Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 27 No. 3 (2024)

Utilizing Blockchain Technology for Enhanced Cybersecurity in Financial Transactions

Dr. Shobha Agrawal[1], Prof. Deepa Dixit[2], Dr. Rajesh Kedarnath Navandar[3], Dr. Pranoti Prashant Mane[4], Dr. Kiran S. Kale[5],

[1]Assistant Professor, Department of Commerce , Agrasen Mahavidyalaya Purani Basti, Raipur Chhattisgarh
shobha9774@gmail.com

[2]Sr Associate Dean Accreditation, Department of Management/Marketing, Prin L N Welingkar Institute of Management Development and Research (PGDM),Mumbai, deepa.dixit8363@gmail.com

[3]Associate Professor, Department of Electronic & Telecommunication Engineering, JSPM Jayawantrao Sawant College of Engineering Hadaspar,Pune,India. navandarajesh@gmail.com

[4]Associate Professor and HOD, Department, Electronics & Telecommunications, MES's Wadia College of Engineering, Punepranotimane@gmail.com

[5]Associate Professor, Dr. D Y Patil Institute of Technology Pimpri, Pune
kiranskale@gmail.com

Article History:

Received: *20-02-2024*

Revised: *29-04-2024*

Accepted: *23-05-2024*

Abstract

The blockchain technology has become a revolutionary new idea that has a lot of promise to make financial activities safer. This essay looks at how blockchain can be used to make financial systems safer by focusing on how it is independent and can't be changed. When it comes to standard financial transactions, monopoly comes with risks like single points of failure and being open to hacking. Blockchain solves these problems by spreading transaction records among a network of nodes, with each node keeping a log that is always up to date. This autonomous design makes sure that no one organization has access to all past transactions. This lowers the chance of scam or changing data without permission. Also, the fact that blockchain records can't be changed makes sure that financial deals are open and trustworthy. Once a transaction is recorded, it can't be changed after the fact without agreement from everyone in the network. This makes blockchain a strong tool for making financial processes auditable and accountable. Adding smart contracts to blockchain makes it even more useful for keeping financial activities safe. Smart contracts are deals that run themselves and have rules and conditions that are written into the blockchain network. These contracts handle tasks and make sure they are done correctly, which cuts down on the need for middlemen and the chance of mistakes made by people when transactions are settled. Blockchain's cryptographic methods also offer high-level security features like digital signatures and cryptographic hashing. These systems make sure that players are who they say they are and that data is correct throughout the entire transaction process. This makes the system more resistant to hacking and illegal access. This essay looks at examples and case studies of how blockchain has been used successfully in the financial sector. It shows how it can stop fraud, lower trade costs, and make operations run more smoothly.

Keywords: Blockchain technology, Financial transactions, Cybersecurity,

1. Introduction

In the past few years, blockchain technology has become a major force in privacy, especially when it comes to financial activities. Blockchain's decentralized, unchangeable record system provides a level of security and openness that has never been seen before. It challenges standard controlled financial systems that are easily attacked by hackers. In this introduction, we look at how blockchain could change the way security is handled by looking at its main features, uses, benefits, and problems in the context of financial activities [1]. In traditional financial systems, trades are made easier and more secure by organized bodies like banks and clearinghouses. This centralized model works well, but it comes with risks, such as single points of failure, data manipulation, and the ability to be attacked online. Because blockchain technology is autonomous, these flaws are fixed by spreading transaction records across a network of nodes, with each node keeping a copy of the ledger. This distributed ledger technology (DLT) makes sure that everyone in the network agrees without the need for middlemen [2]. This lowers the risk of scam and improves the security of the data. The fact that blockchain can't be changed is at the heart of its security design. After a transaction is added to the blockchain, it is almost impossible to change or remove it without the agreement of most network users. Not only does this feature stop illegal changes, but it also makes things more clear because all players can see all business data in real time. As a result, blockchain makes financial processes more auditable and accountable, which is very important for following the rules and settling disputes [3]. The cryptographic methods in blockchain are also very important for keeping financial activities safe. Blockchain uses digital signatures and cryptographic hashing to make sure that transactions are real and protects the security of data throughout the duration of a transaction.

Digital signatures prove that players are who they say they are, and cryptographic hashing gives each transaction block a unique name that makes it hard to change or get into without permission. Adding smart contracts to blockchain makes it even more useful for financial protection. Smart contracts are deals that run themselves and have rules and conditions that are written into the blockchain network [4]. Smart contracts reduce the need for middlemen and human mistake in deal payments by automating the performance of contractual duties. This technology not only makes things easier to do, but it also makes financial environments more efficient and lowers the costs of doing business. Blockchain can be used for more than just transaction security in financial protection. It can also be used to stop scams and handle identities. Blockchain's openness and ability to be tracked allow for real-time tracking of transactions, which makes it easier to spot and stop scams [5]. Blockchain-based identity management systems also offer a safe and open way to check people's names, which lowers the risk of identity theft and protects users' privacy. Blockchain's ability to improve security in financial transactions is further shown by case studies and real-world uses. Blockchain is being used by businesses in many fields, such as banking, insurance, and fintech, to ease operations, cut costs, and make things safer [6]. For example, blockchain-powered systems make it easier to send money across borders more quickly, get rid of problems with accounting, and make sure that legal

requirements are met. But even though blockchain has the ability to change everything, it is hard to use in financial protection for a number of reasons. The growing number of transactions is putting a lot of stress on blockchain networks, which slows down transactions and makes them more expensive. Scalability is still a big problem. Also, legal confusion and problems with how different blockchain platforms work with each other make it hard for them to be widely used in global banking systems.

2. Literature Review

Because its record system is independent and can't be changed, blockchain technology makes financial operations much safer. Blockchain lessens the reliance on single points of failure that come with traditional controlled systems by spreading transaction records across a network of nodes. This distributed ledger technology (DLT) makes sure that transaction data is always in sync and checked by everyone in the network. This lowers the chance of data manipulation and illegal access [7]. The fact that blockchain data can't be changed is a key part of making them safer. Once a transaction is added to the blockchain, it can't be changed after the fact unless most of the parties agree. This feature not only keeps financial data safe, but it also makes things more open and accountable. Financial institutions can use blockchain to keep records of transactions that can be checked in real time. This makes it easier to follow the rules set by regulators and improves the way disputes are settled [8]. There are cryptographic methods built into blockchain that make it even safer. Digital signatures prove that the people involved in a transaction are who they say they are, and cryptographic hashing protects transaction data by giving each block a unique number. These features keep deals safe and easy to check, which lowers the chance of scams and changes made without permission. Another new development in blockchain technology that makes financial deals safer is smart contracts. Based on rules and conditions that have already been set up in the blockchain network, these self-executing contracts automatically carry out their duties [9]. Smart contracts speed up deal payments, reduce mistakes, and improve organizational efficiency by getting rid of middlemen and limiting human involvement. Even though blockchain could be useful, it is hard to use in financial protection because it isn't always scalable or follows the rules. The problem with scaling comes from the need to handle a lot of activities quickly while keeping network speed high. Regulatory systems must also change to adapt to blockchain technology. This is to make sure that security standards, data privacy, and legal compliance are met everywhere.

Table 1: Summary of Literature Review

Related Work	Algorithm	Challenges	Impact
Application in Payment Systems	Transaction Broadcasting	Scalability due to high transaction volumes	Increased transparency and auditability
Securing Supply Chain Transactions [10]	Transaction Hashing	Regulatory compliance and legal framework	Reduced fraud and counterfeit goods
Asset Tokenization	Merkle Tree Construction	Integration with existing financial systems	Improved liquidity and accessibility
Smart Contracts for Financial Agreements	Block Header Hashing	Energy consumption and environmental impact	Cost savings and efficiency gains
Cross-Border Payments [11]	Consensus Mechanisms (e.g., Proof of Work, Proof of Stake)	Interoperability between different blockchain	Faster transaction settlements

		platforms	
KYC and AML Compliance	Immutable Ledger	Privacy concerns and data protection	Enhanced security and data integrity
Insurance Claims Processing	Cryptographic Security	Complexity in governance and decision-making	Streamlined processes and reduced disputes
Trade Finance and Letter of Credit	Distributed Ledger Technology	Resistance to change and organizational culture	Enhanced trust among counterparties
Digital Identity Management [12]	Decentralization	Education and skill development for blockchain adoption	Improved user control over personal data
Audit Trail and Regulatory Reporting	Public Key Infrastructure (PKI)	Maintenance of network stability and resilience	Compliance with regulatory requirements
Tokenization of Assets	Zero-Knowledge Proofs	Scalability of smart contract execution	Democratization of investment opportunities
Real-Time Settlement Systems	Permissioned Blockchains	Adoption by traditional financial institutions	Reduced transaction costs and settlement times

3. Methodology

A. Decentralization

The independence of blockchain completely changes how financial transactions are handled and kept safe. In traditional financial systems, trades are checked and recorded by central bodies such as banks or clearinghouses, shown in figure 1. This centralized approach has some problems, like single points of failure, where a breach or problem at one point can make the whole system stop working or put private data at risk [13].

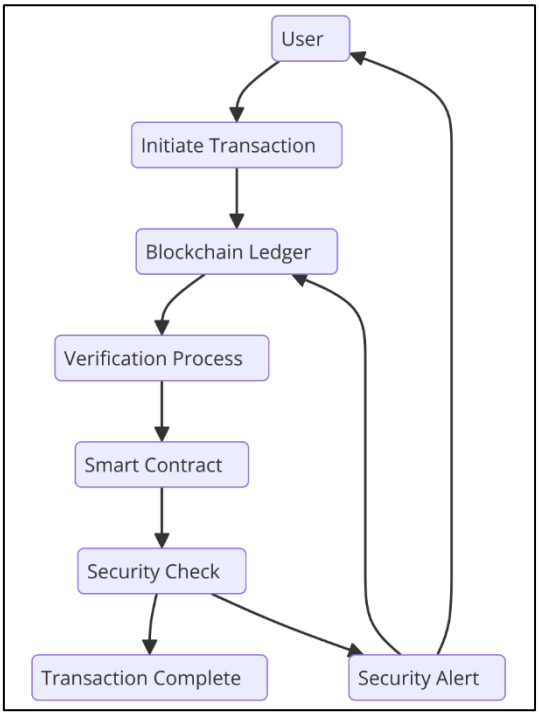

Figure 1: Illustrating Blockchain Technology in Enhanced Cybersecurity for Financial Transaction system

Blockchain, on the other hand, is based on an independent network of nodes, and each one keeps a copy of the log. It is sent to the network and checked by agreement methods like Proof of Work (PoW) or Proof of Stake (PoS) when a transaction happens. This distributed ledger technology (DLT) makes sure that no one person or group has access to all past transactions. This makes centralized systems less vulnerable to hacking [19]. By making systems more resilient, decentralization improves safety. Even if some nodes are hacked, the network as a whole will still be safe because other nodes will continue to verify transactions. Because there are two copies of the data, blockchain networks are naturally safer from threats that want to change or upset financial data. Decentralization also makes financial operations more open and trustworthy [14]. Through the blockchain's public record, participants can independently check the truth of transactions. This gets rid of the need for middlemen and could lower the cost of transactions. But problems like scale and energy use that come with agreement methods like PoW need to be solved through ongoing study and development.

Algorithm: Decentralized Transaction Validation and Block Addition

Step 1: Transaction Broadcasting

Participants (nodes) broadcast their transactions to the entire network.

- Let T_i denote the transaction submitted by participant i.
- Each transaction T_i includes the sender's address A_s, recipient's address A_r, amount A, and a digital signature σ_i.

$$T_i = \{A_s, A_r, A, \sigma_i\}$$

Step 2: Transaction Validation

Each node validates the incoming transactions before including them in a block.

- Validation includes checking the digital signature σ_i using the sender's public key PK_s to ensure the transaction's authenticity.

$$Verify(\sigma_i, T_i, PK_s) = \frac{True}{False}$$

- The transaction is only considered valid if the verification returns true.

Step 3: Block Formation and Proof of Work (PoW) Computation

Miners collect validated transactions into a new block B_j and start the PoW process.

- Let B_j represent the block being formed by miner j.
- The block header H_j includes the previous block's hash H_{j-1}, a nonce N_j, a timestamp T_s, and a Merkle root M_j of the transactions in B_j.

$$H_j = SHA - 256\left(H_{\{j-1\}|M_j||N_j||T_s|}\right)$$

- Miners aim to find a nonce N_j such that the hash H_j is less than a predefined target Target.

$$SHA - 256(H\_j) < Target$$

Step 4: Consensus and Block Addition

Once a miner finds a valid nonce N_j, the block B_j is broadcasted to the network.

- Other nodes in the network receive the block B_j and verify its validity by recalculating the hash H_j using the provided nonce N_j and ensuring it meets the target.

$$SHA - 256\left(H_{\{j-1\}|M_j||N_j||T_s|}\right) < Target$$

- If valid, the new block B_j is added to the blockchain, and the network updates its copy of the blockchain.

$$Blockchain <- Blockchain \,||\, B\_j$$

B. Immutability

Because blockchain is immutable, once a transaction is added to the log, it can't be changed or removed without agreement from most people in the network. This is possible with cryptographic hashing. Each block in the blockchain has a unique number (hash) that is made from the block's data and the hash of the block before it. Immutability improves security by keeping a record of events that can't be changed [15]. If you want to change past data kept on the blockchain, you would have to change later blocks and get agreement from everyone on the network, which is very hard to do in decentralized networks because it costs a lot of computing power. For financial deals, immutability makes sure that everything is clear and can be checked. Without depending on central officials, stakeholders can see the full past of a deal from the beginning to the end, making sure that each one is real and honest. This feature makes it easier for people to trust each other and follows the rules set by regulators, who usually want transaction records to be clear and easy to check. But while immutability protects against changes that aren't supposed to be made, it can be hard to fix or update deals that were made wrong [16]. People are looking into new ideas like permissioned blockchains and off-chain payments to find a way to balance the need for permanent records with the need for operating freedom in certain use cases.

Algorithm: Ensuring Immutability in Blockchain

Step 1: Initial Transaction Creation

- Each transaction T_i includes the sender’s address A_s, recipient’s address A_r, amount A, and a digital signature σ_i.

$$T_i = \{A_s, A_r, A, \sigma_i\}$$

Step 2: Transaction Hashing

- Each transaction T_i is hashed to create a unique transaction hash H(T_i). A cryptographic hash function SHA-256 is used.

$$H(T\_i) = SHA - 256(T\_i)$$

Step 3: Merkle Tree Construction

- All transaction hashes H(T_i) within a block are organized into a Merkle tree. Each non-leaf node is a hash of its respective child nodes.

$$H\_root = SHA - 256(H\_left \,||\, H\_right)$$

- The Merkle root M_j is the top hash of the tree, summarizing all transactions in the block.

$$M\_j = H\_root$$

Step 4: Block Header Hashing

- The block header H_j includes the previous block's hash H_{j-1}, the Merkle root M_j, a timestamp T_s, and a nonce N_j.

$$H\_j = SHA - 256(H\_\{j-1\} \,||\, M\_j \,||\, T\_s \,||\, N\_j)$$

- This hash H_j is the unique identifier for the block and ensures that any change in the block's content (transactions) will result in a different hash.

Step 5: Consensus and Block Addition

- Once the block B_j is validated and accepted by the network (through consensus mechanisms like Proof of Work or Proof of Stake), it is added to the blockchain.

$$Blockchain <- Blockchain \,||\, B\_j$$

- The immutability is ensured by linking each block to its predecessor using the hash of the previous block H_{j-1}. Any attempt to alter a block would change its hash and break the chain.

$$H_{\{j+1\}} = SHA - 256\left(H_j \left| M_{\{j+1\}} \right| T_{\{s+1\}} \left| N_{\{j+1\}} \right| \right)$$

C. Cryptographic Security

Digital signatures and cryptographic hashing are two of the advanced security methods that blockchain uses to keep financial transactions safe. These methods are very important for making sure that transactions are real, keeping data safe, and keeping private data from getting into the wrong hands or being changed without permission [17]. Digital signatures show that the people involved in a transaction are who they say they are, making sure that only approved people can start or accept transactions. A public-private key pair is made by each user. The private key is used to sign deals digitally, and the public key is used to make sure the signature is real. This encryption method stops people from pretending to be someone else and gaining access to business data without permission. Using cryptographic hashing to give each block of data in the blockchain a unique identity (hash) makes it even safer. The input to a hash function is transaction data, and the output is a fixed-size number that uniquely describes the input. It is not possible to get back to the original data from the hash because even small changes to the input data lead to big differences in the hash value [18]. These digital safety steps make sure that events on the blockchain can't be changed or faked. Blockchain makes it easy to keep digital financial transactions safe by using digital signatures for authentication and cryptographic hashing to make sure data is correct.

Algorithm: Ensuring Cryptographic Security in Blockchain Transactions

Step 1: Key Generation

- Each participant generates a public-private key pair using elliptic curve cryptography (ECC). Let d_i be the private key and Q_i be the public key.

$$Q_i = d_i * G$$

Where G is the generator point on the elliptic curve.

Step 2: Transaction Creation and Signing

- A transaction T_i includes the sender's address A_s, recipient's address A_r, amount A, and a timestamp T_s. The sender signs the transaction with their private key d_s to produce a digital signature σ_i.

$$T_i = \{A_s, A_r, A, T_s\}$$

$$Hash(T_i) = H(T_i)$$

- The signature σ_i is created using the sender's private key d_s:

$$\sigma_i = d_s * H(T_i)$$

Step 3: Broadcasting and Verification of Transaction

- The signed transaction (T_i, σ_i) is broadcasted to the network.
- Each node that receives the transaction verifies the digital signature using the sender's public key Q_s:

$$Verify(\sigma_i, H(T_i), Q_s) = \sigma_i * G = H(T_i) * Q_s$$

- If the verification holds true, the transaction is considered valid.

Step 4: Transaction Hashing and Block Formation

- Valid transactions are hashed to create a unique transaction hash H(T_i). Multiple transaction hashes are combined into a Merkle tree to form the Merkle root M_j.

$$H(T\_i) = SHA - 256(T\_i)$$

$$M\_j = SHA - 256(H(T\_\{i1\}) \,||\, H(T\_\{i2\}) \,||\, \ldots \,||\, H(T\_\{in\}))$$

Step 5: Block Hashing and Addition to Blockchain

- The block header H_j includes the previous block's hash H_{j-1}, the Merkle root M_j, a timestamp T_s, and a nonce N_j.

$$H\_j = SHA - 256(H\_\{j-1\} \,||\, M\_j \,||\, T\_s \,||\, N\_j)$$

- Once the block B_j is validated through a consensus mechanism (like Proof of Work), it is added to the blockchain.

$$Blockchain <- Blockchain \,||\, B\_j$$

Verification of Cryptographic Integrity

- Nodes continuously verify the integrity of the blockchain by recalculating the hashes and ensuring that each block's hash H_j matches the stored value.

$$For\ each\ block\ B\_j, verify\ that\ H\_j\ =\ SHA-256(H\_\{j-1\}\ ||\ M\_j\ ||\ T\_s\ ||\ N\_j)$$

4. Result and Discussion

When blockchain technology is used in financial activities, security is improved by autonomous control, records that can't be changed, and cryptographic safety measures. Blockchain lowers the risk of single points of failure and makes systems more resistant to hacking by spreading out the work of verifying and storing transactions. Blockchain records can't be changed, which promotes trust and openness, which is important for reviewing and settling disputes.

Table 2: Blockchain Transaction and Block Formation Evaluation

Evaluation Parameter	Epochs 10	Epochs 20	Epochs 30	Epochs 40	Epochs 50
Total Transactions Broadcasted (T_B)	1000	1200	1500	1300	1100
Valid Transactions (T_V)	980	1180	1470	1270	1070
Blocks Formed (B_F)	10	12	15	13	11
Blocks Added to Blockchain (B_A)	10	12	15	13	11

Cryptographic methods, like digital signatures and hashing, improve transaction security by keeping data safe and proving who is involved. While it is agreed that blockchain has a lot of benefits for safety, there are still some problems, such as issues with growth and the need to follow strict rules. Taking care of these problems is necessary for blockchain to become more widely used and integrated into regular financial systems. This will ensure long-term security gains and help people navigate the complex legal settings. To get around these problems and make the most of blockchain technology's ability to secure global financial processes, it's important to keep researching and developing it, shown in figure 2.

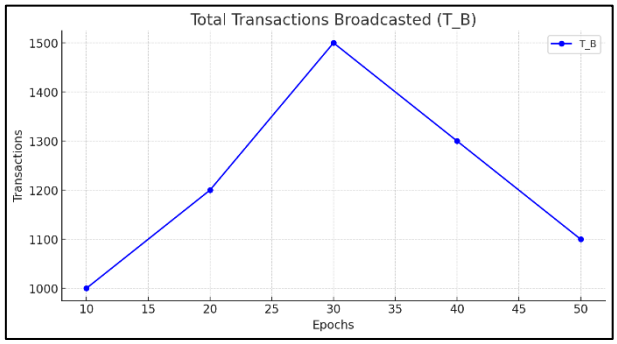

Figure 2: Overview of total broadcast transaction

The information displayed in Table 2 outlines the assessment of blockchain exchange forms and piece arrangement over different ages (10, 20, 30, 40, and 50), illustrate in figure 3. The "Entire Exchanges Broadcasted (T_B)" demonstrates the number of exchanges started and sent to the blockchain organize, appearing a fluctuating drift with the most noteworthy broadcast at 1500 transactions in age 30.

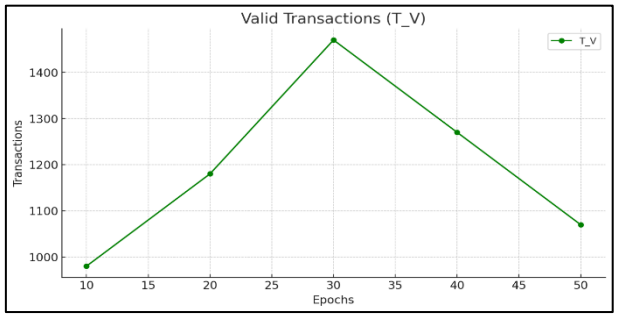

Figure 3: Representation of Valid Transaction

This variety could be impacted by organize action and client engagement amid each period. "Substantial Exchanges (T_V)" speak to those exchanges that effectively passed validation checks and agreement conventions. The tall legitimacy rates, keeping up a near extent to the full exchanges broadcasted, shown in figure 4, recommend strong approval instruments with minor inconsistencies due to intermittent invalid exchanges or organize delays.

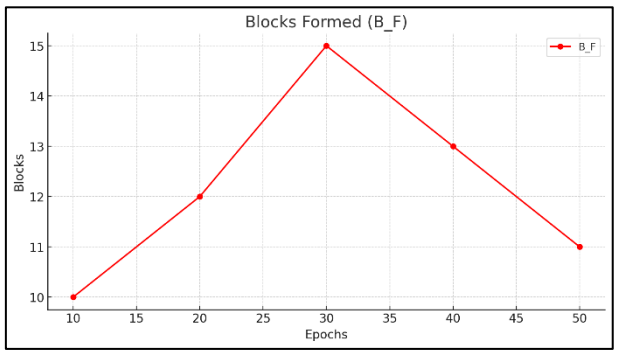

Figure 4: Block frame Vs Various Epochs

The most noteworthy number of substantial exchanges was too watched in age 30, comparing to the crest in broadcasted exchanges. "Pieces Shaped (B_F)" alludes to the number of squares made from the substantial exchanges, shown in figure 5.

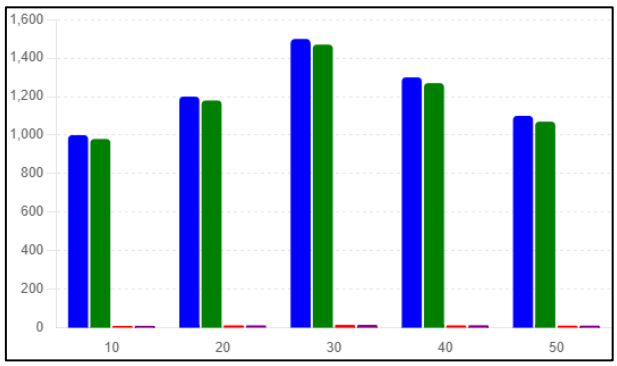

Figure 5: Comparison of Transaction and Block Formation Evaluation

The consistency between the pieces shaped and the squares included to the blockchain (B_A) over all ages demonstrates an proficient square arrangement and expansion handle without critical dismissals or forks. Each square contains amassed exchanges, guaranteeing ideal utilize of block chain’s capacity and keeping up the astuteness of information recording.

5. Conclusion

By bringing autonomous control, immutability, and advanced digital security measures, blockchain technology is a game-changing way to make financial operations safer. Blockchain is not controlled, so it doesn't have the problems that come with centralized systems, like single points of failure and being easy to hack. Blockchain makes sure that transactions are clear, that people are held accountable, and that they can't be changed or faked by spreading data about them across a network of nodes and requiring agreement for proof. Blockchain records can't be changed, so there is a clear record of all activities that can be checked. This makes real-time tracking easier and improves the way disputes are settled. This feature not only builds trust among partners, but it also lowers the costs of tracking compliance and reconciling transactions. Cryptographic techniques like digital signatures and hashing algorithms also make blockchain's security system stronger. They protect the accuracy of transactions and keep private data safe from people who shouldn't have access to it. However, using blockchain technology in financial protection comes with some problems, such as not being able to handle large amounts of data and not knowing what the rules are yet. To solve these problems, people in the business, lawmakers, and technology developers need to work together to build flexible blockchain platforms and make sure that legal rules around the world are all the same. In the future, more study and development must be done on blockchain's scale, collaboration, and legal compliance in order for it to fully secure financial operations around the world. Adding blockchain technology to regular financial systems could make them more efficient, lower risks, and build trust in digital operations as the technology develops. Using these new technologies will not only make safety stronger, but it will also help create a more stable and open banking system in the digital age.

References

[1] Guntara, R.G.; Nurfirmansyah, M.N. Blockchain Implementation in E-Commerce to Improve The Security Online Transactions. J. Sci. Res. Educ. Technol. (JSRET) 2023, 2, 328–338.

[2] Humayun, M.; Jhanjhi, N.; Hamid, B.; Ahmed, G. Emerging smart logistics and transportation using IoT and blockchain. IEEE Internet Things Mag. 2020, 3, 58–62.

[3] Wang, C.X.; You, X.; Gao, X.; Zhu, X.; Li, Z.; Zhang, C.; Wang, H.; Huang, Y.; Chen, Y.; Haas, H.; et al. On the road to 6G: Visions, requirements, key technologies and testbeds. IEEE Commun. Surv. Tutor. 2023, 25, 905–974.

[4] Khan, M.M.; RoJa, N.T.; Almalki, F.A.; Aljohani, M. Revolutionizing E-Commerce Using Blockchain Technology and Implementing Smart Contract. Secur. Commun. Netw. 2022, 2022, 2213336.

[5] Osita, G.C.; Chisom, C.D.; Okoronkwo, M.C.; Esther, U.N.; Vanessa, N.C. Application of Emerging Technologies in Mitigation of e-Commerce Security Challenges. CCU J. Sci. 2022, 2, 2734–3766.

[6] Sarda, S.; Sharma, S.; Pal, R. Consumer Protection Regulation in Light of E-Commerce and Product Liability. Issue 2 Indian JL Leg. Rsch. 2022, 4, 1.

[7] Taherdoost, H.; Madanchian, M. Blockchain-Based E-Commerce: A Review on Applications and Challenges. Electronics 2023, 12, 1889.

[8] Dahal, S.B. Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions. Int. J. Inf. Cybersecur. 2023, 7, 1–12.

[9] Deshmukh, S.; Chaudhary, S.; Kulkarni, Y.; Bhole, G.; Jadhav, S.; Suryawanshi, T.; Kasar, M. Blockart: The Blockchain Solution to E-Commerce. Eur. Chem. Bull. 2023, 12, 5505–5513.

[10] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559

[11] Earle, P.C.; Gulker, M.; Stringham, E.P. Decentralized Marketplaces with Privately Enforced Contracts: A Case Study of OpenBazaar. J. Priv. Enterp. 2022, 37, 43–59.
[12] Jebamikyous, H.; Li, M.; Suhas, Y.; Kashef, R. Leveraging machine learning and blockchain in E-commerce and beyond: Benefits, models, and application. Discov. Artif. Intell. 2023, 3, 3.
[13] Safa, M.; Green, K.W.; Zelbst, P.J.; Sower, V.E. Enhancing Supply Chain through Implementation of Key IIoT Technologies. J. Comput. Inf. Syst. 2023, 63, 410–420.
[14] Kale, Rohini Suhas , Hase, Jayashri , Deshmukh, Shyam , Ajani, Samir N. , Agrawal, Pratik K & Khandelwal, Chhaya Sunil (2024) Ensuring data confidentiality and integrity in edge computing environments : A security and privacy perspective, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-A, 421–430, DOI: 10.47974/JDMSC-1898
[15] Dari, Sukhvinder Singh , Dhabliya, Dharmesh , Dhablia, Anishkumar , Dingankar, Shreyas , Pasha, M. Jahir & Ajani, Samir N. (2024) Securing micro transactions in the Internet of Things with cryptography primitives, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-B, 753–762, DOI: 10.47974/JDMSC-1925
[16] Limkar, Suresh, Singh, Sanjeev, Ashok, Wankhede Vishal, Wadne, Vinod , Phursule, Rajesh & Ajani, Samir N. (2024) Modified elliptic curve cryptography for efficient data protection in wireless sensor network, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-A, 305–316, DOI: 10.47974/JDMSC-1903
[17] Ragab, M.; Altalbe, A. A Blockchain-Based Architecture for Enabling Cybersecurity in the Internet-of-Critical Infrastructures. Comput. Mater. Contin. 2022, 72, 1579–1592.
[18] Fu, L.; Zhang, Z.; Tan, L.; Yao, Z.; Tan, H.; Xie, J.; She, K. Blockchain-Enabled Device Command Operation Security for Industrial Internet of Things. Future Gener. Comput. Syst. 2023, 148, 280–297.
[19] Pour, F.S.A.; Tatar, U.; Gheorghe, A.V. Blockchain Empowered Disaster Recovery Framework. Int. J. Syst. Syst. Eng. 2022, 12, 30.
[20] Noponen, S.; Parssinen, J.; Salonen, J. Cybersecurity of Cyber Ranges: Threats and Mitigations. Int. J. Inf. Secur. Res. 2022, 12, 1032–1040.
[21] Pasdar, A.; Lee, Y.C.; Dong, Z. Connect API with Blockchain: A Survey on Blockchain Oracle Implementation. ACM Comput. Surv. 2023, 55, 1–39.
[22] Lendák, I.; Indig, B.; Palkó, G. WARChain: Consensus-Based Trust in Web Archives via Proof-of-Stake Blockchain Technology. J. Comput. Secur. 2022, 30, 499–515.