applied Mathematics from the National Aerospace University (Kharkov, Ukraine). He received his Ph.D. degree in Computer Science from Belgorod State Technological University (Belgorod, Russia). He worked for many years at universities in Ukraine, Russia, and Ecuador, including chairing the Department of Information Technology in Belgorod. He has written several textbooks on system modeling and information theory. His research interests include information technology in education and modeling of social processes. Igor Ivanov is a member of the editorial board and reviewer of several scientific journals in Spain and Ecuador. He can be contacted at email: i.v.ivanov1960@gmail.com.

Svetlana Zhdanova earned her degree in Information Systems Engineering from Belgorod State Technological University in 2009. She received her master's degree in Information Security in 2020. She is a senior lecturer at the Department of Information Technology, Faculty of Information Technology and Management Systems at Belgorod State Technological University, Belgorod, Russia. At the same university, she headed the Laboratory of Multimedia Systems. Her research interests include theoretical and practical aspects of information security and distributed data registries. She can be contacted at email: svetnii@mail.ru.