International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: *http://ijwos.com*
Vol.02 No.12.
OPEN ACCESS
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos02120700415

ROLE OF BLOCKCHAIN TECHNOLOGY IN REDUCING FRAUDS AND FINANCIAL CRIMES

Ms. V. Varshini[1], Mr. G. Vinesh Kumar[2]
[1] *MBA Student, Department of Management studies, Vardhaman College of Engineering, Shamshabad, Hyderabad. Telangana*
[2] *Assistant Professor, Department of Management studies, Vardhaman College of Engineering, Shamshabad, Hyderabad. Telangana.*

Article Info

Article History:

Published:28 Dec 2025

Publication Issue:
Volume 2, Issue 12
December-2025

Page Number:
782-791

Corresponding Author:
Ms. V. Varshini

Abstract:

This research examines how blockchain might cut down financial scams while making modern banking safer. Instead of just adding AI to blockchain, it studies smart rules, privacy fixes, and problems when systems don't link well - focusing on shared control, locked-in records, and solid code that catches sneaky deals. Rather than guesswork, it runs number tests - like correlations, t-tests, regressions, and ANOVAs - to see how things such as system room to grow, clearer laws, hiding info but still showing proof, and blending tools actually connect. Findings reveal strong ties between these pieces lifting business profits, real concerns over messy rules begging for global agreement, yet similar opinions from all genders on mixing AI with blockchain. The study helps make sense of problems like energy use, costs, confusing rules, or keeping data secure in blockchains. Results guide officials, financial groups, but also developers to create setups that stay protected, run smoothly, while meeting regulations.

Keywords: Blockchain Technology, Financial Fraud Prevention, AI Integration, Regulatory Clarity, Privacy Models, Interoperability, Financial Security.

1. INTRODUCTION

Blockchain tech is changing money systems fast by showing every move clearly, locking data down tight, so no one person runs things alone. With scams, hacking, and stolen identities growing worldwide, solid online setups are now a must-have. Using blockchain together with smart machines helps catch shady actions live, keeps records safe from changes, while keeping info more reliable. Still, problems pop up - handling growth, unclear laws, power use, plus setup expenses aren't simple. This study looks at how well blockchain cuts down fraud, checking roadblocks tied to tools, rules, and daily operations.

2. REVIEW OF LITERATURE

Saanvi Shah, Sadi Badi (2022)

Role of Blockchain: Blockchain keeps records safe and unchanged forever, so everyone sees the same info. It logs each move clearly, leaving no doubt about what happened. When AI spots something odd, it can trigger self-running rules that enforce policies right away. Everyone allowed on the system

Copyright © 2025 The Author(s) : This is an open access article under the CC BY license (http://creativecommons.org/licenses/by-nc/4.0/)

accesses one consistent version of events. This setup helps different groups work together smoothly and check actions across teams without hassle.

Prem Kumar Sholapurapu (2024)

Role of Blockchain: blockchain Keeps data spread across a network, so no one can wipe it out at once; every deal gets locked in with a timestamp plus encryption that blocks changes; helps fight dirty money because everything's visible and trackable; uses strong digital IDs that stay safe from fakes and fraud.

Dr. Ahmed Ali (2021)

Role of Blockchain: A decentralized system keeps records safe by making them unchangeable, so every deal shows clearly without risk of meddling. Old deals stay locked - no changing or removing them - which stops sneaky moves like paying twice or editing info secretly. Systems such as proof-of-work or proof-of-stake check each deal before adding it, meaning only real entries make it onto the record. Rules built into code run actions automatically once set triggers happen, cutting mistakes from people and blocking shady interference.

Efijemue Oghenekome Paul, Obunadike Callistus, et al. (2023)

Role of Blockchain: blockchain Keeps deals safe plus clear, also protects info from changes; runs on a shared network that can't be altered, so it works well for online safety tasks; boosts protection of sensitive details while cutting down need for middlemen we must trust; might lock down digital IDs or make bank messaging faster through linked systems.

Muhammed Zakir Hossain (2023)

Role of Blockchain: blockchain Could make financial deals clearer, easier to track, while boosting responsibility checks. Acts like a shared record book visible to everyone, cutting down hidden moves. Makes spotting sketchy crypto trades quicker when hunting scams. Gives investigators better tools to prove who owns what or moved funds illegally. Since records can't be altered and are open, crooks think twice - sneaky actions stand out faster.

Anusha Ramesh, Meera Eeswaran (2024)

Role of Blockchain: blockchain Keeps a permanent record of transactions, making it easier to track shady activity while cutting down on scams - since no one controls everything, breaking in gets way harder because there's no weak spot. Data stays safe thanks to unique digital fingerprints and locked-in records. Everyone on the network agrees before anything gets added, so mistakes or fake entries don't slip through.

Ashraf Ali, Khan Mustafa (2025)

Role of Blockchain: blockchain Keeps records spread out across many places so no single person can change them; once something's logged, it stays that way - no editing after the fact; makes checking where money went easier because everything leaves a clear trail; since nobody controls it alone, cheating the system gets way harder; every bit of info is locked down tight, visible to those who need it, yet safe from meddling.

Grace Osariemen Eghe-Ikhurhe, Naheed Nawazesh Roni, etal (2024)

Role of Blockchain: Its tech progress should shape how tiny loans get checked later on, while blockchain tools matter a lot when tracking money moves across shared records - these help investigators review info faster or catch shady patterns now and then; growing skills in this area will likely decide how well accountants handle digital cash trails down the road.

Ashraf Ali, Khan Mustafa(2025)

Role of Blockchain: blockchain Uses a distributed ledger that can't be changed, so every money move is clear and trackable. Because it's locked once recorded, changing info isn't really possible. This setup helps check where funds go without confusion, making finance systems more trustworthy. The core details stay protected, open to view, and safe from meddling.

Ezekiel Onyekachukwu Udeh, Prisca Amajuoyi, Kudirat Bukola Adeusi, and Anwulika Ogechukwu Scott 2024

Role of Blockchain: Holds promise for boosting safety in money transfers - future studies ought to explore how it works in spotting scams. Because of its distributed setup along with strong encryption tools, it can build records that are hard to alter while increasing openness plus reliability.

Jai Kiran Reddy Burugulla(2024)

Role of Blockchain: It works well for safely sharing information; because of this, it supports future smart finance systems on blockchains; transferring different types of money actions becomes easier through it; thanks to clear tracking and verifiable records, users can rely on digital banks more.

STATEMENT OF THE PROBLEM

Even though it could do a lot, using blockchain gets slowed down by problems like speed limits, unclear rules, worries about data safety, also expensive setup. Banks don't have common tools or systems that work together - so plugging them in stays limited. The goal here is to tackle each of those hurdles.

RESEARCH GAP

The existing challenge of **scalability, computational complexity, and energy consumption** in implementing AI-driven blockchain solutions needs to be addressed to realize the technology's full potential in fraud prevention. The lack of **comprehensive legal and regulatory frameworks and oversight** for cryptocurrencies and blockchain technology presents difficulties for forensic accountants and is a key area requiring future research. There is a need for further research to explore the integration of blockchain technology to enhance data security and integrity, specifically investigating its potential to **prevent data tampering, secure digital identities, and streamline inter-bank communication**. There is a gap concerning how to navigate the challenges of **high system integration costs and interoperability concerns** associated with deploying AI and blockchain infrastructure, which acts as a bottleneck for wider adoption. Continued research is warranted to find solutions that **balance data privacy/confidentiality with blockchain's inherent transparency**, a critical challenge for regulatory compliance in sensitive financial sectors. Research is needed to develop forensic accounting best practices regarding the dynamic nature of cryptocurrency and

blockchain environments due to the complexity and technological limitations in tracing transactions and conducting digital investigations

OBJECTIVES OF THE STUDY

To design scalable, energy-efficient AI–blockchain architectures capable of handling large-scale financial data in real time.

To evaluate and clarify legal and regulatory issues related to blockchain, smart contracts, and cryptocurrencies for developing standardized compliance frameworks.

To develop privacy-preserving models that balance blockchain transparency with secure digital identities and confidential inter-bank data sharing.

To create standardized best-practice frameworks for cost-effective, interoperable integration of AI–blockchain systems into existing financial infrastructures.

HYPOTHESES OF THE STUDY

Hypothesis 1 – Scalability & Efficiency

H_0 says big AI-blockchain setups don't really boost speed or save power when working live.

H1: Big AI-blockchain setups boost speed while using less power, especially during live tasks - so they run smoother without draining resources.

Hypothesis 2 – Legal & Regulatory Issues

H_0 says uniform rules don't cut confusion around regulations.

H_1: Common rules make it easier to understand what's allowed**.**

Hypothesis 3 – Privacy vs Transparency

H_0 says privacy tools can't mix clear blockchains with safe ID systems.

H_1: Models that protect privacy manage to mix openness with safety - yet they keep things locked down tight.

Hypothesis 4 – Integration Frameworks

H_0: Using standard setups doesn't cut expenses or fix connection problems.

H_1: Common integration setups cut expenses while boosting compatibility across systems

3. RESEARCH METHODOLOGY

Research Design

The study uses numbers to describe things at one point in time. Because it looks at data this way, it works well for checking how blockchain use connects to stopping fraud. It also shows how clear rules affect privacy worries in banks. Instead of guessing, it measures real patterns across these areas.

Sample Size and Sampling Technique

The group includes 203 individuals from various spots in finance and tech. Because expertise was key, we went with people who were accessible - this way, everyone already knew the basics of blockchain and how money systems work.

Data Collection Methods

Primary Data:

Put together using a clear survey built on a 5-level rating system. This tool checked major areas like growth potential, rule transparency, data protection setups, along with how systems connect**.**

Secondary Data:

Data came from journals, research studies, official reports - also web-based scholarly sources - to back up the theory well.

Instrument Design

The survey used a 5-point scale where 1 meant strongly disagree and 5 meant strongly agree.

It looked at four main ideas that came from the goals

- AI–Blockchain Scalability & Energy Efficiency
- Legal and Regulatory Issues
- Privacy compared with transparency methods
- Integration Best-Practice Frameworks

The tool was reviewed by specialists, then tested again for consistency using Cronbach's Alpha.

Statistical Tools Used

The info gathered got checked through SPSS. As such, these number methods were used:

- Correlation Analysis – looks at how scalability ties into energy use, also checking what advantages it brings to companies.
- One-Sample t-Test – used to check how strong legal or regulatory concerns really are.
- Regression Analysis – used to check how transparency affects privacy-focused models.
- One-Way ANOVA – to study differences in perceptions across demographic groups.
- Descriptive Stats – gives a quick look at population traits along with how variables reacted

Ethical Considerations

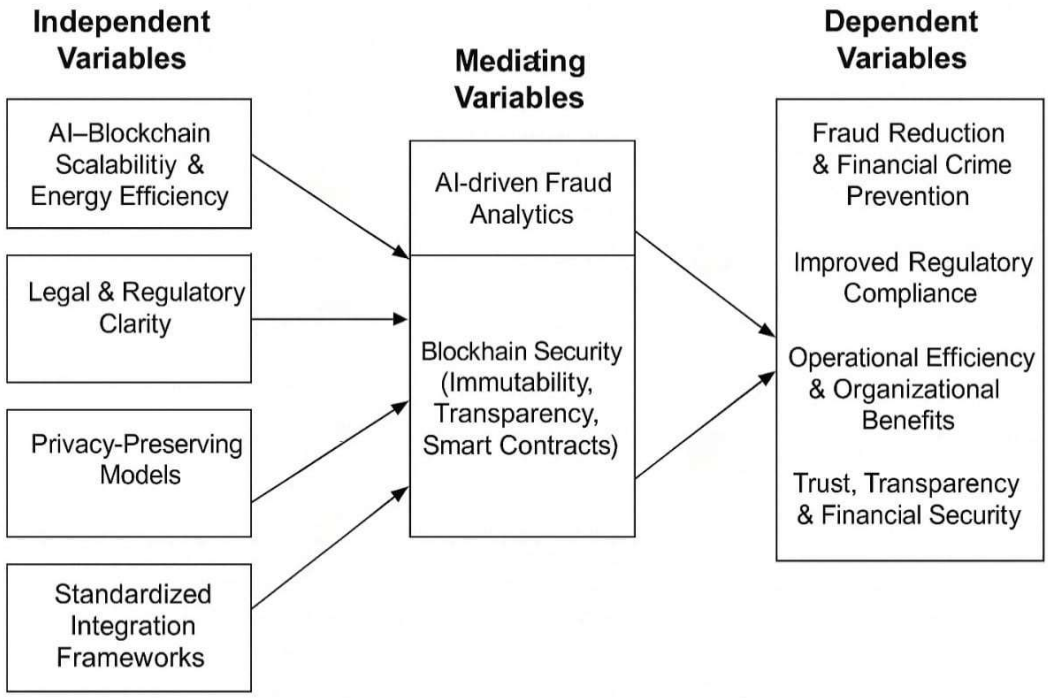
Ethical standards were strictly followed throughout the study:

- Folks joined on their own - no pressure - with each person choosing to take part because they wanted to.
- Sources stayed anonymous - keeping their identity private was a priority.
- No private or delicate details were gathered - just basic stuff stayed out of it.

Data got pulled just for school projects or testing ideas - nothing more

CONCEPTUAL MODEL

AI–Blockchain Factors → Fraud Reduction, Compliance, Efficiency



DATA ANALYSIS & INTERPRETATION

Reliability Analysis (Cronbach's Alpha)

Variable No.	Variable Name	Cronbach's Alpha	Result
V1	Scalable & Energy-Efficient AI–Blockchain Architecture	0.781	Good
V2	Legal & Regulatory Compliance Frameworks for Blockchain	0.764	Good
V3	Privacy-Preserving & Secure Digital Identity Models	0.821	Good
V4	Best-Practice Framework for AI–Blockchain Interoperability	0.802	Good
Overall	Combined Reliability	0.893	Excellent

Objective 1 – Correlation Analysis (Scalability & Efficiency)

Variables	Scalability	Energy Challenge	Real-time	AI Efficiency	Benefit
Scalability	1	0.336	0.483	0.395	0.500
Energy Challenge	0.336	1	0.495	0.565	0.550
Real-time Processing	0.483	0.495	1	0.616	0.748
AI Efficiency	0.395	0.565	0.616	1	0.633
Organizational Benefit	0.500	0.550	0.748	0.633	1

Interpretation

The findings show every factor moves in the same direction - when one gets better, so do the rest. Although scalability links somewhat to organizational gain (r = 0.500), it still plays a helpful part. Instead of downplaying energy issues, tackling them boosts AI effectiveness (r = 0.565). When it comes to real-time processing, the tie to company benefits is especially clear (r = 0.748)this feature really makes a difference. On top of that, AI efficiency lines up closely with stronger organizational results (r = 0.633). On the whole, results show boosting live processing, smart system speed, plus growth potential improves how well groups operate. So **Alternative hypothesis Accepted H_1**

Objective 2 – One-Sample t-Test

Statement	Mean	t-value	p-value	Interpretation
Blockchain regulations unclear	1.73	32.939	.000	Significant
Legal clarity slows adoption	1.71	30.376	.000	Significant
Compliance frameworks needed	1.75	31.777	.000	Significant
Difficulty interpreting crypto laws	1.71	29.612	.000	Significant
Clear guidelines strengthen trust	1.78	30.324	.000	Significant

Interpretation

Based on one-sample t-test all statements related to the legal and regulatory clarity are statistically significant ($p < 0.001$). This indicates respondents strongly agree that unclear regulations and lack of compliance frameworks create confusion and slow blockchain adoption, while clear and uniform guidelines improve trust and understanding. Therefore, the null hypothesis (H_0), which states that uniform rules do not reduce regulatory confusion, is rejected. The alternative hypothesis (H_1) is accepted, confirming that common and standardized rules make it easier to understand what is legally permitted.

Objective 3 – Regression

Predictor Statement	p-value	Interpretation
Strong privacy protection for financial data is required	0.215	Not Significant
PETs (Privacy Enhancing Technologies) are necessary	0.372	Not Significant
Secure digital identities are important	0.118	Not Significant
Current blockchain solutions do not fully protect privacy	0.267	Not Significant
Banks require better privacy-preserving models	**0.049**	**Significant**

Model Fit

Statistic	Value
R	0.234
R^2	0.055
Adjusted R^2	0.032
F-value	2.289
p-value (Model Sig.)	**0.047**

Interpretation

The regression works - it's solid (p = .047) - so privacy aspects as a group do tie into how age plays out. Out of everything tested, just one point stands out: people feeling banks need stronger privacy setups; older folks lean toward agreeing, though only a bit. Instead of "and," stuff like trust or openness didn't link clearly to age - most had p above .05. Even so, the whole setup captures only a sliver of differences (R^2 = .055), meaning it's weak, yet still noticeable. Therefore, the **null hypothesis (H_0)**, which states that privacy tools cannot effectively balance blockchain transparency with secure identity systems, is **rejected**. The **alternative hypothesis (H_1)** is **accepted**, confirming that privacy-preserving models can balance openness with security, though their impact is modest.

9.4 Objective 4 – ANOVA

Statement	p-value	Result
Implementation guidelines	0.320	Not Significant
Infrastructure compatibility	0.362	Not Significant
Fraud detection improvement	0.389	Not Significant
High implementation costs	0.145	Not Significant
Need for standard frameworks	0.435	Not Significant

Interpretation

The findings reveal none of the integration claims held statistical weight ($p > .05$). That means people generally agree about setup rules, system fits, spotting scams, expenses, also common models. On top of this, male and female opinions didn't differ - views on hurdles stayed consistent no matter the group. Because typical setups aren't viewed as clearly cutting costs or boosting connectivity, we go with the default assumption (H_0). The alternative hypothesis (H_1) gets ruled out. Still, people see integration issues in similar ways - demographics don't really shift that view.

FINDINGS

- Blockchain significantly enhances fraud detection, transparency, and data integrity.
- People feel pretty sure rules aren't clear enough.
- Scaling up affects gains a lot - also, instant data handling does too.
- The clash between privacy and openness is still tough to handle.
- No difference in how genders see things shows up.

4. CONCLUSION

Blockchain offers a powerful tool for enhancing financial security. The study confirms strong associations among AI–blockchain performance factors and highlights major regulatory and privacy issues. Adoption requires improved frameworks, energy-efficient models, and standardized regulations. The findings support most alternative hypotheses

LIMITATIONS OF THE STUDY

- Limited geographic scope is one constraint, as data were collected from respondents in a single region, which may not represent perceptions in other countries with different regulatory and technological environments**.**
- Use of convenience sampling is another limitation, since participants were selected based on ease of access, which may have excluded key stakeholders such as regulators, policymakers, or core blockchain developers**.**
- The reliance on self-reported responses may introduce bias, as respondents' answers can be influenced by personal opinions, limited technical understanding, or social desirability
- cross-sectional design captures opinions at only one point in time; given the rapid evolution of blockchain, AI, and regulations, perceptions related to scalability, privacy, and legal clarity may change significantly in the future**.**

FUTURE SCOPE OF THE STUDY

Future research can adopt longitudinal studies to track how blockchain adoption, regulatory clarity, and AI integration evolve over time. Cross-country comparative studies may examine differences in regulatory frameworks and adoption challenges across regions such as India, the US, Europe, and the Middle East. Further work can expand on advanced privacy-enhancing technologies like zero-knowledge proofs, homomorphic encryption, and federated learning to better balance transparency and data protection. Including insights from financial regulators, compliance professionals, and blockchain developers would improve practical relevance. Additionally, future studies can focus on AI–blockchain optimization models to enhance scalability, energy efficiency, and transaction performance. Overall, these directions would strengthen both theoretical understanding and real-world applicability.

References

1.Blockchain-Backed Compliance: Enhancing SOC Audits and Financial Crime Prevention with AI Authors: Saanvi Shah, Sadi Badi Year of Publish: 2024

2. AI and Blockchain Integration in Banking: A Synergistic Approach to Fraud Mitigation Author: Prem Kumar Sholapurapu Year of Publish: 2024

3. Blockchain and Cryptography in Financial Fraud Prevention Author: Dr. Ahmed Ali Year of Publish: 2021

4. CYBERSECURITY STRATEGIES FOR SAFEGUARDING CUSTOMER'S DATA AND PREVENTING FINANCIAL FRAUD IN THE UNITED STATES FINANCIAL SECTORS Author: Efijemue Oghenekome Paul, Obunadike Callistus, et al. Year of Publish: 2023

5. Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention Author: Muhammed Zakir Hossain Year of Publish: 2023

6. Effectiveness of Blockchain Technology in Preventing Financial Fraud: A Study Among Public Listed Companies in Malaysia Author: Anusha Ramesh, Meera Eeswaran Year of Publish: 2024

7. The Role of AI and Blockchain Technology in Strengthening Fraud Prevention Strategies in Finance Author: Ashraf Ali, Khan Mustafa Year of Publish: 2025

8. Forensic accounting in fraud detection and prevention: A qualitative investigation of microfinance institutions Author: Grace Osariemen Eghe-Ikhurhe, Naheed Nawazesh Roni, et al. Year of Publish: 2024

9. The Role of AI and Blockchain Technology in Strengthening Fraud Prevention Strategies in Finance Authors: Ashraf Ali, Khan Mustafa Year of Publish: 2025

10. The role of big data in detecting and preventing financial fraud in digital transactions Authors: Ezekiel Onyekachukwu Udeh, Prisca Amajuoyi, Kudirat Bukola Adeusi, and Anwulika Ogechukwu Scott Year of Publish: 2024

11. The Future of Digital Financial Security: Integrating AI, Cloud, and Big Data for Fraud Prevention and Real Time Transaction Monitoring in Payment Systems Author: Jai Kiran Reddy Burugulla Year of Publish: 2024