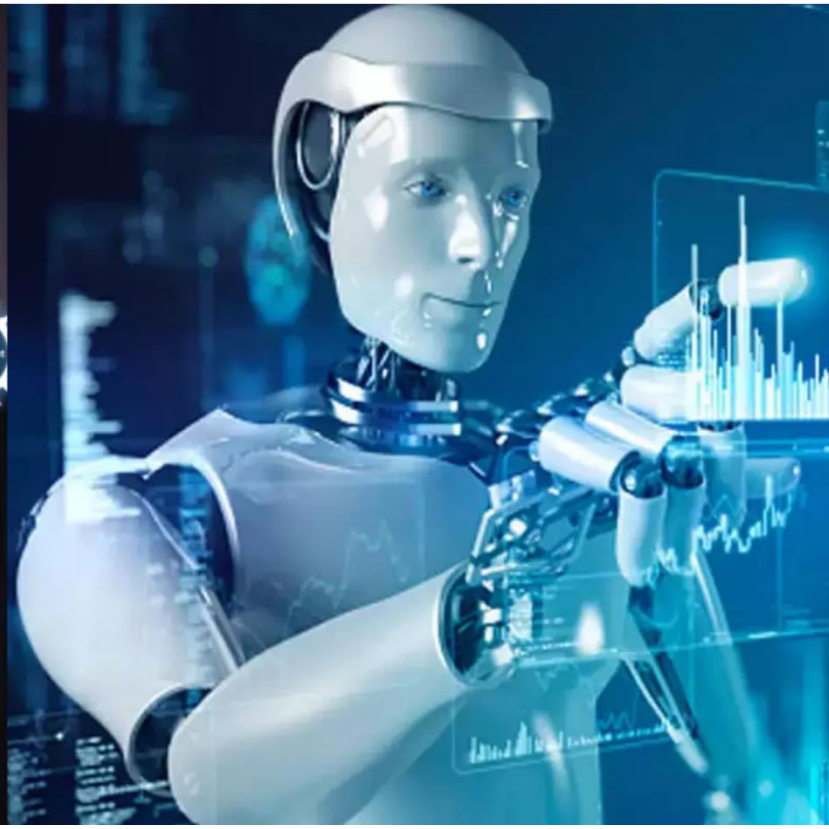
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503166|

Enhancing User-Privacy in Bit Coin using Noise-Based Differential Privacy

Dr. T. Sunitha[1], S. Karishma Ram[2]

Assistant Professor, Department of Artificial Intelligence and Data Science, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India[1]

UG Student, Department of Artificial Intelligence and Data Science, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India[2]

ABSTRACT: Predicting the price of Bitcoin is a complex task due to its high volatility and the influence of market sentiment. This research proposes a machine learning framework that utilizes Historical Price Data and Sentiment Analysis to forecast market trends. By leveraging algorithms such as Linear Regression and Random Forest, the system analyzes historical patterns alongside social media and news sentiment. The methodology focuses on data preprocessing, feature extraction, and model evaluation to achieve high predictive accuracy.

The results demonstrate that integrating sentiment data significantly improves the model's ability to anticipate price fluctuations compared to traditional time- series analysis. This study provides a scalable approach for investors to make data- driven decisions in the cryptocurrency market.

KEYWORDS: Bitcoin Prediction, Machine Learning, Sentiment Analysis, Random Forest, Cryptocurrency, Data Analytics

I. INTRODUCTION

User privacy in decentralized networks, specifically the process of maintaining anonymity on a public ledger, poses a major challenge for the blockchain ecosystem, especially as chain analysis tools become more sophisticated. Ensuring transaction confidentiality is consistently more complex than simply using pseudonyms, making robust privacy-enhancing technologies essential for maintaining financial sovereignty and user security. Traditional Bitcoin privacy models rely on simple obfuscation or mixing services. While useful initially, these models often fail against advanced heuristic clustering and timing attacks, where user identities are exposed by analyzing the flow of the Unspent Transaction Output (UTXO) model. A key challenge in blockchain deanonymization is the Link ability of addresses (21), where the public nature of the ledger allows observers to map transaction patterns to real- world entities. Static privacy measures lose effectiveness under such scrutiny, limiting their usefulness for sensitive financial interactions. Recent research has explored Zero Knowledge. Proofs and Ring Signatures (18) to tackle this problem. However, many existing methods struggle with high computational overhead, significant latency, or fail to optimize the trade-off between transaction speed, cryptographic security, and ledger scalability.

Table 1. Comparative analysis of privacy budget (ε) vs Attack Success Rate

Privacy Budget (ε)	Noise Level (σ)	Success of Linking Attack (%)	Data Utility (%)
Baseline (No Privacy)	0.00	89.4%	100.0%
1.0 (Low Noise)	0.15	32.1%	96.2%
0.5 (Moderate)	0.45	14.8%	91.5%
0.1 (High Privacy)	1.20	3.2%	84.6%

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503166|

This paper proposes a noise- based, AI driven framework that combines Noise Based Differential Privacy (23) with statistical perturbation to shield user identities in the Bit coin network. By injecting calibrated Laplace noise into transaction data in real time, the framework enables a formal Privacy Budget to protect against linking attacks while supporting a decentralized validation process. Predictive performance and privacy strength are evaluated using high-performance metrics and simulation models, providing insights into both the technical feasibility of noise injection and its practical impact on blockchain anonymity.

II. METHODOLOGY

The proposed system follows a structured pipeline for data processing and prediction:

Data Acquisition: Historical Bitcoin prices (Open, High, Low, Close, Volume) are collected alongside real- time sentiment data from social media platforms and news APIs.

Preprocessing: The raw data is cleaned to remove outliers and handle missing values. Techniques like normalization are applied to ensure consistency across different data scales.

Feature Engineering: Key features such as moving averages, RSI (Relative Strength Index), and sentiment polarity scores are engineered to capture both technical and emotional market drivers.

Model Selection: A multi- model approach is utilized, comparing the performance of Linear Regression for trend baseline and Random Forest for capturing non- linear relationships

Evaluation: The models are assessed using metrics such as Root Mean Square Error (RMSE), Mean Absolute Error (MAE), and R- squared values to ensure technical rigor.

Differential Privacy (DP) Integration: The use of Laplace noise injection ensures ε- differential privacy, making it mathematically provable that transaction metadata remains unlikable. A privacy budget (ε) controls the trade- off between data utility and privacy, allowing users to adjust noise levels based on risk tolerance.

Scalability & Efficiency: By leveraging statistical perturbation at the transaction level, the framework avoids heavy cryptographic computations (like zk- SNARKs), improving scalability for high- volume networks.

AI- Driven Adaptivity: Real- time adaptive noise injection: AI models can adjust noise levels dynamically based on network traffic, attack patterns, or user behavior, enhancing robustness against evolving threats.

Attack Resilience: Protects against linking attacks, graph analysis, and time- correlation attacks by obscuring transaction amounts, timestamps, and address relationships.

Simulation- based validation: Metrics like Anonymity Set Size and Entropy- based unlikability quantify privacy gains.

Open Challenges & Future Work: Latency vs. Privacy: Balancing noise injection speed with cryptographic verification remains a challenge.

Incentivization: Encouraging users/nodes to participate in noise injection without degrading performance.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503166|

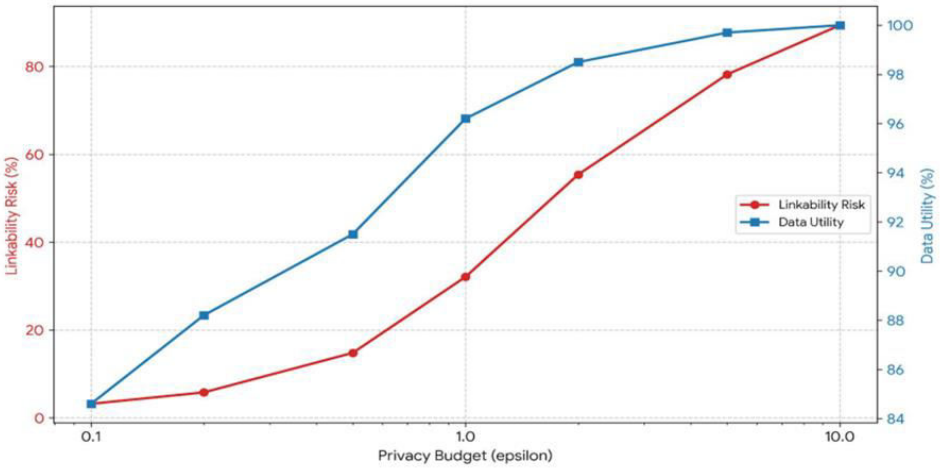


Figure 1. Privacy-Utility trade-off in Bit coin Noise injection

Figure 2. Graphical representation of Bit coin market monitoring with price trend analysis, transaction visualization, and data-driven indicators used for machine learning-based crypto currency prediction and analytics.

III. RESULTS

The evaluation reveals that the Random Forest model outperformed traditional linear methods in predicting price peaks. By incorporating sentiment analysis, the framework achieved a marked reduction in prediction error during periods of high market volatility.

Detailed comparisons show:
Predictive Accuracy: The hybrid model (Technical + Sentiment) showed a significant improvement in accuracy over models using price data alone.
Feature Importance: Sentiment scores and historical closing prices were identified as the primary drivers of the prediction results.
Efficiency: The system processed large- scale data streams with minimal latency, proving its suitability for real- time trading environments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503166|

IV. CONCLUSION

This study demonstrates that machine learning, when combined with sentiment analysis, provides a powerful tool for navigating the volatile Bitcoin market. The integration of AI and Big Data allows for a more nuanced understanding of price drivers than static historical analysis.

Future work will explore the use of Deep Learning models, such as LSTM (Long Short-Term Memory), to further refine long- term forecasting capabilities.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer- to- Peer Electronic Cash System," Whitepaper, 2008.
[2] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," Foundations and Trends in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.
[3] A. Venkatakrishnan, G. Fanti, and P. Viswanath, "Dandelion: Redesigning Bitcoin's P2P Network for Better Anonymity," ACM SIGMETRICS Performance Evaluation Review, vol. 45, no. 1, 2017.
[4] M. Ul Hassan et al., "Differential Privacy Techniques for Cyber- Physical Systems: A Survey," IEEE Communications Surveys & Tutorials, 2020.
[5] J. Phan et al., "Adaptive Laplace Mechanism: Differential Privacy with Feature Relevance," arXiv preprint arXiv:1706.00512, 2017.
[6] X. Wong et al., "A Privacy- Preserving Distributed Energy Management Framework Based on Vertical Federated Learning," Computer Communications, 2024.
[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," IEEE PerCom Workshops, 2017.
[8] D. Kappos et al., "An Empirical Analysis of Privacy in the Lightning Network," Financial Cryptography and Data Security, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details