Volodymyr Malovichko[1], Roman Rybalka[2], Kostiantyn Honcharov[3]

Ukrainian State University of Science and Technologies, Dniepr

https://doi.org/10.29316/9788368103304_8

PROPOSAL FOR ENHANCING SUSTAINABILITY IN THE DIGITALISATION OF EDUCATION IN THE USUST

PROPOZYCJA ZWIĘKSZENIA ZRÓWNOWAŻONEGO ROZWOJU W CYFRYZACJI EDUKACJI W USUST

Abstract

The purpose of this study is to develop a proposal to enhance the resilience of the education-related network infrastructure at the Ukrainian State University of Science and Technologies by utilising blockchain technology. This study focuses on defining the criteria for selecting the best candidate among existing blockchain frameworks, selecting one, and evaluating its performance in terms of transaction throughput using five regression and three artificial neural network models. The best model is then selected based on the mean-squared error. Findings showed that the current network topology is sufficient to allow deploying and maintaining the Hyperledger Fabric. This study implies that network throughput can be predicted for a given number of peers and endorsers using the selected model.

Keywords: blockchain, regression, radial basis neural network, Hyperledger Fabric

[1] https://orcid.org/0009-0008-2704-5555, e-mail: v.v.malovichko@ust.edu.ua
[2] https://orcid.org/0000-0001-7444-0517, e-mail: r.v.rybalka@ust.edu.ua
[3] https://orcid.org/0000-0002-0432-1077, e-mail: k.v.honcharov@ust.edu.ua

Streszczenie

Celem badania jest stworzenie propozycji zwiększenia odporności infrastruktury sieciowej związanej z edukacją Ukraińskiego Państwowego Uniwersytetu Nauki i Technologii w oparciu o technologię blockchain. Badanie koncentruje się na zdefiniowaniu kryteriów wyboru najlepszego kandydata spośród istniejących frameworków blockchain, wybraniu jednego z nich i ocenie jego wydajności pod kątem przepustowości transakcji za pomocą pięciu modeli regresji i trzech modeli sztucznych sieci neuronowych, przy jednoczesnym wyborze najlepszego modelu z uwzględnieniem błędu średniokwadratowego. Wyniki badań wykazały, że obecna topologia sieci jest wystarczająca do wdrożenia i utrzymania Hyperledger Fabric. Badanie sugeruje, że przepustowość sieci można przewidzieć dla danej liczby peerów i endorserów, biorąc pod uwagę wybrany model.

Słowa kluczowe: blockchain, regresja, radialna sieć neuronowa, Hyperledger Fabric

Introduction

The current stage of societal development is characterised by the rapid proliferation of digital technologies across all areas of human activity. Digitalisation has become a crucial prerequisite for the innovative advancement of the economy, science, and education. In higher education, it enhances the efficiency of educational process management, expands access to academic resources, and fosters new learning formats and interactive engagement between students and instructors. The necessity of digitalising educational processes is driven not only by global trends but also by the need to adapt to contemporary challenges, including data security and resilience against cyber threats.

In Ukraine, the digitalisation of education has become particularly relevant following the COVID-19 pandemic and the full-scale invasion by the Russian Federation (RF). On the one hand, the introduction of digital technologies facilitates the continuity of the educational process regardless of the learners' location; on the other hand, it introduces new challenges in the field of information security, particularly concerning the protection of personal data of students and instructors, as well as the confidentiality of educational course materials and administrative systems (Kravtsov et al., 2021; Pavlysh et al., 2023).

At present, a wide variety of digital tools are utilised across the education sector. In particular, Learning Management Systems (LMS) such as Moodle, Google Classroom, Blackboard, and others provide the ability to create educational courses, upload and integrate various types of content (lecture texts, presentations, videos, audio files, documents, and links), develop interactive assignments and tests, enable communication between students and instructors through forums, chats, and private messages, as well as monitor learners' progress and assess their performance. Video conferencing tools (Zoom, Google Meet, Microsoft Teams) enable lectures and consultations to be held online. Various online learning platforms (Coursera, edX, Udemy, and others) expand opportunities for student self-education. In addition, cloud services (Google Drive, Microsoft OneDrive) are used for collaborative project work and data storage, while administrative information systems help automate the management processes of educational institutions.

In Ukraine, several nationwide digitalisation projects are underway in the education sector. The state online platform "Diia.Osvita" offers free online courses and educational series designed to enhance digital literacy, promote professional development, and cultivate new entrepreneurial, professional, and social skills among citizens (Kyrylenko, Jakimova, 2025). The Unified State Electronic Database on Education (EDEBO) serves as an information system that ensures centralised record-keeping, promotes transparency, and automates key processes within Ukraine's education sector.

For secondary education, various national-level digital solutions have also been developed. The "All-Ukrainian Online School" electronic platform offers students nationwide access to video lessons, tests, and educational materials. Additionally, state electronic grade books and attendance journals, integrated into the software-hardware complex "AIKOM," enable automated tracking of student performance and attendance. Moreover, the educational mobile application "Mriia" is designed to support students and parents by facilitating interactive engagement with the educational process.

At the same time, higher education institutions lack unified state-standardised digitalisation solutions. Each university is compelled to develop its own platforms and tools, taking into account the specific characteristics of the educational process and the available resources (Fernández et al., 2023; Pavlysh et al., 2023). For

example, some institutions implement Learning Management Systems, such as Moodle or Google Classroom, while others develop proprietary electronic portals tailored to the university's internal needs for students and instructors. Higher education institutions also operate internal administrative information systems to manage academic processes, personnel, document circulation, and financial accounting. Such autonomy enables the creation of flexible digital solutions; however, it also complicates efforts toward unification, system integration, and maintaining a high level of cybersecurity (Areshonkov, 2020).

The localisation and organisational structure of the Ukrainian State University of Science and Technologies (USUST) make it a suitable candidate for examining proposals to improve sustainability in the digitalisation process. USUST was established in the city of Dnipro, Ukraine, in 2021 through the merger of the Dnipro National University of Railway Transport named after Academician V. Lazaryan and the National Metallurgical Academy of Ukraine (UDUNT, n.d.). At present, USUST comprises five formerly independent higher education institutions, located across five separate campuses within the city. Each institution has been reorganised into an educational and research institute. The shortest distance between adjacent campuses is the width of a roadway, while the longest distance is approximately 5 km. Operational processes at USUST are divided into intra-institute and inter-institute (university-wide) activities. Consequently, information exchange – whether in electronic or paper form – occurs between geographically distributed institutes.

Digitalised workflows at the USUST are supported through client-server interaction between automated workstations (AW) and the databases (DBs) of the respective institutes. AW functions as a rich-client application, with user access protected by passwords. Access to the AWs from the DB is organised within each institute's local area network (LAN) and is regulated by predefined user roles corresponding to the workstation's hierarchical level. The lowest level consists of departmental AWs, followed by those of the dean's offices and directorates. Independent DB instances are hosted on servers within each institute, making these DBs centralised data repositories at the institute level.

The AW automates a wide range of operational processes at USUST related to student record management. These include logging the progress of individual student study plans, generating grade sheets for recording academic performance

during assessment activities, and preparing academic transcripts and diploma supplements. The AW significantly simplifies the preparation of various student-related documents, such as submissions for student transfers, withdrawals, and reinstatements, as well as the generation of scholarship orders and directives for forming academic groups. Depending on their access rights, AW users can view statistical information, including academic group lists, student performance rankings, the presence of academic debts, affiliation with specific preferential categories, and forms of educational funding, among others. Additionally, AW users have access to operational documentation that supports the educational process, including curricula, educational programs, and related materials.

The current digitalisation support infrastructure at USUST covers the majority of the university's operational processes. However, it remains vulnerable to certain risks, including blackouts (temporary power outages lasting several hours to several days), physical damage to elements of the university's IT infrastructure, and cyber threats. Between October 2022 and September 2024, the armed forces of the RF carried out 1,024 attacks on Ukraine's energy infrastructure using aerial means of destruction (unmanned aerial vehicles and missiles) (Ghalushhenko, 2024). During 2021-2023, the RF conducted approximately 150 cyberattacks per month targeting Ukraine's infrastructure, primarily critical infrastructure systems (Чайка, 2023). Among other consequences, these attacks have resulted in partial or complete power outages in populated areas. Considering the nature and scale of threats posed by the RF, the risks of blackouts, physical destruction (or damage) to critical infrastructure facilities in Ukraine, and cyber threats are expected to persist throughout the ongoing full-scale invasion launched by the RF on 24 February 2022.

Enhancing the current organisation of client-server interaction between the AW and the DB would significantly reduce the risks associated with the aforementioned threats, even without altering the USUST's existing network infrastructure. The presence of several geographically distributed servers within USUST enables the establishment of a distributed data storage system (distributed ledger).

One of the most relevant solutions for the specified problem is blockchain. Among its advantages (Capocasale et al., 2023) are:

- DB decentralisation through redundancy – copies of the DB are stored on multiple servers (each at a respective institution), consequently eliminating a Single Point of Failure (SPoF) and increasing resilience to the failure of a single DB repository (and under certain conditions, even more);
- Immutability of DB records – data is stored in an ordered sequence of blocks that are cryptographically linked;
- Transparency – the ability to view the history of performed actions on the DB (a consequence of immutability);
- Resistance to data forgery due to consensus mechanisms, which ensures the ability to function in a network environment without complete trust in its nodes.

The need to enhance the resilience of USUST's current network infrastructure against the aforementioned threats substantiates the relevance of this research's topic.

The purpose of this research is to formulate a proposal to enhance the resilience of the IT infrastructure supporting the digitalisation of the educational process at USUST against physical threats (e.g., destruction, damage, or temporary incapacitation due to blackouts) and cyber threats.

Methodology

Current network infrastructure of USUST and risk analysis

Electronic communication between the institutes of USUST (labelled as "Organisation" in Figure 1) is carried out via the Internet, while within each institute, it is implemented through LAN. The network infrastructure of each USUST institute is organised as follows (Figure 1): Internet connectivity is provided by at least one service provider; the institute's LAN provides all (N + M) client computers (Clients) with Internet access, among which M computers are configured as AWs, whose access to the corresponding DBs is ensured through the LAN. On each institute's server (Server 1), a DB instance containing records relevant to that institute is deployed. Each AW has assigned permission roles (password-protected), enabling role-based access to the DB for reading and writing operations. Other servers (e.g., Server 2) host additional resources, including the

institute's website, a learning management system (e.g., Moodle-based "Lider"), a platform for developing practical skills for students in relevant specialities (e.g., computer engineering and cybersecurity), a library repository, and other services. On average, each institute operates about 5 servers (only 2 are shown in Figure 1).

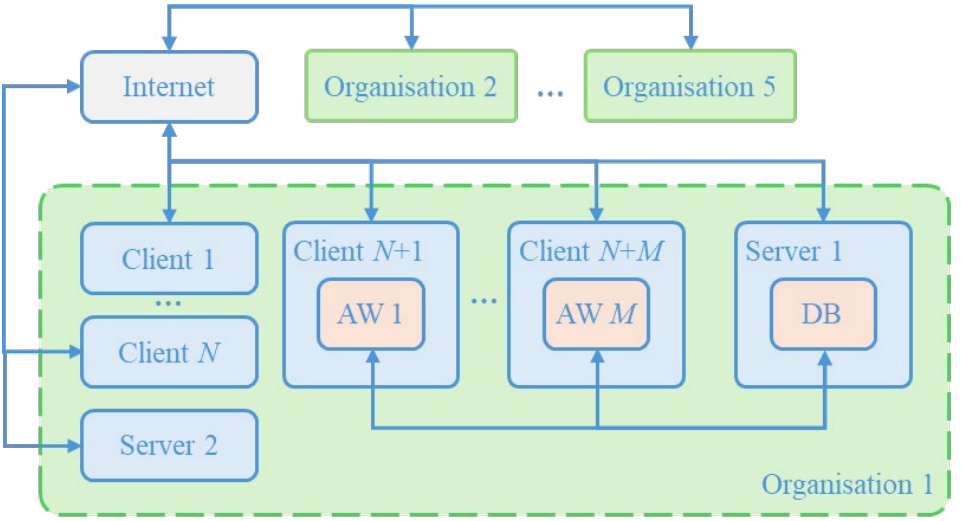


Figure 1. Network infrastructure of the USUST

Source: compiled by the author.

Blackouts can significantly hinder the maintenance of electronic communication within USUST. During blackouts, access to the institutes' DBs may be wholly or partially unavailable in cases of (1) power supply interruption at the institute or (2) power outage affecting the internet service provider's equipment. Under the current USUST network structure (Figure 1), DB access for a given institute is impossible in the first case and limited to the institute's LAN in the second.

The centralised placement of DBs (Figure 1) within each USUST institute has certain drawbacks typical of this network topology. Among these drawbacks (Merlec, In, 2024) (Yuan et al., 2025) (Nasir et al., 2024) are the following: SPoF (Single Point of Failure) – a server failure makes access to the corresponding DB impossible; data tampering – unauthorized modification of DB records; limited data transparency – lack of a built-in capability to trace the sequence of DB modifications; and scalability limitations – reduced performance due to the

potential increase in the volume of requests directed to a single processing point, i.e., the server.

Table 1 presents the results of risk identification and analysis for the current configuration of the USUST network infrastructure. As shown in this table, risk R1 has the highest likelihood and impact scores. Therefore, its processing priority is also the highest.

Table 1. Risk identification & analysis for the current configuration of the USUST network

Risk ID	Description	Source	Likelihood	Impact
R1	Blackouts leading to DB/server downtime	War-related power outages, unstable energy supply	High	High (loss of service continuity, disruption of academic processes)
R2	Internet disconnection between institutes	War-related infrastructure damage, Internet Service Provider issues	High	Medium (loss of inter-institute communication, delays)
R3	Single point of failure of the central server	Hardware failure, misconfiguration, or cyberattack	Medium	High (unavailability of services, data loss)
R4	Data tampering within the centralised DB	Insider misuse or compromised AW credentials	Medium	High (loss of data integrity, reputational damage)
R5	Data breach exposing personal information	External hacking, weak password policies and phishing	Medium	High (legal, ethical, and reputational consequences)
R6	DDoS attack on servers or the network	External adversaries are exploiting weak network protection	Medium	Medium (temporary denial of services)

Source: compiled by the author.

A brief overview of blockchain

The use of distributed ledger technology reduces the risk associated with centralised DB storage. This technology involves storing identical copies of the DB on different network nodes (peers) and maintaining them in a consistent state.

One example of this technology is blockchain. Data in blockchain is represented as ‘blocks’ that are cryptographically linked in pairs to form a ‘chain’. This organisation of data allows blockchain to ensure at least the following (Capocasale et al., 2023): decentralisation – elimination of SPoF by storing DBs on different network nodes; significant complication of the procedure for changing block data – due to the need to change all subsequent blocks, which leads to the practical immutability of blocks; transparency – due to the ability to view all blocks in the chain.

One of the most important attributes of blockchain is the consensus algorithm. It allows consensus to be reached on the distributed ledger without the need for a single decision-making centre (i.e., SPoF is eliminated). It ensures network resilience in the event of faulty or malicious nodes or certain types of attacks (e.g., double-spending, 51% attacks, DDoS). Consensus mechanisms are classified into proof-based and voting-based (Nasir et al., 2024). The former are typically used in permissionless blockchains, while the latter are used in permissioned blockchains. As of 2022, there are approximately 30 consensus algorithms (Guru et al., 2023). Comparing the characteristics of all these algorithms is beyond the scope of this study.

In general, voting-based consensus mechanisms are more energy-efficient and faster than proof-based ones, but they can be less decentralised. The energy efficiency of voting-based consensus mechanisms stems from the lack of competition for computing power to obtain the right to create a block. Unlike, for example, Proof-of-Work (PoW), network validators do not consume significant amounts of energy. The high speed of voting-based consensus is enabled by the absence of anonymous nodes in private (permissioned) networks, which allows the use of faster consensus algorithms. On the other hand, voting-based consensus mechanisms can typically have problems with decentralisation. These consensus mechanisms are used in private (permissioned) networks, where decision-making is limited to a predetermined set of peers. The result is a risk of collusion among these peers, which can lead to network manipulation.

Blockchain selection criteria

The effectiveness of consensus algorithms (and, as a result, network security and performance) depends on how scalability, security, and decentralisation are optimised (the so-called 'Blockchain Trilemma problem'). For instance, the PoW advantage offers high security and decentralisation, but the scalability of business transactions remains insufficient (Nasir et al., 2024). Conversely, in Practical Byzantine Fault Tolerance (PBFT) – a representative instance of Byzantine Fault Tolerance (BFT) – the use of comparatively weaker consensus algorithms results in a lower level of security than that provided by PoW, while achieving higher performance. The scalability of PBFT is, to some extent, superior to that of PoW. However, it is notably constrained by the exponential increase in communication overhead as the number of participating nodes grows. (Tomić, 2021). Choosing a consensus algorithm involves choosing a specific implementation of the Blockchain Trilemma problem solution.

When selecting a blockchain implementation, numerous criteria must be considered, which can be categorised as follows:

- Governance and Architecture: public (permissionless) or private (permissioned); level of decentralisation – the impact of the distribution of decision-making power among peers.
- Performance and Scalability (Nasir et al., 2024): transaction throughput – number of successful transactions per second (TPS); latency – the time interval between the moment a transaction is submitted and its final confirmation; scalability – the ability of blockchain to operate effectively when the number of peers and/or the volume of transactions increases; resource consumption – energy consumption, central processing unit operating time, memory capacity, channel bandwidth; complexity of deployment and maintenance.
- Security, Privacy, and Reliability: resilience to cyber-attacks, e.g., 51%, DoS, Sybil; fault tolerance – Crash Fault Tolerance (CFT), which tolerates failure (due to hardware, software or network-related issues) of f nodes (while the total number of nodes is not less than $2f + 1$) (Zhou et al., 2023), Or BFT, which tolerates even the presence of f nodes with malicious behaviour

(while the total number of nodes is not less than $3f + 1$) (Capocasale et al., 2023); the ability to ensure data and/or user confidentiality (anonymity).

- Functionality and Technical Details: consensus algorithm; programming language support; DB type; interoperability – the ability to exchange data with other blockchains; relationship to cryptocurrency.

To reduce the likelihood of risks R1-R4 (Table 1), we suggest choosing a blockchain implementation that meets the following requirements: is private (permissioned); has a moderate level of decentralisation, transaction throughput and latency; has low or moderate scalability, resource consumption, deployment and maintenance complexity, and resistance to cyber-attacks; has high fault tolerance (CFT); is capable of ensuring data confidentiality. Desirable features include support for common programming languages for blockchain development, the use of DB structures capable of handling complex queries, and the flexibility to replace the consensus algorithm with a BFT-based one if required. Non-essential features include interoperability, integrated cryptocurrency support, and mechanisms for ensuring user anonymity. When selecting blockchain requirements, the current network infrastructure of USUST (Figure 1), which operates in a relatively trustworthy environment, the expected peak transaction intensity of approximately 100 TPS, and risk identification and analysis (Table 1) were considered.

Hyperledger Fabric (HLF) has met these requirements since version 3.0; therefore, we recommend adopting HLF for USUST. In HLF, every component, whether internal or external to the network – such as peers, orderers, client applications, and administrators – possesses a unique digital identity. Consequently, all network entities are explicitly identifiable.

The HLF ledger comprises two components: the current state of the ledger (the world state), which is maintained in a DB, and the transaction log (the history of updates to the current state), which forms the blockchain and is implemented as a file. HLF enables ledger operations – such as executing transactions, performing queries, and managing controlled access to the ledger – through smart contracts, which can be defined within the same chaincode or across separate chaincodes (Hyperledger Fabric, n.d.) HLF supports Go, Node.js, and Java for chaincode implementation. When a client application invokes a chaincode function to interact with the ledger (for read or write operations), a transaction is generated. These

transactions trigger state transitions, and their records collectively constitute the ledger in HLF.

In HLF, ledger hosting is carried out by a set of peer nodes (peers), which utilise smart contracts to enable read and write operations on the ledgers (Hyperledger Fabric, n.d.) Each peer maintains copies of the ledgers and smart contracts and exposes a set of APIs that allow client applications to interact with it. Beginning with HLF version 2.4, the Fabric Gateway Service (FGS) is deployed on peers, enabling them to manage transaction proposals and endorsements. The number of peers responsible for endorsing transactions (referred to as 'endorsers') is determined by the endorsement policy of a given network. In addition to peer nodes, there are orderer nodes (also known as orderers) and the corresponding ordering service, which ensure ledger consistency. Orderers aggregate transactions into blocks and subsequently distribute these blocks to peers for validation and commitment. At the same time, orderers do not maintain a state database and do not support unilateral switching from CFT (Replication and Fault Tolerant – Raft protocol, which is an example of CFT) to BFT (using the SmartBFT protocol).

Performance evaluation of the selected blockchain

Evaluating the performance of blockchain systems in general, and HLF in particular, is a non-trivial task due to the influence of numerous factors, including transaction size, block size, network scale, and available hardware resources such as CPU, memory, disk space, and disk or network I/O. As a rule, such an assessment is performed for a network of a specific configuration by changing the blockchain parameters using computer modelling.

With an increase in the number of peers, HLF performance is expected to improve due to the ability to load-balance endorsement requests across them (Hyperledger Fabric, n.d.) The results of HLF modelling reported by (Guggenberger et al., 2022) indicate that the highest sustainable throughput, approximately 400 TPS, was achieved with a peer count ranging from 8 to 32, a fixed number of endorsers (2) under an endorsement policy of '2 of 8 endorsers,' the Raft consensus mechanism, and CouchDB as the state DB. It is noteworthy that the mentioned modelling was performed for HLF version 2.0 and validated for version 2.2. Although the FGS has been available since version 2.4, this remains

the most comprehensive and detailed open-access study identified on the topic. We further assume that the introduction of FGS does not significantly influence the outcomes of the referenced modelling.

In general, an increase in the number of orderers is expected to reduce HLF performance. However, modelling results reported by Guggenberger et al. (2022) using the Raft consensus mechanism and CouchDB indicate that, for request rates below 1500 TPS, increasing the number of orderers to 64 has almost no impact on the maximum sustainable throughput. A slight improvement in throughput was observed when using four orderers.

To perform the max sustainable throughput assessment, depending on the number of peers and endorsers, we implemented and investigated the following machine learning models:

- Regressions: decision tree regression (DTR), ordinary least squares linear regression (LR), polynomial linear regression (PLR), random forest regression (RFR), support vector regression (SVR).
- Artificial neural networks (ANN): generalised regression ANN (GRANN), radial basis ANN (RBANN), exact radial basis ANN (ERBANN).

Regression models were implemented in Python using NumPy, pandas, and scikit-learn. ANN models were implemented in MATLAB (Deep Learning Toolbox). The raw dataset for training and validating these models was obtained from Guggenberger et al. (2022) and consists of 21 records. The dataset comprises three model inputs – total number of peers, endorsements, and orderers – and one output, the maximum sustainable throughput (TPS). Prior to model training, the dataset was analysed to identify correlations among the input variables. A strong correlation ($r = 0.89$) was observed between the total number of peers and the number of orderers. Consequently, orderers were excluded from the model inputs. The raw dataset was then randomly permuted and divided into 16 records for training and 5 for validation. Each subset was normalised to the range (0, 1).

Initially, we conducted the training and simulation of regression models. Their performance was evaluated using the coefficient of determination (R^2). For the model achieving the highest R^2 value, we computed the mean squared error (MSE) between the model's predicted values (obtained using the validation dataset) and the corresponding true values. This MSE value, denoted ε_{reg}, served as a reference for evaluating the ANN models' effectiveness.

Subsequently, we trained and simulated ANN models. The performance of the implemented models (GRANN, RBANN, and ERBANN) is strongly influenced by a key parameter – the spread of radial basis functions (hereinafter referred to as "spread"). The smoothness of function approximation increases proportionally with the spread value. To determine the optimal spread for each ANN model, we performed training, simulation, and MSE calculation following the same procedure used for regression models. The spread parameter for each model was sequentially varied within the range (1 × 10^-5, 2 × 10^-5… 10), encompassing 1,000 values. To identify the best-performing model, we compared the obtained MSE values with ε_{reg} and selected the ANN model with the smallest MSE below ε_{reg}, along with its corresponding spread value.

The choice of DB type is a key factor influencing HLF performance. When LevelDB is used, throughput can be two to three times higher than that achieved with CouchDB. Increasing the number of endorsers enhances system robustness but reduces throughput. Furthermore, the performance degradation observed with LevelDB is more pronounced than that with CouchDB (Guggenberger et al., 2022).

Optimising the deployment of HLF elements on different servers affects overall performance. According to the simulation results (Guggenberger et al., 2022), the highest throughput was observed when orderers, peers, and CouchDB instances were deployed on separate servers. When two or more of these entities were deployed on a single server, throughput decreased by approximately 35% with three entities per server.

Several other factors can influence HLF performance. A modest improvement of approximately 12% can be achieved by switching from a single-channel to a dual-channel configuration (Guggenberger et al., 2022). However, further increasing the number of channels does not yield a noticeable increase in maximum throughput. As the number of channels grows, so do the network's hardware requirements. Server hardware resources have a substantial impact on HLF performance. For instance, upgrading from two threads per physical CPU core (with 8 GiB of memory) to four threads (with 16 GiB of memory) improves CouchDB performance by approximately 90% (Guggenberger et al., 2022). It is worth noting that additional hardware upgrades yield diminishing returns

in performance. Therefore, given the associated cost increase, this approach to enhancing HLF performance requires economic justification.

Finally – the block parameters. Analysis of the dependencies of maximum sustainable throughput on block timeout, maximum block size, and size of data per transaction reveals certain values (approximately) at which a significant change in this performance occurs (Guggenberger et al., 2022): block timeout 0.5s, maximum block size about 100 transactions, size of data per transaction 1 KB.

Results

Hyperledger Fabric performance modelling results

Figure 2 shows the coefficient of determination values for five regression models (DTR, LR, PLR, RFR, and SVR). The MSE value for the RFR model is $\varepsilon_{reg} \approx 0.014$.

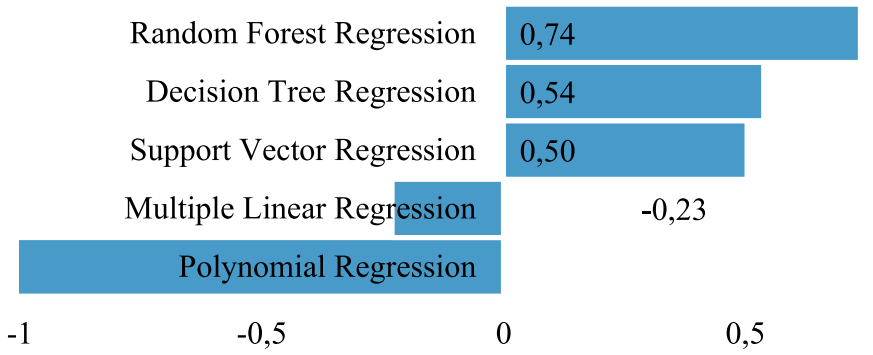


Figure 2. Coefficient of determination for the regression models

Source: compiled by the author.

Figure 3 shows the dependence of MSE on the “spread” value for each of the three considered ANN models. In this case, MSE was calculated for the validation dataset.

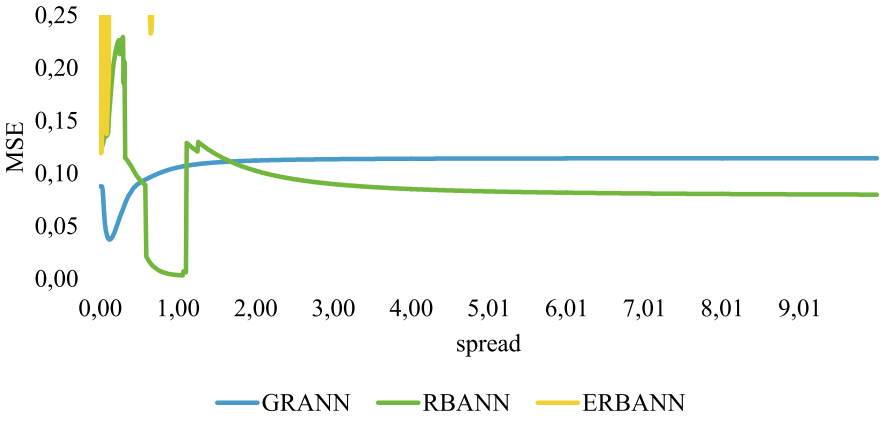


Figure 3. Mean-squared error for the ANN models

Source: compiled by the author.

Figure 4 presents the results of predicting the maximum sustainable throughput (TPS) for the RBANN model at a "spread" value of 1.06, with a corresponding MSE of 3.23×10^{-3}.

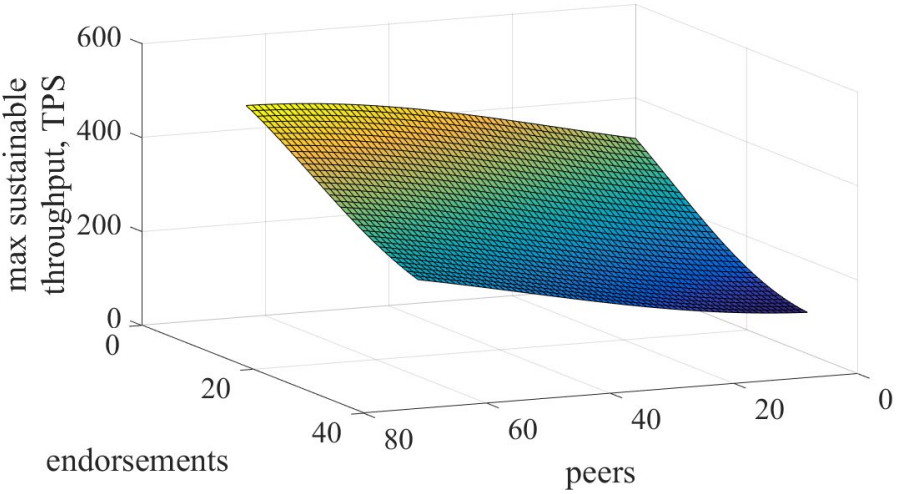


Figure 4. Max sustainable throughput predicted by RBANN

Source: compiled by the author.

Proposed network architecture

The proposed network infrastructure of USUST at the initial stage of HLF implementation is shown in Figure 5. In each institute (Organisation 1 … Organisation 5), one peer (P1) and one orderer (O1) are deployed on separate servers (Server 1 and Server 2). Thus, the USUST network comprises 5 orderer nodes and 5 peer nodes. On the same servers where the peers (P1) are deployed, a CouchDB is also deployed.

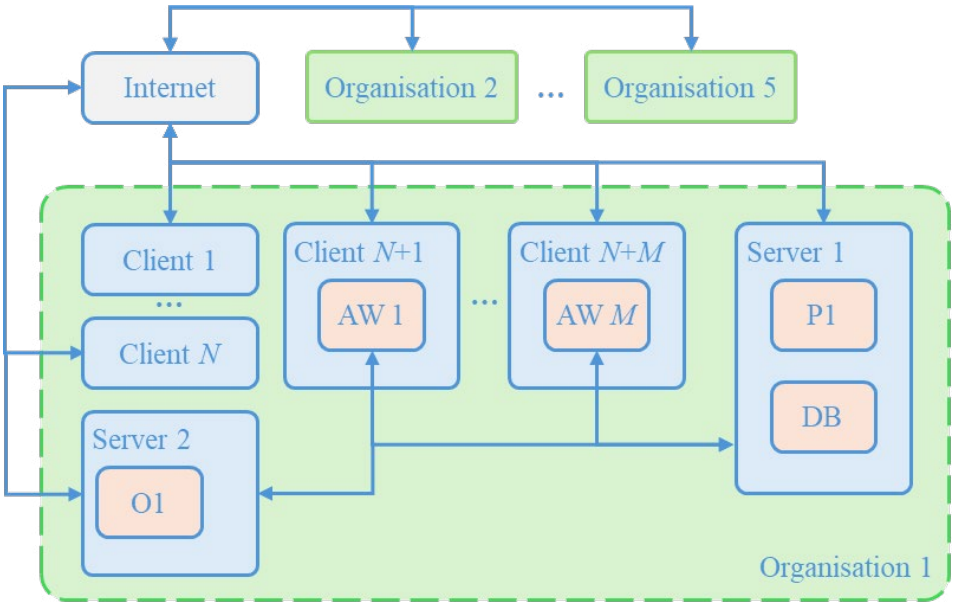


Figure 5. Proposed network infrastructure

Source: compiled by the author.

The configuration of HLF deployed on the proposed network infrastructure (Figure 5) is as follows: a single channel is available to all peers; the consensus mechanism is CFT (Raft protocol); no private collections are provided; the FGS enables an application connected to the institute's LAN to connect to one of the available trusted peers in this network; the number of endorsers is 2; the block timeout is 0.5 s; the maximum block size is about 100 transactions; the data size per transaction is 1 KB. According to the RBANN model evaluation shown

in Figure 4, for this number of peers and endorsers, the maximum sustainable throughput is expected to reach approximately 300 TPS.

Discussion

According to Table 1, risk R1 is identified as the highest-priority risk. To mitigate risk R1, it is sufficient to configure HLF to use the CFT (Raft protocol) consensus mechanism. Using five orderer nodes with Raft consensus ensures HLF operation in the presence of up to two non-Byzantine faults. Increasing the number of orderer nodes may reduce network performance. To tolerate up to three orderer node failures, their number should be increased to seven. The use of the Raft protocol also helps to mitigate the impact of risks R2 and R3 (Table 1), since they are similar to R1. Still, their effect is weaker, at least because communication is maintained within the institute's LAN, and at most because of possible access to a subset of servers in other institutes (Figure 3). Risk R6 (Table 1) in HLF is mitigated by verifying the digital identity of each network entity and by the ability of both available consensus mechanisms (CFT and BFT) to tolerate server access delays, which are equivalent to risks R1, R2, and R3. The characteristics of risk R5 (Table 1) remain unchanged and are more dependent on the organisation's access policy for authorised personnel than on HLF's built-in capabilities. To mitigate risk R4 (Table 1), we propose switching from CFT (Raft protocol) to BFT (SmartBFT protocol) by utilising HLF's built-in functionality. At the same time, we acknowledge that in a permissioned network such as HLF, resilience against specific cybersecurity threats is lower than in a permissionless network, for example, one that uses PoW.

Among the regression models evaluated by the coefficient of determination (Figure 2), the best-performing model was RFR, yielding a coefficient of determination of 0.74. The poorest performance was observed for PLR (less than -5.7 million). Therefore, the reference value ε_{reg} was computed specifically for RFR. As shown in Figure 3, starting from a "spread" value of approximately 0.64, the MSE for ERBANN becomes quite large and exceeds the plot range. The MSE curves for GRANN and RBANN tend to approach asymptotic values as the "spread" increases: 0.12 and 0.08, respectively. The most noticeable changes in the curves occur within the "spread" parameter range up to approximately 2.5. Among the three dependencies, the MSE for RBANN reaches the smallest value:

3.23×10^{-3} at a "spread" of 1.06, which is lower than ε_{reg}. Therefore, the RBANN model exhibits lower error than RFR and, consequently, than the other regression models. Hence, RBANN was selected for further analysis.

As shown in Figure 4, throughput increases with the number of peers when the number of endorsers remains constant. In this case, the throughput growth rate up to approximately 30 peers follows an O(n) order. For example, increasing the number of peers from 5 to 10 results in an approximate 4.5 % increase in throughput. Beyond 30 peers, throughput growth scales at O(log *n*), and increasing the number of peers from 30 to 60 results in approximately a 12% increase in throughput. This relationship can be used to assess the cost-effectiveness of adding new peers to the network. It is also worth noting that as the number of peers increases, the network's robustness improves. When the number of endorsers increases (while the number of peers remains fixed), the throughput declines more rapidly than when the number of peers decreases (with a fixed number of endorsers). This observation can guide rational adjustments to the network topology.

Additional performance gains can be achieved by deploying CouchDB on a separate server. Provided that the servers have sufficient processing capacity, further performance improvements can be achieved by using two channels instead of one. An interesting area for future research is integrating LevelDB with an off-chain database to enhance HLF (Hyperledger Fabric Docs Main Documentation, n.d.) performance. This approach allows, for example, the deployment of an SQL DB created from HLF while operating outside of it. In this way, significantly better DB management capabilities can be achieved without affecting HLF performance.

Conclusions

This study aimed to develop and justify a blockchain-based proposal to enhance the resilience of USUST's IT infrastructure against hardware-, software-, or network-related issues, as well as cyber threats. The findings of this study demonstrate that Hyperledger Fabric (HLF) can be deployed within the USUST network without significant modifications to its topology, thereby enabling the achievement of the defined objective. We have substantiated the parameters under which HLF delivers sufficient performance to support communication processes associated with the USUST network's educational environment. A key contribution

of this work is the development of eight predictive models: five regression-based and three artificial neural networks (ANNs) that capture the relationship between maximum sustainable throughput and the total number of peers and endorsements. Each model was evaluated, and the optimal one (RBANN) was selected. This model enables the prediction of throughput values as a function of the number of peers and endorsements, thereby facilitating the assessment of resource efficiency in configuring and maintaining the HLF network.

This study is limited to a relatively small number of available datasets, particularly those with peers that exhibit large step sizes at higher numbers (above 16); therefore, the findings cannot be generalised well. Despite this limitation, this study makes a significant contribution by applying it to the current topology of the USUST network, which is well-represented in the mentioned dataset (with fewer than 16 peers). As a result, it is suggested that future research conduct a study with a larger dataset.

References

1. Areshonkov, V. J. (2020). Cyfrovizacija vyshhoji osvity: Vyklyky ta vidpovidi. *Herald of the National Academy of Educational Sciences of Ukraine*, *2*(2). https://doi.org/10.37472/2707-305X-2020-2-2-13-2
2. Capocasale, V., Gotta, D., Perboli, G. (2023). Comparative analysis of permissioned blockchain frameworks for industrial applications. *Blockchain: Research and Applications*, *4*(1), 100113. https://doi.org/10.1016/j.bcra.2022.100113
3. Fernández, A., Gómez, B., Binjaku, K., Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. *Education and Information Technologies*, *28*(10), 12351-12382. https://doi.org/10.1007/s10639-022-11544-0
4. Guggenberger, T., Sedlmeir, J., Fridgen, G., Luckow, A. (2022). An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Computers & Industrial Engineering*, *173*, 108716. https://doi.org/10.1016/j.cie.2022.108716
5. Guru, A., Mohanta, B. K., Mohapatra, H., Al-Turjman, F., Altrjman, C., Yadav, A. (2023). A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Applied Sciences*, *13*(4), 2604. https://doi.org/10.3390/app13042604
6. Kravtsov, O. V., Kravtsova, T. V., Lashchenko, O. V. (2021). Derzhavna polityka v sferi vyshchoi osvity Ukrainy v umovakh tsyfrovizatsii. *Bulletin of the National*

University of Civil Protection of Ukraine. Series: Public Administration, 1(14), 73–85. https://doi.org/10.52363/2414-5866-2021-1-10

7. Kyrylenko, S. A., Jakimova, M. E. (2025). Dejaki pytannja formuvannja cyfrovoji kompetentnosti zdobuvachiv vyshhoji osvity Ukrajiny ta Poljshhi. *Osvita Ta Rozvytok Obdarovanoji Osobystosti*, *1*, 129-133. https://doi.org/10.63437/2309-3935-2025-1(96)-17
8. Merlec, M. M., In, H. P. (2024). Blockchain-Based Decentralised Storage Systems for Sustainable Data Self-Sovereignty: A Comparative Study. *Sustainability*, *16*(17), 7671. https://doi.org/10.3390/su16177671
9. Nasir, N. M., Hassan, S., Mohd Zaini, K. (2024). Securing Permissioned Blockchain-Based Systems: An Analysis on the Significance of Consensus Mechanisms. *IEEE Access, 12*, 138211-138238. https://doi.org/10.1109/ACCESS.2024.3465869
10. Pavlysh, T., Basarab, V., Tereshhenko, O., Roghiv, M. (2023). Cyfrovizacija osvitnjogho procesu v zakladakh vyshhoji osvity v umovakh vojennogho stanu. *Osvitni Obriji*, *56*(1), 106-109. https://doi.org/10.15330/obrii.56.1.106-109
11. Tomić, N. Z. (2021). A Review of Consensus Protocols in Permissioned Blockchains. *Journal of Computer Science Research*, *3*(2), 19-26. https://doi.org/10.30564/jcsr.v3i2.2921
12. Yuan, F., Huang, X., Zheng, L., Wang, L., Wang, Y., Yan, X., Gu, S., Peng, Y. (2025). The Evolution and Optimization Strategies of a PBFT Consensus Algorithm for Consortium Blockchains. *Information*, *16*(4), 268. https://doi.org/10.3390/info16040268
13. Zhou, S., Li, K., Xiao, L., Cai, J., Liang, W., Castiglione, A. (2023). A Systematic Review of Consensus Mechanisms in Blockchain. *Mathematics*, *11*(10), 2248. https://doi.org/10.3390/math11102248

Netography

1. Ghalushhenko, G. (2024). *Za dvaroky rosija atakuvala ukrajinsjku energhetyku ponad 1000 raziv*. Ministerstvo energhetyky Ukrajiny. Retrieved from: https://mev.gov.ua/novyna/za-dva-roky-rosiya-atakuvala-ukrayinskuenerhetyku-ponad-1000-raziv-herman-halushchenko (dostęp: 02.09.2025).
2. Hyperledger Fabric. (n.d.). *A Blockchain Platform for the Enterprise*. Retrieved from: https://hyperledger-fabric.readthedocs.io/en/latest/ (access: 02.09.2025).

3. UDUNT. (n.d.). *Istorija uniwersytetu*. Retrieved from: https://ust.edu.ua/universytet/istoriya-universytetu/ (access: 02.09.2025).
4. Чайка, О. (2023). *Kiberataky na energhosystemu Ukrajiny: Jak kompaniji protystojatj khakeram?* Forbes. Retrieved from: https://forbes.ua/company/rosiyski-khakerikoordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yakukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242 (access: 02.09.2025).