Received: 20 June 2022 | Revised: 19 January 2023 | Accepted: 6 March 2023

IET Blockchain

DOI: 10.1049/blc2.12028

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm

Umair B. Chaudhry[1,2] | **Aysha K. M. Hydros**[2]

[1]School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK

[2]School of Computing, Engineering and Information Sciences, Northumbria University, London, UK

Correspondence
Umair B. Chaudhry, School of Electronic Engineering and Computer Science, Queen Mary University of London, Mile end road, London E1 4NS, UK.
Email: ubchaudhry@gmail.com

Abstract

Cyber security in the banking sector is of high importance nowadays. The rate of cyber-attacks is spiking every year, and the implementation of strong cybersecurity models is required to ensure the confidentiality and integrity of data. Since protecting a bank requires a wide range of security practices, this paper focuses on protecting the bank resources from malicious actors and securing the transactions using a blockchain consensus mechanism that uses a zero-trust security approach among the participants in the transaction. In addition to the framework, an algorithm for blockchain-based online transactions was designed to make use of practical implementation in the future. The ideas formulated during the research and literature review were integrated to design the framework and the algorithm. The proposed framework ensures that the security of the banking sector can be enhanced by adopting the zero-trust concept and blockchain technology. The consensus algorithms used for the transaction make it immutable and decentralized. Zero-trust principles adopted in the model ensure the confidentiality and integrity of the banking system.

1 | INTRODUCTION

As technology advances, organizations and institutions are moving towards digital transformation. This quick transition is making businesses evolve their business practices to technological innovations. Along with technological advancements, the series of cyber threats are growing exponentially. Malicious phishing attempts, ransomware attacks, and denial of service attacks are the most common attacks launched by cybercriminals. Irrespective of the size of organizations, attacks are performed to target every possible vulnerable institution. Financial institutions are subjected to a daily bombardment of cyberattacks that can result in the loss of data, reputation, and huge penalties. According to [1], a rise of 1318% in cyberattacks was faced by financial industries in 2021. The major threats to the financial sector now are climate change and cyberattacks [2]. The frequency and growth of cyberattacks is a major concern among experts now.

According to [3], seven top banks in the United Kingdom were attacked by cybercriminals, which made banks halt their services. In most cases, consumers might not lose their money, but this huge loss will affect banks losing their funds which in turn will reciprocate the economy of the nation. Since customers prefer online banking services over traditional banking systems, studies focusing on online banking security and strong access control policies should be implemented to ensure confidentiality, integrity, and data availability [4]. It is to be considered that most cyberattacks happening in organizations are due to intentional or unintentional mistakes by employees. This indicates a lack of cyber awareness among each level of employee. Cyber security should be a top concern for not only the IT team, every employee in an organization along with third-party contractors should have enough understanding of the relevance of cyber security. Policies should be evaluated at regular intervals for healthy cyber hygiene. This indicates the relevance of a zero-trust security model which will consider every user with the same trust value.

This study aims to investigate the security models used in banks and develop a framework based on zero-trust principles to protect bank assets and environments from cyberattacks. Through a systematic literature review of recent publications, the paper proposes that integrating a zero-trust model with blockchain technology can enhance the security of the banking

sector. The significance of the problem and research gap was identified through podcast interviews, critical analysis of recent publications, and TEDx talks from industry experts. A comparison of traditional security models and zero-trust models was conducted to establish the relevance of the chosen topic. The framework was designed by incorporating ideas from the analysis and key concepts from [5, 6] zero-trust architecture (ZTA) and blockchain-based zero-trust transactions from [7].

The paper is composed as follows. Section 1 introduces the problem followed by Section 2 with a detailed literature review. Section 3 discusses the methodology and puts forth the proposed model and framework. Section 4 concludes the research.

2 | LITERATURE REVIEW

The literature review mainly focuses on four areas. The first quarter discusses various studies focusing on the reasons behind cybercrimes in banks. The second section focus on the importance of implementing a zero-trust security approach in banks. The third section concentrates on the application of blockchain technology to secure bank transactions. The final area investigates the adaption of integration of zero-trust and blockchain models to secure enterprise resources and examines the necessity of such a framework to be implemented in the banking sector.

2.1 | Cyber security in banks

Scams on the internet damage individuals as well as the nation, either directly or indirectly [8]. Financial institutions are subjected to a daily bombardment of cyberattacks that can result in the loss of data, money, and trust, and as digital banking grows, they are becoming more vulnerable [9]. As technology progresses, the demand of the public to access every service online without waiting for the delay in transactions and the increase in the usage of cloud storage for bulk amounts of data makes the banking sector more vulnerable.

[10] relates the current trend in cyber risks with the Covid-19 outbreak, as the pandemic led most employees to adopt work from home culture. The comparison between pandemic-affected various industries is shown in Figure 1. As stated in [11], many financial crimes go unnoticed by the public because bank executives do not want to upset their shareholders. Executives are frightened of exposing their firm to fresh attacks, afraid of sullying its reputation as a reliable storage medium and, as a result, losing clients. This approach encourages attackers to make numerous efforts to continue with their attacks.

According to [9], banks are increasingly outsourcing to purchase and manage IT assets while controlling costs. The bank is responsible for the security of services offered under outsourced contracts, including cloud hosting. On the other hand, many banks are unaware of how their IT partners operate, and just a handful have put in place mechanisms and protocols for oversight and monitoring. Banks do not have the resources to monitor external vulnerabilities and networks or to police every vendor they engage with. Strong measures should be considered to ensure legal compliances are met to prevent penalties imposed due to data breaches. [12] discusses the ethical concepts and their application to the jobs of IT security employees. Ethical standards of the IT security team play an essential part in the banking sector's brand value and long-term reputation in the field. Although the IT security team has access to numerous system events and records, not all access and situations result in the disclosure of private and confidential information. [13] provides a security risk model that uses inline biometric measures to safeguard a customer's online banking account from being hacked. It aids in the detection of unintended transactions on their account that occurs without their knowledge. Biometric authentication techniques including face and fingerprint recognition are utilized to secure the data. Even though the model enables the development of efficient cyber security protection mechanisms in the financial system at the canonical, logical, and physical levels of representation, it still requires protection against various potential cyberattacks making it more user-friendly. The automated teller machine (ATM) security designed in [14] considers the potential use of current implementations like credit cards and sensitive data like personal Identification number (PINs) as proxies in the existing ATM security mechanisms. In every feasible transaction, the bank account holder is considered in real-time. Implementation and maintenance of the system appear straightforward. However, the definition or process of formal verification is lacking in the paper.

[11] classifies threats to banking information systems as Internal (deliberate and inadvertent activities of employees) and external (actions of third parties). Most assailants involved with financial fraud are clerks. Although top bank employees can commit crimes and do significant damage to the bank, such instances are uncommon [11]. The customers' trust is a bank's most precious asset. However, when it comes to cyber security, this trust is jeopardized. New cyber security threats may arise because of technology advancements and data governance transformations in the banking industry. Resurrecting core systems, cloud migrations, using automated decision-making models, and implementing remote office technology are all instances of emerging and shifting enterprise environments that create vulnerabilities for cyberattacks. Banks can efficiently future proof the security of their digital assets with a zero-trust approach [15].

[16] proposes a Central Bank Digital Currency Evaluation and Verification (CEV) Fframework for recommending and verifying technical solutions in the central bank digital currency (CBDC) system. This framework includes two sub-frameworks: an evaluation sub-framework that provides consensus algorithm and operating architecture solutions, and a verification sub-framework that validates the proposed solutions. The framework offers a universal CBDC solution that is compatible with different national economic and regulatory regimes. The evaluation sub-framework generates customized solutions by splitting the consensus algorithms into several components and analyzing their impacts on CBDC systems.

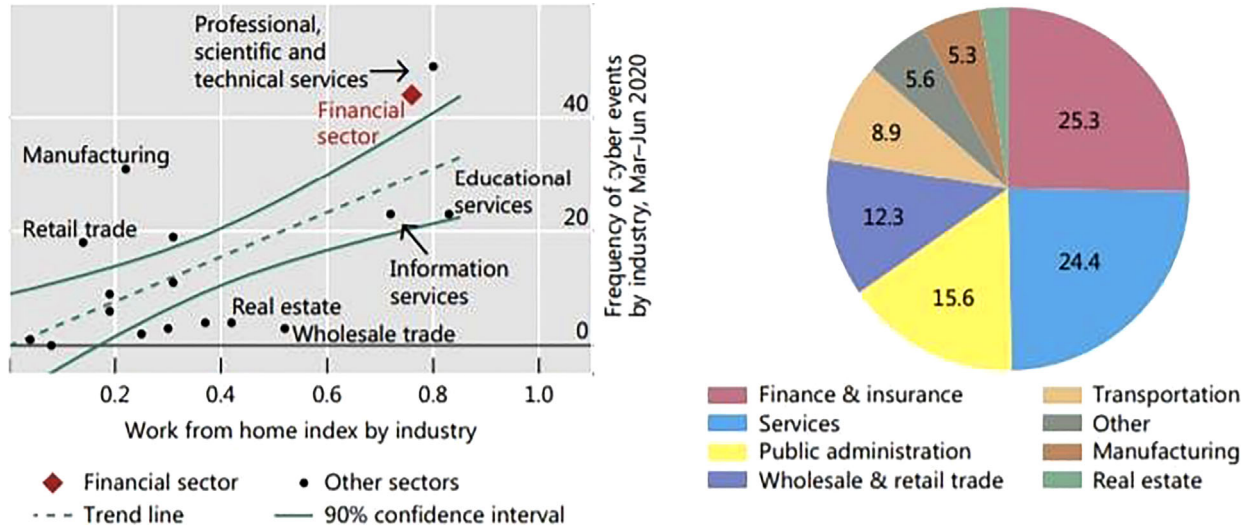


FIGURE 1 Covid-19 related cyber breaches in various sectors.

CBDC design involves a trade-off between system features—the consensus algorithm cannot achieve all system features simultaneously. The framework offers CBDC designers the flexibility to iteratively tune the trade-off between CBDC system features for the desired solution. Future work could include considering more CBDC system features and solutions into the framework, updating the impact table for proposing solutions more accurately and improving the efficiency of the verification sub-framework. Additionally, the CEV framework can also be used to propose stablecoin and other regulated cryptocurrency solutions.

2.2 | Zero-trust security in banks

In the face of a compromised network, [6] defines zero trust as a set of abstract ideas and principles aimed at reducing ambiguity in imposing precise and restricted resource access for users. ZTA is a cyber security approach that can be adopted by an organization incorporating zero-trust principles and includes integral communications, productivity devising, and access management. Based on a zero-trust architectural scheme, a combination of physically connected infrastructure as well as a virtual network along with company policies comprises a zero-trust venture. According to [17], a ZTA is a system design technique in which the network's inherent trust is eliminated. Rather, the network is presumed to be vulnerable, and every request to access the resources is checked against a set of rules. Building context ensures that a request is trustworthy, which is dependent on user authentication, authority to access, health information of the device from which the access is being requested, and the worth of requested data.

User and application authentication, device authentication, and, most critically, trust are three components of ZTA. In traditional architecture, a user is only authenticated once. A zero-trust model continuously verifies the user's identity, monitors the user's devices, and looks for any location changes made by the user's device. Furthermore, it checks for any anomalies in the program that the user is utilizing frequently. Should there be any kind of change, the architecture must immediately end the connection. Data is restored from backups in the event of any data modification, and logs of every microscopic operation are kept [18].

Implementing a zero-trust security model can result in a high-security system, which benefits business processes including the company's visibility in protecting client data. External parties with a good reputation in developing security systems may gain from the adoption of a zero-trust security model, as well as financial savings in security system audits. On the company's internal side, it has a high degree of feasibility and efficient use of time in monitoring security systems with great visibility, decreasing the complexity of creating security systems [19]. Since the zero-trust network model naturally aligns with the security concept and requirement of key secret units, important confidential units should design and deploy suitable solutions quickly [20]. For example, the zero-trust paradigm used by Google is 'BeyondCorp' [21]. Security is ensured irrespective of the location from where the user access the resources besides using a virtual private networks (VPN) is offered by BeyondCorp. Access control strategies, single sign-on solutions, end-user authentication as well as gadget authentication are all possible with BeyondCorp. The following are the BeyondCorp principles:

- The network from which you connect should not determine your ability to access services.
- Access to services is granted based on the user's identity and their device health.
- Every access attempt must be authenticated and approved before being used.
- Data encryption and access logs should be enforced for every granted access

While these installations demonstrate the practicality of zero-trust network with risk-based access control, they do not go into enough depth about how to enforce policies and implement risk-based access control in zero-trust network [22]. Hence, many organizations are still attached to presumption-based trust networks, even though zero trust is advocated by governments, industry, and academia who push for their implementation [23].

Also, the zero-trust network strategy according to [22] is based on treating the internal network and public network equally as untrustworthy. The network inside the organization's premises is organized into several divisions, each with its own set of purposes and data. Separate trust levels need to be assigned to each division that reflects the value of the resources kept there. For every access request, a trust level comparison should be conducted to grant access. [24] offers the notion of zero-trust federation (ZTF), which integrates the zero-trust network approach to identity federation and demonstrates in what way ZTF maintains access requests. For a ZTF, authority is needed to share conditions between enterprises. By federating with Identity Provider (IdP) and Context Attribute Provider (CAP), each Relying Party (RP) can conduct access control based on a zero-trust approach. The identification and authentication of users, as well as distribution of policies related to authentication among organizations in the identity federation, is performed by the IdP. Whereas, the CAP gathers and manages a user's contexts, as well as provides context information to entities. The RP manages access by making use of IdP declarations and conditions from CAP. The connotations of conditions in ZTF regarding how to build policies and how to implement them are all unclear in the proposed concept. Such a model must consider a vast number of different circumstances to make accurate authorization decisions. However, an access control mechanism may not be able to gather enough context to make choices in other instances due to the conditions being assembled in single programs, and no centralized authority is available to regulate the policies.

According to [25], a system that combines micro-segmentation and the zero-trust model will be able to regulate access to a company's or industry's important assets. To put the collaboration into action, an approach called 'light verification' which refers to a method of reducing traffic inspection to a minimum is proposed by the authors. Micro-segmentation is a network strategy that generates safe zones to segregate and secure application workloads, both physical and virtual. Further investigation is needed on the proposed paradigm to reduce verification latency and hence reduce resource consumption. [19], on the other hand, investigated the round trip time, jitter, and packet loss of data center networks based on software-defined networking with a zero-trust security model, using micro-segmentation and measured using a testbed simulation of Cisco Application Centric Infrastructure. The findings of the performance evaluation demonstrate that micro-segmentation adds an average round trip time of 4 and 11 s of jitter without packet loss, allowing security to be increased without compromising network performance in the data center.

To meet the new security difficulties that come with cloud architecture, [26] suggests a zero-trust security paradigm for cloud computing environments. The fundamental purpose of a cloud-based ZTA is to secure a cloud service provider's (CSP) resource from successful data breaches. The proposed trust strategy will make it easier for CSPs and customers to select trustworthy organizations in the cloud. It provides both the cloud provider and the consumer with effective trust management benefits of cloud computing technology. Perhaps, mathematical modeling with precise details, correct formal languages, and the relevant technology platform can be pursued as future work. Alternatively, [27] introduces a zero-trust-based platform that implements numerous functional modules such as sensitivity analysis service, cipher index service, and attribute encryption service to satisfy the needs of users uploading sensitive data to untrusted third-party cloud platforms. As suggested by [28], considering an attribute-based encryption system, the generation of private keys for users should be carefully examined.

Meanwhile, [20] used Elastic Stack to create a modest zero-trust network architecture. Elastic Stack is the most popular open-source real-time data analysis system, and it has become the industry standard for log real-time processing. For users to log in, the model utilized fingerprint identification technology as an important credential. Authors claim that this model allows people to easily move confidential files and exchange information while maintaining anonymity and security. However, security experts have discovered a critical and wide-ranging application programming interface (API) vulnerability caused by Elastic Stack's erroneous implementation, which might put clients' businesses in danger [29]. [30] used trust degree calculation and dynamic access control to give a dependable and new idea solution for the security protection of Power Internet of Things (PIoT) terminals. Even though a framework based on zero trust is presented, the zero-trust security concept of continuous monitoring is only considered in the framework. Authors should consider implementing basic zero-trust tenets discussed in the (NIST, 2020) paper to achieve potential benefits of the concept.

[31] performed risk analysis in various levels of power mobile internet applications and presented a zero-trust-based security protection framework Figure 2 to provide logical identities to multiple individuals, devices, and applications by combining the two components of identity recognition and access control with finer granularity based on identity trust. Similarly, [22] proposed a risk-based access control enforcement system to address future security needs, specifically zero-trust networks. Researchers also specified the policy languages required to enable the framework, as well as the design and implementation of a firewall provisioning component. A runtime mechanism of the language introduced and its collaboration with an existing policy decision point (PDP) must be considered in the proposed work.

Furthermore, [32] presents a multi-cloud framework and a testing strategy for analyzing data plane performance under stress and the influence on the control plane when zero trust is facilitated. The results show that, depending on the service

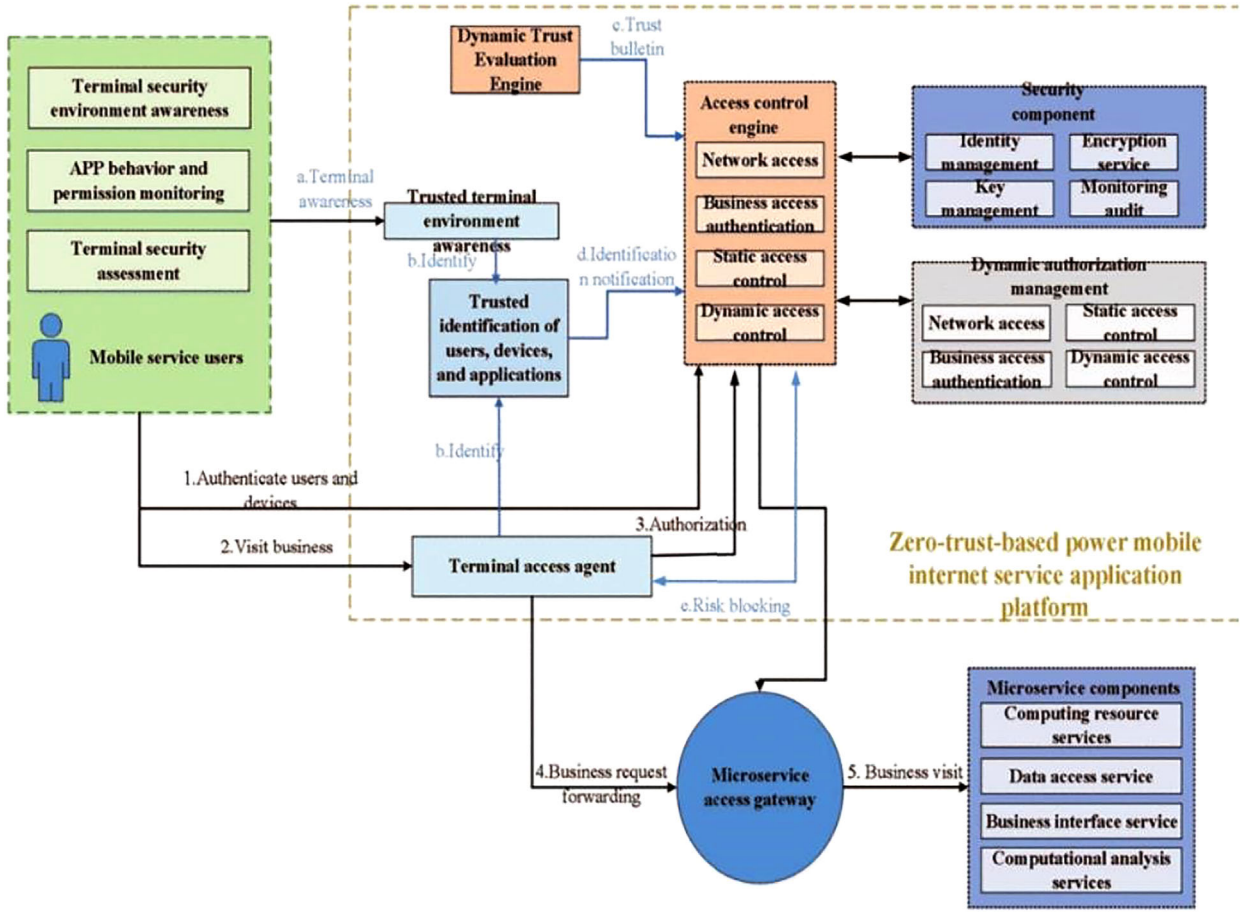


FIGURE 2 Zero-trust framework for power mobile internet business.

mesh setup and the cloud environment, overall CPU and memory use can increase. In addition, [18] discussed micro-segmentation by containerizing apps and utilizing Kubernetes to achieve it in a ZTA. Being open-source software, Kubernetes deployments are vulnerable to security flaws, such as the ones discovered at Tesla in 2018. Kubernetes security techniques can be systematized to help practitioners mitigate risks in their Kubernetes systems [33]. Likewise, [34] states that for the time being, zero-trust algorithms cannot be used for vehicular communications since the vehicles emit time-sensitive safety messages. Hence, zero-trust solutions will not be unable to authenticate messages in real time. Also, since vehicles will be moving, the network topology will become unstable. The domain of ZTA encompasses the removal of various elements of trust [35].

2.3 | Blockchain applications in banks

Since 2011, blockchain technology is serving the world across various sectors and business applications. Technically, a blockchain is a collection of distributed records stored in every distributed node of the system [36]. Each node has the same rights and obligations, and all participating nodes share the same data. In traditional transactions, a central authority controls the transaction process. In contrast to this approach, transactions take place in a blockchain system without a central authority. Hence, the blockchain system follows a decentralized process that includes cryptographically signed blocks being added to the chain of nodes after verifying by the existing nodes. Blocks will be added only after the verification and based on the consensus agreement. This makes data tampering a tedious task since newly created blocks will be shared among every node that is participating in the system. This makes the system more trustworthy and secure. As shown in Figure 3, a hash of previous block data is added to every new block added to the chain [37]. Tampering of a block results in a different hash appearing in the subsequent blocks [38]. Thus, alterations to data can be identified and eliminated.

According to [39], adopting blockchain-based banking will help to reduce payment processing time and transaction fees, which are considered to be major drawbacks of the traditional banking system. Various publications are released suggesting the implementation of blockchain technology into the banking sector. [40] introduced a blockchain-based system that stores and transmits bank transaction data and removes the need for a third-party storage system used in traditional banks. The proposed Hyperledger blockchain system uses a consensus

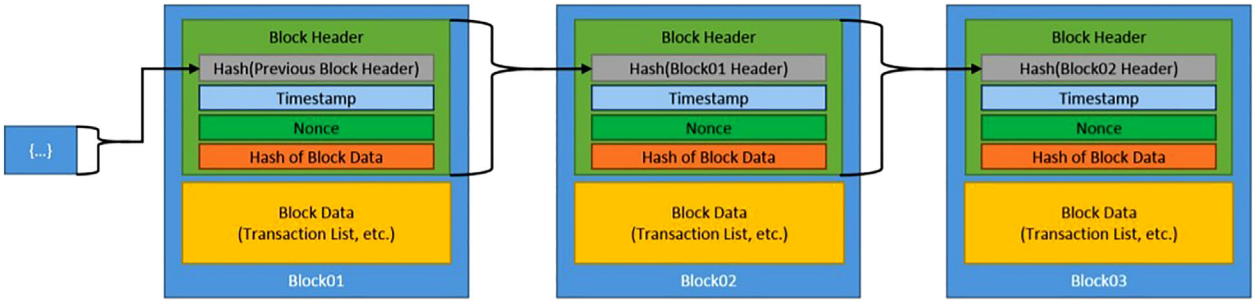


FIGURE 3 Blockchain architecture and structure.

mechanism that acts as a trusted foundation for transaction data maintained on the blockchain. Transaction between banks in the proposed system will be executed with the help of smart contracts. The proposed system will help banks to conduct transactions without the need for an intermediary authority and with reduced transaction charges.

The consensus algorithm is the core technology in blockchain, which describes how peers in the network achieve data consistency and directly determines the overall efficiency of the blockchain system. [41] provides an overview of existing consensus algorithms and categorizes them into three groups: consensus algorithm based on certain attribute value proof of peers, consensus algorithm based on peer voting mechanism, and Paxos class consensus algorithm. The paper also offers an in-depth analysis of the implementation details of these three types of algorithms, conducts a comparative research based on Mundell's impossible triangle theory, and suggests possible future development direction for consensus algorithm. These include: (1) modifying the logical structure of the block, such as using a directed acyclic graph; (2) using the idea of division and autonomy to fragment the blockchain network, reducing communication scale, and increasing consensus speed; (3) using a hybrid consensus algorithm that combines proof consensus algorithms with byzantine fault tolerance (BFT) technology, such as using node credit attributes to elect nodes and integrating credit mechanisms and artificial intelligence algorithms.

[42] introduces a novel blockchain consensus algorithm that operates by first selecting a function to preserve the randomness of input variables, then generating a random number for each node participating in the consensus calculation. These random numbers are then used as variables in the function to calculate a value and a node is chosen as the accounting node based on the highest correlation between the random number and the function value. The algorithm allows for a random selection of the blockchain's accounting node. The consensus algorithm's performance has a direct impact on the distributed system's overall performance, such as security, robustness, cost, and efficiency. Improving efficiency while maintaining security and robustness is a crucial topic that requires ongoing research and discussion.

The majority of current consensus algorithms rely on a leader node to propose new blocks and communicate with other nodes. This makes the leader node a prime target for malicious attacks. Additionally, as the number of nodes increases, the blockchain system's scalability and throughput become inadequate. To address these issues, the AnonymousFox consensus algorithm [43] is proposed for use in a consortium and private blockchains. It starts by designing an anonymous leader node sorting algorithm that obscures the leader node's identity through various encryption methods and periodically changes the ordered leader list to conceal the target from malicious attackers. Furthermore, it designs a consensus algorithm based on anonymous leader node identities that reduces the number of messages through one-to-many communication and has a complexity of O(n) which solves the problem of ordered replication of state machines when the leader node is anonymous. The algorithm is analyzed and it ensures safety and liveness when the fault nodes are less than one-third of the total. The performance of the algorithm is evaluated through experiments on throughput, latency, scalability, resource consumption, exception processing, smart contracts, and blockchain network [44]. In comparison to the practical byzantine fault tolerance (PBFT) algorithm, AnonymousFox has a higher performance and scalability. The study however does not investigate the impact of sharding technology on the algorithm and improve its scalability by addressing the CPU and bandwidth resources of the leader node.

[45] focuses on the use of blockchain technology in the identification of digital products in the information industry. It is crucial to pay attention to the information security of these digital products, which has become a significant issue in modern society. To address this issue, the author proposes a combination of current blockchain technology and the expansion of the blockchain protocol for digital products in the information industry. This is achieved by defining and distributing smart contracts, and designing a blockchain protocol and expansion system for the digital products of the smart contract information industry. Authors also analyzes blockchain technology in detail and proposes an effective combination of blockchain protocol extension and blockchain for digital products in the information industry. It uses blockchain technology to extract key information from the information industry data and integrate it into the construction process of the blockchain. Authors also draws on the development process of the blockchain consensus algorithm and defines the address of each part of the blockchain to ensure that valid information can be completely

extracted and irreplaceable. This research has a certain guiding role for developing the use of blockchain technology in the information industry in the future.

[46] proposes a new consensus algorithm using Proof of Majority (PoM) to address the issue of centralization in blockchain networks caused by energy-intensive mining pools. The proposed algorithm aims to increase decentralization and reduce the carbon footprint by eliminating resource-intensive tasks. The algorithm has been evaluated for its latency and throughput and has been found to outperform popular existing consensus algorithms. The initial results from the proof of concept suggest higher throughput, increased decentralization, and reduced barriers to entry compared to blockchains using Proof of Work or Proof of Stake algorithms. The future scope of this work includes implementing and deploying additional nodes across various geographical locations to achieve near real-time performance and exploring the use of PoM in other domains. However, the PoM consensus algorithm puts a significant network load when nodes are more than 20, future work will consider the network architecture by creating a group of nodes that conducts elections to decide the leader, significantly decreasing the network payload. Multiple levels of leaders can be used to make their decision based on the majority of inputs received from nodes.

Incorrectly selecting a consensus algorithm for a private blockchain can lead to low efficiency, waste of energy, unfairness, and more. As businesses are increasingly looking to integrate blockchain into their systems, there is a growing demand for selecting consensus algorithms that are suitable for private chains. Most current consensus algorithms are either voting-based or PBFT-based, but voting-based algorithms may suffer from leader crashes, while PBFT-based algorithms may experience network congestion when implemented in large networks due to their broadcast-like confirmation steps. [47] proposes a new type of consensus algorithm based solely on random number generation, called Mosaic. The selection is not only due to its low computational cost compared to cryptographically proof-based algorithms, but also because of its acceptable unpredictability that makes the election fairer. The evaluation demonstrates that Mosaic is more efficient than PBFT-based schemes in large scale while also providing fault tolerance compared to Raft. Mosaic algorithm has better performance and scalability compared to PBFT, and though it poses more overhead compared to Raft, the complexity of reaching consensus is linear towards the network size.

[48] examines the proof-of-work (POW) and POS algorithms in the context of blockchain consensus mechanisms, analyzing the advantages and existing problems of these two mechanisms. Authors also discusses important issues related to safety and performance, and provides researchers with a comprehensive reference on blockchain consensus mechanisms. As the consensus algorithm is the core technology of blockchain and has many influencing factors, the paper discusses current problems and proposes potential improvements. The paper also presents some typical algorithms for a more systematic introduction. As blockchain technology continues to integrate with real industries, the consensus algorithm is crucial for achieving consistency of results in a network environment where nodes are highly dispersed and there is no mutual trust mechanism. The choice of a consensus algorithm is a balance between efficiency, security, and stability, with specific application scenarios taken into account.

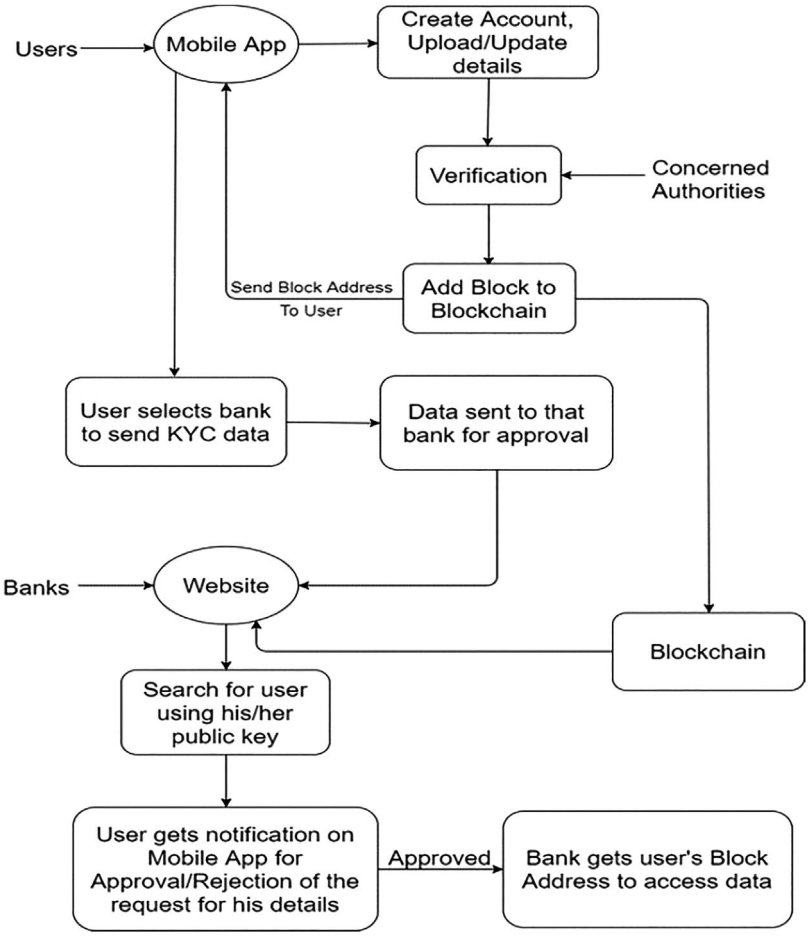
In addition, [49] established a blockchain-based 'Know Your Customer (KYC)' processing which claims to minimize the processing cost for financial institutions and minimal time consumption for the processing to help with customer satisfaction. The major advantage of the proposed solution is the entire verification procedure is managed at one time for every individual. The solution also provides transparency as the verification process is shared with the consumer using distributed ledger technology. This model ensures customer satisfaction, reduced expenses associated with processing as well as openness. The KYC process used in the paper is illustrated in Figure 4. A similar study presented by [50] discusses the application of blockchain to KYC outcome distribution among various banks. If any security breach happened in the proposed model, sensitive data might get leaked as customer data as well as documents are stored in the blockchain itself.

Furthermore, [51] instigates a blockchain-based self-sovereign identity framework to secure KYC processes by keeping up with data protection regulations as well as consumer privacy. The proposed framework does not store any customer data in the blockchain. Authors claim that all the sensitive data of users can be stored individually without relying on a third party. Data, when requested by the bank for processing any transaction, will only be shared by the customer from their digital wallet if they intend to do so. Data manipulation by the internal factors in a bank can thus be prevented using this method. Since the self-sovereign identity concept is still in its infancy, the implementation of this proposed framework still needs time and work. The proposed framework is shown in Figure 5.

Meanwhile, [52] discuss the benefits of introducing blockchain technology into the banking sector. The authors state that blockchain-based transactions will have 24×7 availability, openness, minimum transaction charges, and on-chain settlement. Also, alterations to the blocks can be traced ensuring the security of transactions. This will prevent fraudulent activities and scams to a greater extent [53]. Another benefit of banks is to guarantee the adoption of regulatory compliance in an efficient manner. Blockchain algorithms will enhance regulatory compliance by consolidating market interests and security practices. This will prevent malicious communications and enhance data protection [54].

In addition, [55] examines employing banks as participants when considering a blockchain platform. Authors claim that using such a system will help banks quickly identify and authenticate the debtor. Also, all the participants in the blockchain, banks in this case, will have to agree to approve loan applications. Implementing smart contracts will help loan regulations by reporting on time which will help banks to decide if multiple loan requests are made or not and act accordingly. Such a system will help banks to review the records of loans associated with every customer. With all these advantages, the confidence level

FIGURE 4 KYC process verification.



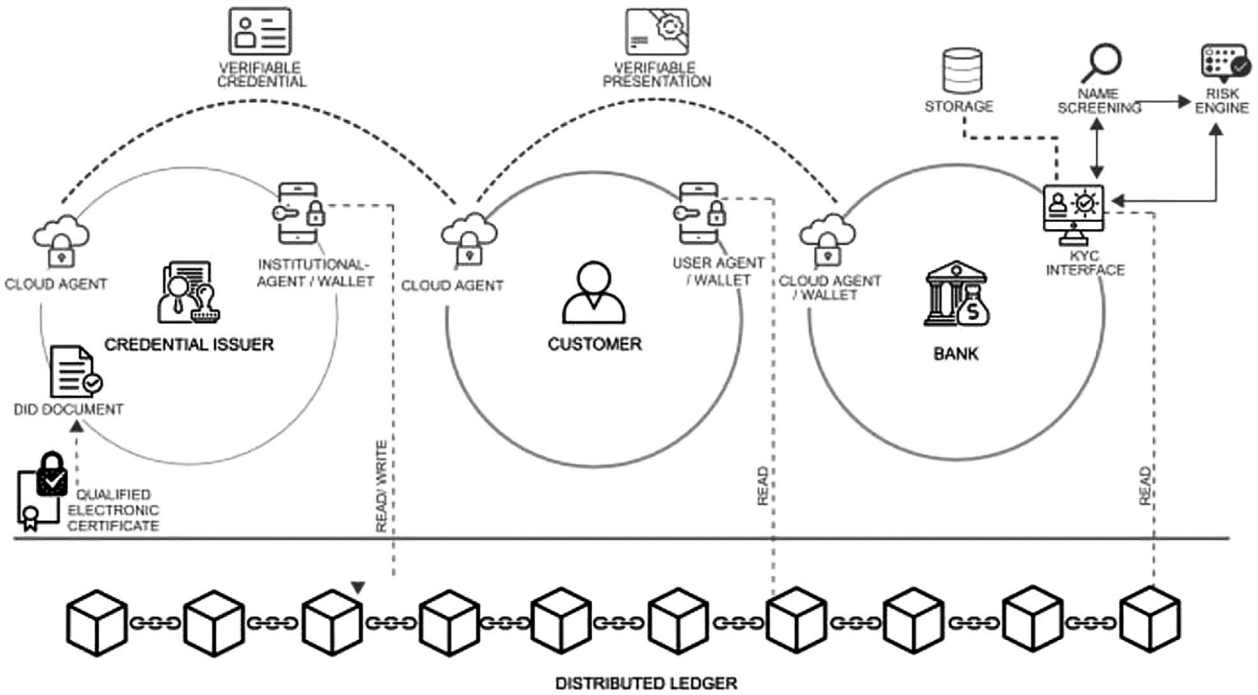


FIGURE 5 Blockchain-based SSI framework for KYC processes.

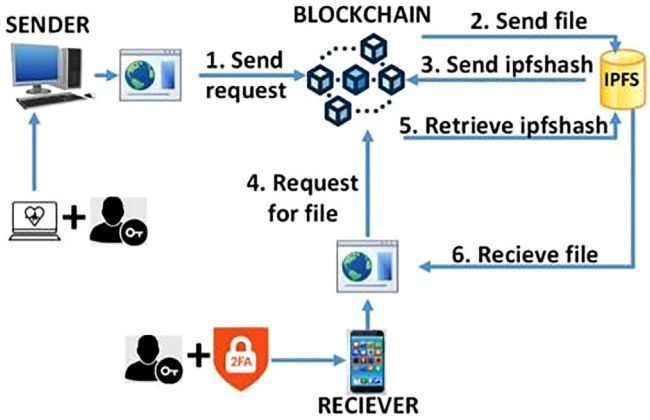


FIGURE 6 Zero trust and blockchain integration.

of investors will increase, and this will help banks to improve their transparency, and build the trust of stakeholders.

On the contrary cost saving as the key benefit of blockchain implementation, categorize the implementation and maintenance cost of blockchain in banks as three elements: cost of the transaction, cost of power, and cost of storage. With the high energy consumption and increase in the need for storage with increased transactions, transaction charges will also increase [56]. [57] examines the constraints faced by the banking industry to adopt blockchain technology as the insufficient technical parameters of technology compliance with the needs of participants in the financial sector of the economy. Also, excessive openness of transactions in the digital environment inhibits the conclusion of high-risk transactions or the intervention of third parties with malicious intentions.

2.4 | Integration of zero trust and blockchain

The integration of blockchain technology and the zero-trust approach is yet to bloom which will make tremendous advancements in the field of security. [35] proposed a blockchain-based zero-trust model to share medical images between patients and doctors. In the proposed model, blockchain is used for transparency and accuracy of data while zero trust is for user authentication. The image being shared is encrypted using a cryptographic algorithm and stored in the interplanetary file system (IPFS) database. IPFS ensures the security of shared files being encrypted with an asymmetric algorithm and thus data integrity is maintained. The model of the proposed system is illustrated in Figure 6.

The proposed consensus algorithm [7] utilizes a zero-trust model, where each node is responsible for verifying and approving transactions before they are committed to the network. This ensures data security as data owners can track their data as it is shared among various data custodians. The algorithm is a hybrid of Proof of Work and Proof of Elapsed Time, and uses rivest-shamir-adleman (RSA) for authentication and authorization. The proposed algorithm is demonstrated in the context of a college placement system, where it is used to create a diversified, decentralized, and automated system. The future research possibilities include maintaining network security through cryptography and extending the proposed model to other industries such as banking and healthcare.

[58] presents a novel solution for information sharing in zero-trust Internet of Things (IoT) environments using blockchain technology. The proposed solution guarantees anonymity while ensuring entity authentication, preserves data privacy while ensuring data trustworthiness, and promotes participant participation while maintaining fairness. Smart contracts are used to filter fabricated information, effective voting and consensus mechanisms are used to prevent unauthenticated participants from sharing inaccurate information. The security of the proposed solution is proven in the universal composability framework and its performance is evaluated using an ethereum based platforms (ETH)-based platform to demonstrate its effectiveness.

[59] proposes a Blockchain-Based, Zero-Trust Security-Enabled Federated Learning system called 'Skunk' to address privacy and data provenance requirements in 5G/6G mobile networks. The proposed system uses a sharding-based architecture in the blockchain to enable deployment in network slicing environments. It also utilizes zero-trust security mechanisms to ensure security and transparency in the federated learning process. As a use case, we have considered a scenario where IoT device attacks are detected in a 5G/6G network. The proposed system is designed to address the challenges of centralized coordinator-based federated learning systems and support deployment in 5G/6G network slicing environments.

[60] proposes a Blockchain-enabled Intrusion Detection and Prevention System (BIDPS) that aims to augment ZTA onto endpoints to effectively deter Advanced Persistent Threats (APT) attack capabilities. The BIDPS aims to detect and prevent attackers' techniques and tactics earlier than the lateral movement stage, strip trust out of the endpoint itself, and create an immutable system of explicit trust on the blockchain. The effectiveness of the BIDPS was evaluated using a testbed where various APT attacks were launched against the endpoint and found to have a high success rate in defending against the attacks. It uses a whitelisting approach, where it only allows authorized system files to run, blocking any unauthorized activity and triggering an alert. The system was tested and showed a high success rate in detecting and preventing APT tactics and techniques.

[61] aims to address the security issues surrounding the use of JSON Web Tokens (JWT) in One Time Token (OTT) enrollment for zero-trust networking (ZTN) by incorporating the JWT as encrypted metadata into a Non-Fungible Token (NFT) on a blockchain. By using the blockchain public key of the intended owner for encrypting the JWT and mapping it to the owner's blockchain address, we can assure the ownership of the OTT and prevent impersonation. This mechanism is applied to an existing ZTN framework, OpenZiti, and a permissioned Ethereum blockchain, Hyperledger Besu. In the future, we plan to enhance the system by implementing real-time monitoring and analysis of the zero-trust

network resources for more advanced smart control of access policies.

In addition, [62] examines how the zero-trust concept can collaborate with blockchain technology. As a part of the study, the authors propose a zero-trust model augmented with blockchain-based intrusion detection systems for every endpoint in the network. A blockchain-based intrusion detection systems (IDS) will ensure the integrity of access logs and data stored in the blocks. Such systems will have efficient trust management since both approaches work in a decentralized and borderless environment. However, the duplication of data in every node in the blockchain helps the overall security of data.

According to [63], the immutability of a blockchain can help safeguard the implementation of a zero-trust policy. [64] recommends using blockchain technology in ZTA for the following purposes:

- Online fraudulent detection in transactions.
- Connectivity isolations.

The user's access is restricted until the transactions are approved by an IT security team member.

Financial institutions are subjected to a daily bombardment of cyberattacks that can result in the loss of data, money, and trust, and as digital banking grows, they are becoming more vulnerable [9]. ZTA is a cyber security approach that can be adopted by an organization incorporating zero-trust principles and includes integral communications, productivity devising, and access management. Based on a zero-trust architectural scheme, a combination of physically connected infrastructure as well as a virtual network along with company policies comprises a zero-trust venture. Adopting a zero-trust approach will help banks to mitigate data breaches and financial loss. Adopting a blockchain implementation to the zero-trust approach will enhance banks' security and will help them to meet regulatory compliance requirements. Furthermore, hardly any work that discusses adopting a zero-trust-based blockchain model in the banking sector exists. This made the researcher conduct a study that addresses the bank security issues using the proposed model. The following section discusses the methodologies adopted to conduct the study.

3 | METHODOLOGY AND DATA ANALYSIS

This study focuses on the theoretical aspects of a blockchain-based zero-trust security paradigm in banks, but no system deployment is planned as of now. Qualitative research methods were used to find a solution to the research question in this study. which was intended to gain a thorough understanding of the key concepts of the technical terms used in this study. As a part of the qualitative study, digital platforms including IEEE Xplore, Google Scholar, Science Direct, ACM digital library, and ResearchGate were explored for data collection. A qualitative study on a case study of a recent cyberattack on banks was also considered. However, a detailed report on cyberattacks faced by banks was not available to the public. Hence, a case study of 'Bangladesh Bank Heist' that took place in 2016 was conducted to investigate the cyberattack scenario on banks. Case studies on cyberattacks on Bangladeshi banks were only available online, even though cybercriminals are targeting banks on regular basis across the world. Following an attack in November 2017, seven of the United Kingdom's largest banks had to limit operations or shut down entire systems. This proves the claim by [11] about financial crimes going unnoticed by the public because bank executives do not want to upset their shareholders. Executives are frightened of exposing their firm to fresh attacks, afraid of sullying its reputation as a reliable storage medium and, as a result, losing clients.

The research problem in the selected field was identified through recent research papers, TEDx talks, podcast interviews, etc. From this, the gap of study on the integration of blockchain and zero trust in the banking sector was identified. To design the framework, ideas, and concepts from (NIST, 2020) ZTA, and blockchain platform from [65] were considered. Development and testing of the feasibility of the framework were performed iteratively. An outcome evaluation was done to determine how the solution to the research question was achieved. Finally, a summative evaluation was performed to reflect on the entire project performance and to determine if the future goals of the project need to be considered for complete research.

3.1 | NIST zero-trust model

The conceptual model of a user requesting a connection to the bank server is presented in Figure 7. A PDP and a policy enforcement point (PEP) decide in combination whether to provide access (NIST, 2020). The authenticity of the request and the device trying to get connected to the resources must be verified by this system. The PDP/PEP makes the appropriate decision to allow the user to establish a connection to the server. The two key areas of the zero-trust concept, authentication, and authorization are thus validated. Sensitive resources should have PDP/PEP close to their perimeter to allow an implicit trust zone keeping its range as minimal as possible. This is because the trust zone beyond PEP/PDP is considered trustworthy.

Every component mentioned is considered a resource of equal importance. Communication within the internal network, as well as an outer network, is considered as the same trust level. Once access is granted to a resource, lateral movement within the same network is not permissible. Authentication and authorization should be verified for every access on a session basis. Users including clients, employees, and third-party contractors are verified equally in the system. Access to the resources is granted upon multi-factor authentication [66], device health check, location, etc. In addition, a system to monitor (Continuous Diagnostics and Monitoring) the devices owned by the organization for any kind of compromise or vulnerabilities should be maintained.

The core logical components of an national institute of standards and technology (NIST) architecture are shown in Figure 8. The PDP has two core components, policy admin-

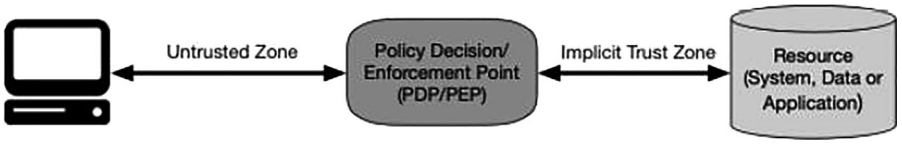


FIGURE 7 Zero-trust access.

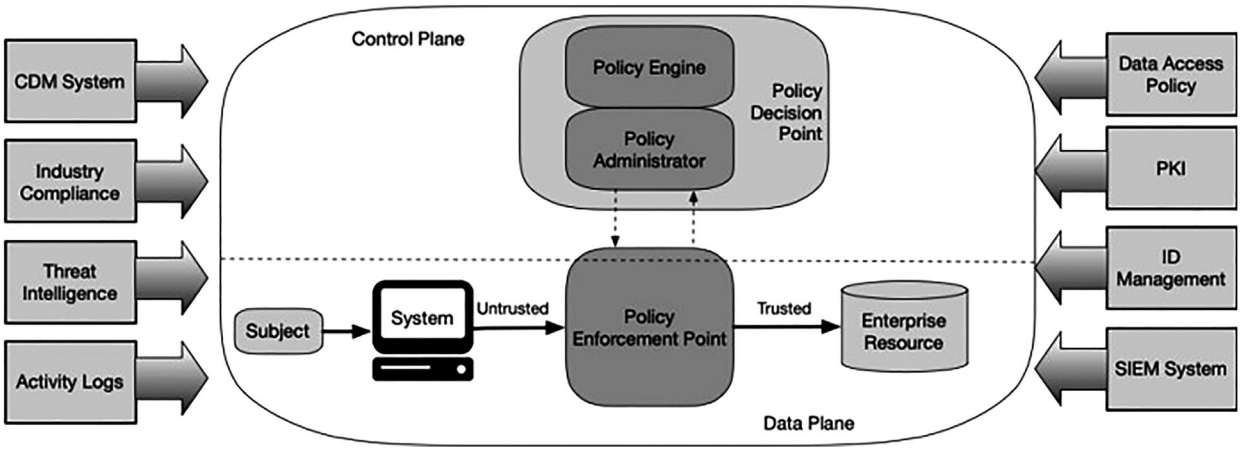


FIGURE 8 Core zero-trust logical components.

istrator (PA) and policy engine (PE). The ultimate decision to grant access is determined by PE. To establish the decision, inputs from components like CDM, SIEM, etc. are collected to calculate a trust algorithm. Once the decision is made, PE handover the decision to PA to execute it. The decision received from PE makes PA communicate with PEP to allow or terminate the communication from user to resources based on the decision. If PE grants access, PA communicates with PEP to permit access. Else, PA composes PEP to terminate the communication.

In addition to the PEP/PDP, a few other components in conjunction are used for security evaluation purposes. They are:

- Continuous diagnostics and mitigation (CDM) systems take care of the device health of company assets by applying regular updates and patches. When an access request is generated, CDM informs PE about the device condition, if the software used in the system is outdated or vulnerable if any irregularities are identified with the device, etc. Devices that do not belong to banks, or that belong to customers or third-party contractors are controlled by CDM imposing relevant security control policies.
- The industry compliance system (ICS) encourages banks to comply with industry-related compliances. The system comprises processes, controls, documentation, etc. to make compliance easy for an organization. Risk management can be implemented effectively with the use of an IDS. By monitoring ICS, the company can evaluate the security practices followed by their users and educate them if any failure to adhere to compliance is noticed. This will ensure cyber awareness among users.
- Data access policies (DAP) store the access control policies generated by the policy engine. The policies associated with accessing resources are encoded in this system. When an access request is notified, the policy engine communicates with DAP to determine the access privileges and policies related to the access request. Each policy is made about the business requirement.
- Access logs on the other hand keep a record of every resource access and activity logs and network traffic happening in the cloud premises as well as company premises. Logs are maintained across every resource to ensure if any security incident happens, traces can be made use of to analyze the activities.
- Threat intelligence feed (TIF) gathers threat data from internal as well as external resources to notify the policy engine regarding the access request decision.
- Public key infrastructure (PKI) takes control of the producing certificates to distribute among the assets and resources in banks.
- ID management system (IDMS) is responsible for establishing, maintaining, and managing user accounts and data. The key information regarding a user is stored in this system. It also communicates with PKI to services required for account users.

Security information and event management (SIEM) gathers security-related data for future examinations and helps in

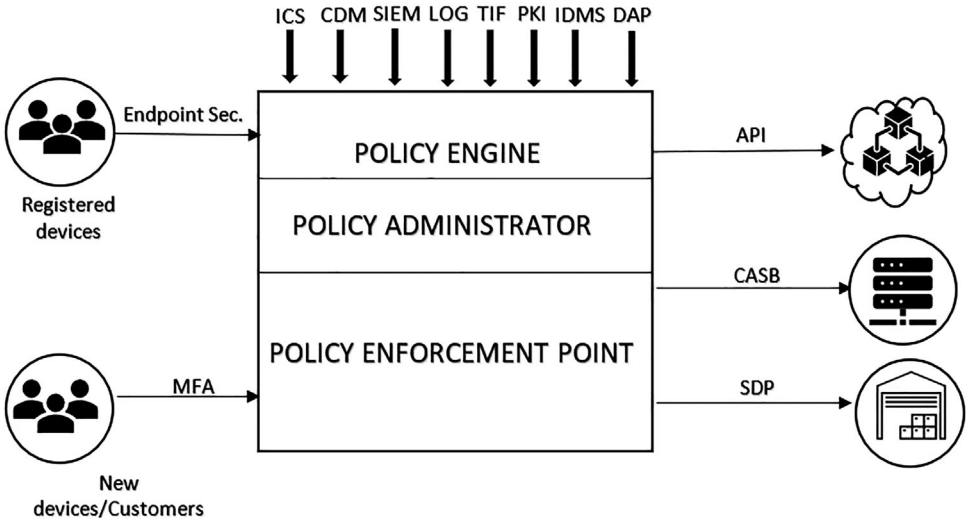


FIGURE 9 The proposed framework.

policy revising. It also notifies the enterprise of any possibility of attacks.

3.2 | Blockchain mechanism in the proposed model

Considering the security of banks, online payment transactions must be scrutinized as well. A consensus mechanism consolidating the algorithms like Proof of Work and Proof of Elapsed Time (PoET) is used in this proposed transaction method [7]. When a customer requests a transaction, the PoW algorithm is used by the customer node to execute the transaction request and a block is created. To this block, an associated variable is added as the structure of the proof. It is the duty of both customer's bank and the recipient's bank to verify the customer node's computational function to verify the transaction request. Only upon verification by both nodes, the block will be added to the blockchain, else it will be rejected. Thus, the request generated by the customer node is authenticated by the customer bank and recipient bank. By using a PoET consensus mechanism, the chance for increased resolution consumption and power of computing resources can be eliminated. Verifying timestamps using PoET will help to mitigate the damage caused by man-in-the-middle attacks. The malicious attempts from foreign intruders to alter the block will be prevented by recording the timestamp and this will be corroborated by each participant in the blockchain. If the verification phase is taking longer, the chance for block tampering can be expected and the block is eliminated. The block issued by the customer node will be sent over to the customer bank node who will verify the timestamp to check if the verification by the customer took the allowed time spell or not. Only upon confirming that, the customer bank will check the database to confirm if the customer has already updated all the required data to prove his identity. If the identity of the customer is verified, then checking for confirming enough balance will be performed using smart contracts. If successful, the block will be transferred to the recipient's bank. The recipient's bank will verify the block by again checking the timestamp. The data is also verified by the node to confirm the identity of the recipient and the authenticity of the transaction. If verification by the recipient's bank is successful, the node will sign the block and communicate with the customer's bank to approve the transaction.

3.3 | Zero-trust integration with blockchain technology

The concepts of zero-trust principles and blockchain technology are integrated to propose the model as shown in Figure 9. The blockchain consensus mechanism used in this model ensures decentralization and immutability of transactions holding the zero-trust principle 'never trust, always verify', while zero-trust principles are used for access control and authorization [7, 35]. Considering the cases of online banking transactions between customers and bank servers, the functionalities of the proposed model are illustrated in Figure 10. In the proposed framework, the same level of trust is applied to the clients, employees, and third parties. When a user tries to connect to the web server, if access is requested from a registered device, the endpoint security configuration on the device authenticates the user along with login credentials. If the access request is generated from a new device, multi-factor authentication [67] is required to verify the user. This comprises the first layer of security. Authentication of clients also requires multi-factor authentication to gain access to the services.

Upon the first level of authentication, the request reaches a policy engine that determines if the access needs to be allowed or not. A trust algorithm is working in this engine to calculate the trust level. Based on the information gathered from the policy database, continuous diagnostics, mitigation system, and

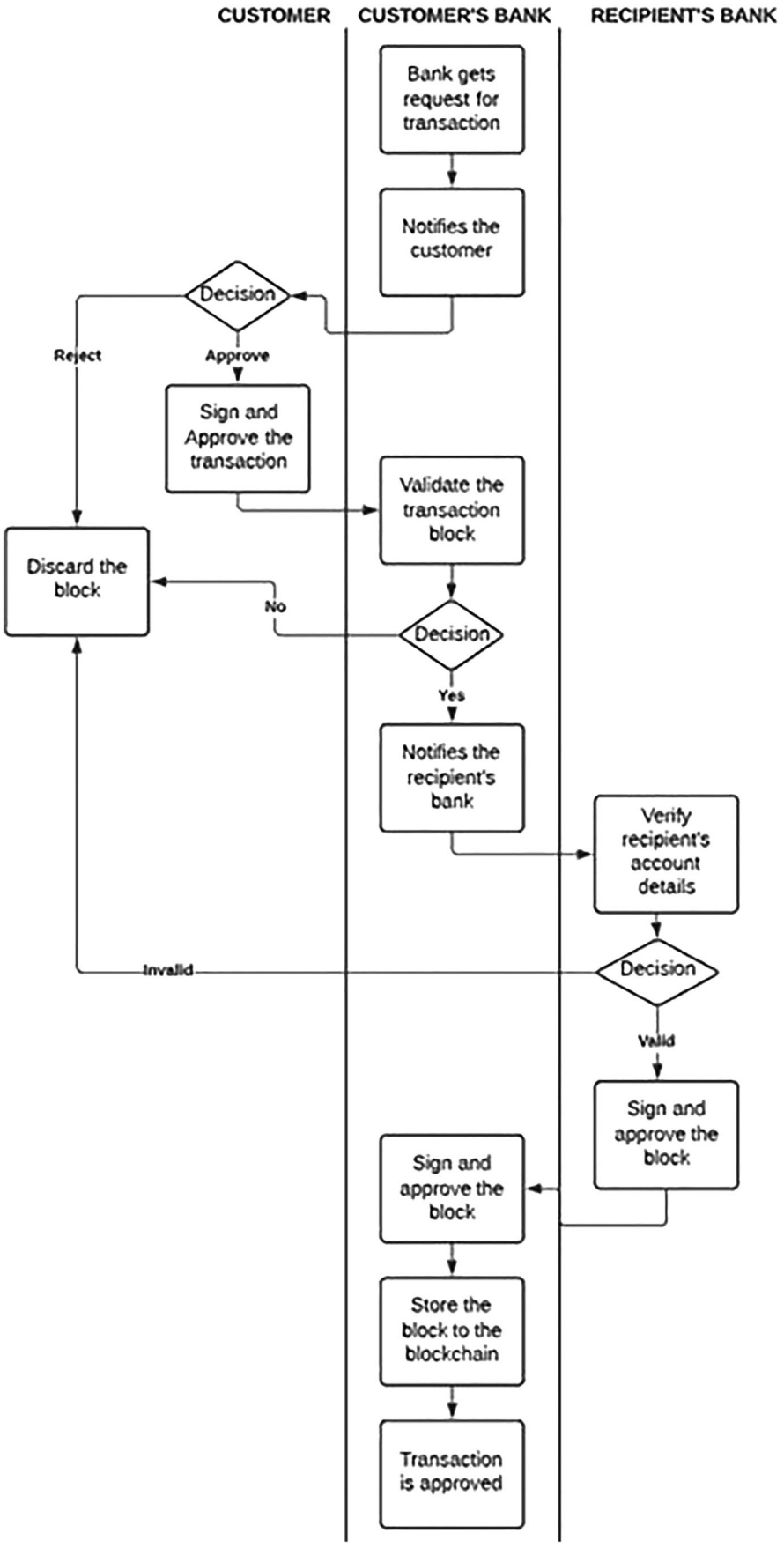


FIGURE 10 Proposed zero-trust-based blockchain transaction flowchart.

```
Algorithm USER REGISTRATION
START
    Initialize Block-Chain.
    USER
        Requests System Registration
        Successfully completes registration
        Creates Cypher
            Encrypts Data using Private Key
            Signs Data using RSA
        Adds Cypher to Block
        Saves Block into buffer
        Requests Bank to initiate verification
    BANK
        Extracts Block from Buffer
        Initiates De-cyphering
            Decrypts Data using Public Key
            Verifies digital signature
        Re-cyphers Data using Private Key
        Adds Cypher to Block
        Saves Block into Block-chain
END
```

FIGURE 11 User registration algorithm.

```
Algorithm INITIALIZATION PHASE
START
    Initialize Block-Chain.
        Add Genesis Block to the chain
        Initialize Bank Node
            Generate Private and Public Keys for the bank.
            Store Bank node keys in Database
        Initialize Customer Node
            Generate Private and Public Keys for the customer.
            Store Customer node keys in Database
        Initialize Recipient Node
            Generate Private and Public Keys for recipient bank.
            Store Recipient Bank node keys in Database
END
```

FIGURE 12 Initialization phase algorithm.

threat intelligence services, the decision on the access request is determined. The trust algorithm reports the change in the behaviour of access. For instance, if an access request is made at night or on weekends, the system considers it a suspicious activity. Thus, the policy engine calculates the trust level based on the access and grants access accordingly.

PE informs PA about the decision. PA shares this information with PEP via a control plane. If PE permits the access, PEP allows the user to access the requested service. Else, the connection is terminated. Access to a single service does not guarantee lateral movement within the network. Every session will terminate within a specified time. Assets of banks including hardware, software, cloud deployments, and every sensitive resource are secured with security devices and controls. All communications must be encrypted to mitigate man-in-the-middle attacks. Data stored should be classified, labeled, and encrypted [68].

The key elements of the bank transaction model Figure 10 proposed here are the customer node, customer's bank node, and recipient's bank node. The algorithm used for registering a user to the bank system using blockchain is shown in Figure 11. When a customer requests a transaction, a notification is sent to the customer's registered device to verify the identity of the customer. If the request is rejected by the customer, the transaction request is aborted and recorded in the database. If the request is verified by the customer, a block is created which contains the transaction details entered by the customer including customer account number, amount to be transferred and recipient account details along with the timestamp of the verification time. A PoW algorithm is executed on this block. The data is then encrypted using the public key of the customer's bank node to ensure the confidentiality of the transaction. The customer's private key is used to generate a signature. This signature and data encrypted are added to the block and saved in the buffer. The customer node then notifies the bank's node about the progress.

Now the customer's bank node retrieves the block from the buffer. The encrypted data from the block is decrypted utilizing its private key and the signature of the customer is verified with the customer's public key. The bank's node then checks its database to verify the identity of the customer and to confirm if enough balance is available in the customer's account. If verification fails, the block is discarded, and the customer node will be notified of the transaction failure. If successful, the PoW performed on the block is validated by the bank node. This PoET algorithm is executed on the block along with the timestamp of the bank node's verification. The block data is encrypted utilizing the public key of the recipient bank node and uses its private key to generate a signature. Now this block is added to the buffer and notifies the customer node about the successful verification of the bank. Simultaneously, the recipient bank is also notified by the sender's bank about the transaction.

Upon getting the notification from the sender's bank, the recipient's bank retrieves the block from the buffer. The data in the block is decrypted by the recipient bank utilizing its private key and confirms the sender bank's signature using its public key. The node then confirms the identity of the recipient and confirms the transaction is genuine or not. If verification fails, the block is discarded, and subsequent nodes will be notified. If successful, the validation of the PoW algorithm is performed by the recipient bank node and executes the PoET algorithm on the block. The verification timestamp is then added to the block and data encryption will be performed utilizing the customer bank's public key. Subsequently, a signature is generated with the recipient bank's private key. The data along with the signature is added to the block and saved to the buffer. Upon verification, the customer bank is notified about the successful verification.

Algorithm TRANSACTION

START
Bank
Receives transaction request.
Asks Customer to verify.
if (Verification = True) ***then***
Customer
Creates new block executing PoW
Encrypts and digitally signs using RSA
Adds to block and stores to buffer
Customer's Bank
Retrieves block from buffer
Decrypts customer's Data
Verifies and Validates Block
Verifies identity and bank balance
Encrypts data and sign it using RSA
Adds cypher to block
Stores block in buffer
Recipient's Bank
Extracts data from buffer.
Decrypts Data
Verifies and Validates Block
Verifies identity and validates transaction
Encrypts data and sign it using RSA
Adds cypher to block
Stores block in buffer
Customer's Bank
Decrypts Data
Verifies and Validates Block
Encrypts data and sign it using RSA
Adds cypher to block
Stores block in Block-chain
Mark transaction approved
else
Discard block
END

FIGURE 13 Transaction algorithm.

Once the verification is obtained from the recipient's bank, the customer bank will decrypt the block data using the recipient bank's public key and a PoET algorithm is again performed to verify the block. If successful, the data is encrypted, and the signature is generated using its private key and stored the block in the blockchain. Thus, the transaction is approved by the customer's bank and both the customer node and the recipient node are notified about the transaction. If verification fails, the block is discarded. The algorithms used in the transaction phase is shown in Figures 12 and 13.

This proposed algorithm ensures the confidentiality of the transaction and builds trust among the sender, sender's bank, and recipient's bank. The data transferred by the customer is stored in a blockchain which helps the customer to keep track of their data. Each node participating in the transaction is trusted before the consensus is agreed upon and the transaction is approved. The data is stored and secured using blockchain which ensures immutability and decentralization. The PoW algorithm used by the participants performs a computational task in the block which is used by the other participants to verify the same. Whereas the PoET is used by the participants to verify the timestamp of verification and decide if any intruders are acting in between the transaction [7].

The proposed framework Figure 9 and algorithm Figure 10 can be implemented in a bank to ensure that insider threats, as well as threats related to fraudulent transactions, are addressed. Thus, the overall security of a bank can be enhanced by integrating a zero-trust security model and blockchain technology into the security practices. Thus, the research question is answered. The following section concludes the findings of this research and discuss the future works related to the study.

4 | CONCLUSIONS

The study aimed at providing a framework that would assist banks in securing their data and transactions. To propose the framework, key concepts of the (NIST, 2020) [69] zero-trust model and blockchain consensus mechanisms were used. In addition to the framework, a transaction algorithm, and a flowchart to provide a detailed understanding of the zero-trust-based consensus mechanism was provided. The suggested model is based on the zero-trust concept, which assigns the same level of trust to every entity in the network.

The major advantage of the proposed model is key important assets and factors in the banking industry are considered while designing the framework. Users accessing from inside the company premises as well as outside are treated with the same trust value. The case study conducted as a part of this research has proven that actors inside the company team can also cause harm to the company data and resources both intentionally and unintentionally. Having strong access control policies in place will help organizations to protect themselves to a great extent. This model discusses that following a zero-trust approach will help financial institutions from compromised assets as well as data leaks, whereas having a blockchain technology for transactions will help banks to secure the transaction processes making it tamper resistant and decentralized. The use of a consensus mechanism ensures the reliability of the system maintaining the trust among every participant in the network. However, the transition from a traditional security model to a zero-trust model is time consuming and proper planning should be implemented to enforce security. The key challenge faced in the study is to integrate the zero-trust concept and blockchain technology as adequate resources were not available to experiment with the integration. But due to the rapid increase in cyberattacks and the immutable nature of blockchain, institutions like banks will start thinking out of the box to achieve maximum security. The security of banks can be improved by implementing the proposed concepts of the zero-trust approach and blockchain consensus mechanism. The decentralization of transaction data and its immutability can be obtained utilizing blockchain technology. Whereas, the zero-trust concept will help the bank to secure its assets from intentional or unintentional malicious activity caused by insiders or foreigners. The consensus mechanism used in the proposed transaction model ensures trust among every participant in the transaction.

Zero-trust concept is a new approach, no standard is yet released. Hence choosing a model was a time-consuming factor. Since everything related to banks are confidential, the idea of interviewing bank security officers was out of scope. The idea of comparing security models used in banks was also out of scope as no banks agreed to share the security approaches used in the banks. Only limited resources were available online revealing cyberattacks against the financial sector. The future work of the study includes practical implementation of the proposed model and the design of a trust algorithm used by the policy engine to evaluate access requests. All the key areas of bank security need to be addressed to secure the entire data and infrastructure.

AUTHOR CONTRIBUTIONS

Umair Chaudhry: Conceptualization, project administration, resources, supervision, writing - review and editing. Aysha Hydros: Conceptualization, data curation, formal analysis, investigation, methodology, validation, writing - original draft.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing not applicable - no new data generated, or the article describes entirely theoretical research

ORCID

Umair B. Chaudhry https://orcid.org/0000-0002-8609-8357

REFERENCES

1. Henriquez, M.: Banking industry sees 1318% increase in ransomware attacks in 2021. https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021 (2021). Accessed 12 Feb 2022
2. RBA - Bank of Australia, R. (2021) Reserve Bank of Australia Annual Report 2021. Available at: https://www.rba.gov.au/publications/annual-reports/rba/2021
3. Bank of England: Is my money safe from cyberattacks? https://www.bankofengland.co.uk/knowledgebank/is-my-money-safe-from-cyber-attacks. Accessed 17 March 2022
4. Hammood, W.A., Arshah, R.A., Asmara, S.M., Hammood, O.A.: User-authentication model based on mobile phone IMEI number: A proposed method application for online banking system. In: International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), pp. 411–416 (2021). https://doi.org/10.1109/ICSECS52883.2021.00081
5. Yaga, D. et al.: Blockchain Technology Overview. https://doi.org/10.6028/NIST.IR.8202
6. NIST - Task Force, J. (no date) NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations JOINT TASK FORCE. doi: https://doi.org/10.6028/NIST.SP.800-53r5
7. Patil, A.P., Karkal, G., Wadhwa, J., Sawood, M., Reddy, K.D.: Design and implementation of a consensus algorithm to build zero trust model. In: IEEE 17th India Council International Conference (INDICON), pp. 1–5 (2020). https://doi.org/10.1109/INDICON49873.2020.9342207
8. Datta, P., Tanwar, S., Panda, S.N., Rana, A.: Security and issues of MBanking: A technical report. In: 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1115–1118 (2020). https://doi.org/10.1109/ICRITO48877.2020.9198032
9. BCG: Banking's cybersecurity blind spot—And how to fix it. https://www.bcg.com/publications/2018/banking-cybersecurity-blind-spot-how-to-fix-it (2018). Accessed 17 March 2022
10. BIS: Covid-19 and cyber risk in the financial sector. https://www.bis.org/publ/bisbull37.pdf (2021). Accessed 26 Feb 2022
11. Anatoliy, P.N. et al.: Technologies of safety in the bank sphere from cyber attacks. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 102–104. IEEE (2018)
12. Mahalle, A., Yong, J., Tao, X.: Ethics of IT security team for cloud architecture infrastructure in banking and financial services Industry. In: IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 506–511 (2019). https://doi.org/10.1109/CSCWD.2019.8791928
13. Dhoot, A., Nazarov, A.N., Koupaei, A.N.A.: A security risk model for online banking system. In: Systems of Signals Generating and Processing

in the Field of on-Board Communications, pp. 1–4 (2020). https://doi.org/10.1109/IEEECONF48371.2020.9078655
14. Popoola et al.: Design of a customer-centric surveillance system for ATM banking transactions using remote certification technique. In: IEEE 2nd International Conference on Cyberspace (CYBER NIGERIA), pp. 104–111 (2021). https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428795
15. Deloitte: Zero trust – Never trust, always verify. https://www2.deloitte.com/nl/nl/pages/financial-services/articles/zero-trust-never-trust-always-verify-tech-trends-banking.html Accessed 24 Feb 2022
16. Jin, S.Y., Xia, Y.: CEV framework: A central bank digital currency evaluation and verification framework with a focus on consensus algorithms and operating architectures. IEEE Access 10, 63698–63714 (2022). https://doi.org/10.1109/ACCESS.2022.3183092
17. National Cyber Security Centre: Introduction to zero trust. (2021). https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust Accessed 7 March 2022
18. D'Silva, D., Ambawade, D.D.: Building a zero trust architecture using Kubernetes. In: 6th International Conference for Convergence in Technology (I2CT), pp. 1–8 (2021). https://doi.org/10.1109/I2CT51068.2021.9418203
19. Mujib, M., Sari, R.F.: Performance evaluation of data center network with network micro-segmentation. In: 12th International Conference on Information Technology and Electrical Engineering (ICITEE), pp. 27–32 (2020). https://doi.org/10.1109/ICITEE49829.2020.9271749
20. Kong, C., Liu, J., Xian, M., Wang, H.: A small LAN zero trust network model based on Elastic Stack. In: 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 1075–1078 (2020). https://doi.org/10.1109/ICMCCE51767.2020.00236
21. Google: BeyondCorp An approach to enterprise security. https://cloud.google.com/beyondcorp Accessed 26 Feb 2022
22. Vanickis, R., Jacob, P., Dehghanzadeh, S., Lee, B.: Access control policy enforcement for zero-trust-networking. In: 2018 29th Irish Signals and Systems Conference (ISSC), pp. 1–6 (2018). https://doi.org/10.1109/ISSC.2018.8585365
23. Wylde, A.: Zero trust: Never trust, always verify. In: International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–4 (2021). https://doi.org/10.1109/CyberSA52016.2021.9478244
24. Hatakeyama, K., Kotani, D., Okabe, Y.: Zero Trust Federation: Sharing context under user control towards zero trust in identity federation. In: IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 514–519 (2021). https://doi.org/10.1109/PerComWorkshops51409.2021.9431116
25. Zhang, P. et al.: Dynamic access control technology based on zero-trust light verification network model. In: International Conference on Communications, Information System and Computer Engineering (CISCE), pp. 712–715 (2021). https://doi.org/10.1109/CISCE52179.2021.9445896
26. Mehraj, S., Banday, M.T.: Establishing a zero trust strategy in cloud computing environment. In: International Conference on Computer Communication and Informatics (ICCCI), pp. 1–6 (2020). https://doi.org/10.1109/ICCCI48352.2020.9104214
27. Zhang, F., Jiang, X.: The zero-trust security platform for data trusteeship. In: 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), pp. 1014–1017 (2021). https://doi.org/10.1109/AEMCSE51986.2021.00207
28. Cao, Z., Markowitch, O.: Comment on "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing". IEEE Trans. Parallel Distrib. Syst. 32(2), 392–393 (2021). https://doi.org/10.1109/TPDS.2020.3021683
29. Muncaster, P.: API flaw exposes elastic stack users to data theft and DoS. Infosecurity Magazine (2021). https://www.infosecurity-magazine.com/news/api-elastic-stack-data-theft-dos/ Accessed 1 Jan 2022
30. Wu, K., Shi, J., Guo, Z., Zhang, Z., Cai, J.: Research on security strategy of power internet of things devices based on zero-trust. In: International Conference on Computer Engineering and Application (ICCEA), pp. 79–83 (2021). https://doi.org/10.1109/ICCEA53728.2021.00023
31. Chen, L., Dai, Z., Chen, M., Li, N.: Research on the security protection framework of power mobile internet services based on zero trust. In: 6th International Conference on Smart Grid and Electrical Automation (ICSGEA), pp. 65–68 (2021). https://doi.org/10.1109/ICSGEA53208.2021.00021
32. Rodigari, S., O'Shea, D., McCarthy, P. McCarry, M., McSweeney, S.: Performance analysis of zero-trust multi-cloud. In: IEEE 14th International Conference on Cloud Computing (CLOUD), pp. 730–732 (2021). https://doi.org/10.1109/CLOUD53861.2021.00097
33. Shamim, M.S.I., Bhuiyan, F.A., Rahman, A.: XI commandments of Kubernetes security: A systematization of knowledge related to Kubernetes security practices. In: IEEE Secure Development (SecDev), pp. 58–64 (2020). https://doi.org/10.1109/SecDev45635.2020.00025
34. Sateesh, H., Zavarsky, P.: State-of-the-art VANET trust models: Challenges and recommendations. In: 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 0757–0764 (2020). https://doi.org/10.1109/IEMCON51383.2020.9284953
35. Sultana et al.: Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med. Inf. Decis. Making 20, 256 (2020). https://doi.org/10.1186/s12911-020-01275-y
36. Taguchi, Y., Kanai, A., Tanimo, S.: A distributed log management method using a blockchain Scheme. In: IEEE International Conference on Consumer Electronics (ICCE), pp. 1–3 (2020). https://doi.org/10.1109/ICCE46568.2020.9043151
37. Curran, B.: What is a Merkl tree? Beginner's guide to this blockchain component. https://blockonomi.com/merkle-tree/ (2020). Accessed 26 Feb 2022
38. Alupotha, J. How to calculate the hash of a block in bitcoin?. https://dlt-repo.net/how-to-calculate-a-bitcoin-block-hash-manually/ Accessed 26 Feb 2022
39. Bagrecha, N.R., Polishwala, I.M., Mehrotra, P.A., Sharma, R., Thakare, B.S.: Decentralised blockchain technology: Application in banking sector. In: International Conference for Emerging Technology (INCET), pp. 1–5 (2020). https://doi.org/10.1109/INCET49848.2020.9154115
40. Sakho, S., Jianbiao, Z., Essaf, F., Badiss, K.: Improving banking transactions using blockchain technology. In: IEEE 5th International Conference on Computer and Communications (ICCC), pp. 1258–1263 (2019). https://doi.org/10.1109/ICCC47050.2019.9064344
41. Deng, X. et al.: A survey of blockchain consensus algorithms. In: 2022 International Conference on Blockchain Technology and Information Security, ICBCTIS, pp. 188–192 (2022). https://doi.org/10.1109/ICBCTIS55569.2022.00050
42. Ye, J., Yang, L., Ye, H.: A blockchain consensus algorithm based on node random number calculation. In: 2022 International Conference on Blockchain Technology and Information Security, ICBCTIS, pp. 85–87 (2022). https://doi.org/10.1109/ICBCTIS55569.2022.00030
43. Wan, J. et al.: AnonymousFox: An efficient and scalable blockchain consensus algorithm. IEEE Internet Things J. 9, 24236–24252 (2022). https://doi.org/10.1109/JIOT.2022.3189200
44. MSRvantage: MSRvantage promise delivered [LinkedIn] January. https://www.linkedin.com/feed/update/urn:li:activity:6886258007731146752/ (2022). Accessed 20 Feb 2022
45. Fang, J.: Research on blockchain consensus algorithm based on DWBA protocol. In: 2022 IEEE International Conference on Artificial Intelligence and Computer Applications, ICAICA, pp. 639–642 (2022). https://doi.org/10.1109/ICAICA54878.2022.9844501
46. Praveen, G. et al.: Novel consensus algorithm for blockchain using Proof-of-Majority (PoM). IEEE Netw. Lett. 4, 208–211 (2022). https://doi.org/10.1109/LNET.2022.3213971
47. Sun, Z., Chiu, W.Y., Meng, W.: Mosaic - A blockchain consensus algorithm based on random number generation. In: 2022 IEEE International Conference on Blockchain, Blockchain 2022, pp. 105–114 (2022). https://doi.org/10.1109/BLOCKCHAIN55522.2022.00024
48. Yan, S.: Analysis on blockchain consensus mechanism based on Proof of Work and Proof of Stake. In: 2022 International Conference on Data

Analytics, Computing and Artificial Intelligence (ICDACAI), pp. 464–467 (2022). https://doi.org/10.1109/ICDACAI57211.2022.00098
49. Yadav, P., Chandak, R.: Transforming the know your customer (KYC) process using blockchain. In: International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1–5 (2019). https://doi.org/10.1109/ICAC347590.2019.9036811
50. Norvill, R., Steichen, M., Shbair, W.M., State, R.: Demo: Blockchain for the simplification and automation of KYC result sharing. In: IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 9–10 (2019). https://doi.org/10.1109/BLOC.2019.8751480
51. Schlatt, V., Sedlmeir, J., Feulner, S., Urbach, N.: Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Inf. Manag. 59(7), 103553 (2021). https://doi.org/10.1016/j.im.2021.103553
52. Sinha, S.K., Bathla, R.: Implementation of blockchain in financial sector to improve scalability. In: 2019 4th International Conference on Information Systems and Computer Networks, pp. 144–148. ISCON 2019. Institute of Electrical and Electronics Engineers Inc., (2019). https://doi.org/10.1109/ISCON47742.2019.9036241
53. Patel, B.: How can blockchain help with AML KYC. https://www.finextra.com/blogposting/15022/how-can-blockchain-help-with-aml-kyc (2018). Accessed 12 Jan 2022
54. Garg et al.: Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technol. Forecasting Social Change 163, 120407 (2021). https://www.sciencedirect.com/science/article/pii/S0040162520312336
55. Dadhich, M. et al.: Analytical study of stochastic trends of non-performing assets of public and private commercial banks in India. Proceedings - 2021 3rd International Conference on Advances in Computing, Communication Control and Networking, ICAC3N (2021). IEEE, pp. 71–76. https://doi.org/10.1109/ICAC3N53548.2021.9725463
56. Osmani, M., et al.: Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. Journal of Enterprise Information Management. Emerald Group Holdings Ltd. 34(3), 884–899. https://doi.org/10.1108/JEIM-02-2020-0044/FULL/PDF
57. Kruglova, I.A., Dolbezhkin, V.A.: Objective barriers to the implementation of blockchain technology in the financial sector. In: International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI), pp. 47–50 (2018). https://doi.org/10.1109/IC-AIAI.2018.8674451
58. Liu, Y. et al.: A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust Internet-of-Things. IEEE Trans. Comput. 72, 501–512 (2022). https://doi.org/10.1109/TC.2022.3157996
59. Bandara, E. et al.: Skunk — A blockchain and zero trust security enabled federated learning platform for 5G/6G network slicing. In: 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 109–117 (2022). doi: https://doi.org/10.1109/SECON55815.2022.9918536
60. Alevizos, L. et al.: Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture. IEEE Access 10, 89270–89288 (2022). https://doi.org/10.1109/ACCESS.2022.3200165
61. Diaz Rivera, J.J. et al.: Secure enrollment token delivery for Zero Trust networks using blockchain. In: 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1–6 (2022). https://doi.org/10.23919/APNOMS56106.2022.9919940
62. Alevizos, L., Ta, V.T., Eiza, M.H.: Augmenting zero trust architecture to endpoints using blockchain: A state of the art review. https://arxiv.org/ftp/arxiv/papers/2104/2104.00460.pdf (2021). Accessed 24 Jan 2022
63. Forbes: Enhancing security by leveraging blockchain tech as an enabler for zero-trust frameworks. https://www.forbes.com/sites/forbestechcouncil/2018/08/23/enhancing-security-by-leveraging-blockchain-tech-as-an-enabler-for-zero-trust-frameworks/?sh=7db442763192 (2018). Accessed 25 Jan 2022
64. Sajić, M., Bundalo, D., Bundalo, Z., Pašalić, D.: Digital technologies in the transformation of classical retail bank into digital bank. In: 25th Telecommunication Forum (TELFOR), pp. 1–4 (2017). https://doi.org/10.1109/TELFOR.2017.8249404
65. Popova, N.A., Butakova, N.G.: Research of a possibility of using blockchain technology without tokens to protect banking transactions. In: IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1764–1768 (2019). https://doi.org/10.1109/EIConRus.2019.8657279
66. Amrutiya, V., Jhamb, S., Priyadarshi, P., Bhatia, A.: Trustless two-factor authentication using smart contracts in blockchains. In: International Conference on Information Networking (ICOIN), pp. 6671 (2019). https://doi.org/10.1109/ICOIN.2019.8718198
67. Zand, M., Gupta, R.: How two-factor authentication works with blockchain https://www.securitymagazine.com/articles/94479-how-two-factor-authentication-works-with-blockchain (2021)
68. Microsoft: Evolving zero trust. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT (2021). Accessed 13 Feb 2022
69. Scott, et al.: Zero Trust Architecture - NIST Special Publication 800-207. Nist, p. 49. https://doi.org/10.6028/NIST.SP.800-207.

How to cite this article: Chaudhry, U.B., Hydros, A.K.M.: Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. IET Blockchain 3, 98–115 (2023). https://doi.org/10.1049/blc2.12028