The Intersection of Blockchain and AI in B2B Embedded Finance: A Comprehensive Review of Trends, Applications, and Future Prospects

Maharshi Patel[1], Kaivan Shah[2], Hirvraj Gohil[3]
[1]Department of Computer Science and Engineering,
NEWLJ, Gujarat Technological University,
Gujarat, India

***Abstract*—Business-to-Business (B2B) embedded finance is reshaping enterprise ecosystems by integrating financial services—such as payments, lending, and insurance—directly into non-financial platforms. The convergence of Artificial Intelligence (AI) and blockchain technologies is central to this evolution, offering enhanced security, automation, and transparency. This paper presents a comprehensive review of trends and applications at this intersection, including AI-powered fraud detection, smart contract key management, blockchain-based identity verification, and quantum-resistant encryption. Special attention is given to the role of the Hill Cipher in lightweight, matrix-based security models. We conclude by highlighting challenges and opportunities that will define the future of secure, AI-driven digital finance infrastructures [1].**

***Index Terms*—Business-to-Business (B2B) Embedded Finance, Artificial Intelligence (AI), Blockchain, Smart Contracts, Fraud Detection, Identity Verification, Quantum-Resistant Encryption, Financial Technology (FinTech), Cryptographic Security, Hill Cipher, AI-Driven Finance, Secure Digital Transactions, Enterprise Financial Ecosystems.**

I. Introduction

Business-to-Business (B2B) embedded finance is revolutionizing how enterprises interact with financial systems by enabling seamless integration of financial services like lending, payments, insurance, and investment directly into their digital platforms. Unlike traditional financial services that operate as standalone systems, embedded finance brings these capabilities into the daily operational workflows of businesses, improving user experience, streamlining operations, and enhancing customer retention.

As we move deeper into the digital economy, the demand for frictionless, secure, and intelligent financial infrastructure has intensified. Enterprises now expect financial services that are not only embedded and contextual but also responsive and predictive. This demand is being met through the convergence of blockchain and Artificial Intelligence (AI) technologies [2].

Blockchain provides a decentralized, tamper-proof ledger for recording transactions, enhancing transparency, trust, and auditability. AI contributes its strengths in data analysis, pattern recognition, and autonomous decision-making, enabling real-time fraud detection, credit scoring, and financial forecasting. When these technologies are combined and underpinned by robust cryptographic mechanisms—such as the Hill Cipher and emerging post-quantum encryption—they create a comprehensive framework for secure, intelligent, and scalable B2B financial ecosystems [3].

This paper explores the integration of blockchain and AI in B2B embedded finance, discussing how these technologies are used for encryption, identity verification, fraud prevention, and smart contract automation. The goal is to provide a broad yet detailed view of the state-of-the-art innovations and the challenges that lie ahead as we enter a new phase of enterprise finance.

II. B2B Embedded Finance Infrastructure Trends in 2025

Key infrastructure trends in 2025 are revolutionizing B2B finance through scalable, secure, and intelligent solutions. These trends reflect the growing need for modular, compliant, and adaptive systems capable of handling real-time, high-volume financial operations:

- **Composable Finance:** Modular financial services are being built using APIs and microservices, allowing companies to plug-and-play different capabilities such as lending, KYC, or insurance directly into their platforms without developing them from scratch. These composable architectures empower businesses to remain agile and innovate at a faster pace [4].
- **Decentralized Finance (DeFi) Integration:** DeFi is now interacting with traditional B2B platforms. Protocols like Aave and Compound are being adapted into permissioned environments where businesses can participate in lending/borrowing while maintaining regulatory compliance. This hybrid approach ensures both innovation and trust [5].
- **AI-Powered Analytics:** Financial dashboards embedded within enterprise software use AI for pattern recognition, anomaly detection, and forecasting. Predictive models help businesses optimize cash flow, reduce risk, and improve decision-making in real time. Machine learning algorithms also assist in personalized credit assessment and transaction categorization [6].
- **Tokenized Commercial Assets:** Commercial documents—like invoices, bills of lading, and trade credits—are being tokenized on blockchain networks. These

tokenized assets improve liquidity by enabling real-time settlement, automated compliance checks, and programmable asset behavior. Smart contracts enforce logic around ownership transfer, payment release, and dispute resolution [7].

- **Permissioned Ledgers:** Enterprises are moving away from public blockchains to permissioned ledgers such as Hyperledger Fabric or Quorum. These platforms ensure privacy, offer better governance controls, and enable selective data visibility for stakeholders. They are particularly suited for industries requiring high auditability and secure collaboration [8].
- **Event-Driven Architecture:** Traditional batch-processing is being replaced by real-time, event-driven architecture. This shift enables instantaneous transaction processing, fraud detection, and regulatory reporting, aligning well with the just-in-time needs of modern B2B operations. Event brokers like Apache Kafka facilitate these real-time integrations.

These developments are not only enhancing operational agility but also enabling hyperautomation—where AI and blockchain automate entire financial processes, reducing manual interventions, improving accuracy, and significantly lowering the risk of fraud. As businesses continue to digitalize, these infrastructure components will play a central role in shaping the financial technology landscape of 2025 and beyond.

III. Secure Transaction Encryption

Secure encryption of financial transactions is fundamental in preventing data breaches, fraud, and unauthorized access. In the landscape of B2B embedded finance, encryption ensures confidentiality, integrity, and non-repudiation across decentralized financial systems.

A. Data Integrity and Blockchain Security

The Hill Cipher, a matrix-based symmetric encryption algorithm, offers lightweight and efficient encryption, making it suitable for blockchain environments. By encrypting transaction records before storage on distributed ledgers, the Hill Cipher minimizes computational overhead while preserving data confidentiality and integrity. This method is especially advantageous in cross-border B2B payments, where performance and security are paramount [3].

In practice, the cipher ensures that each transaction remains immutable and tamper-proof, safeguarding against unauthorized access even within permissioned networks. Because the algorithm supports parallel processing and matrix operations, it is scalable to enterprise-grade volumes.

B. Use Case: Cross-border B2B Payments

Cross-border financial exchanges often require enhanced privacy due to regulatory differences and sensitive business data. Employing the Hill Cipher in permissioned blockchain networks enhances both data security and operational speed. It ensures encrypted payloads are only accessible to authorized participants and compliance auditors, maintaining trust among international trade partners.

C. Man-in-the-Middle (MITM) Attack Prevention

Matrix-based encryption techniques can also play a vital role in preventing MITM attacks—where attackers intercept or alter communications between two parties. In AI-driven systems, secure communication endpoints must be enforced. By combining encryption with endpoint verification protocols, businesses can confirm the identities of transaction participants.

This is especially useful when deploying smart contracts that automate payments and asset transfers. Verifying each endpoint reduces the risk of adversarial intervention and increases confidence in machine-to-machine transactions.

IV. Key Management in Smart Contracts: Theoretical Underpinnings

Smart contracts, as self-executing agreements with the terms directly written into code, necessitate robust key management strategies to ensure security and trust, especially in complex B2B financial ecosystems. The theoretical foundations of key management in this context draw from several cryptographic and distributed systems principles [9].

A. Lightweight Cryptography and Resource Constraints

The application of lightweight cryptography, specifically matrix-based ciphers like the Hill Cipher, addresses the inherent resource constraints of blockchain environments. Traditionally, cryptographic operations are computationally intensive, which poses a challenge for smart contracts deployed on blockchains with limited computational resources.

Theoretical Basis: * **Computational Complexity:** The theoretical efficiency of matrix-based ciphers stems from their linear algebraic structure. The operations involved, such as matrix multiplication and inversion, have well-defined computational complexities. In the case of the Hill Cipher, the complexity is primarily determined by the matrix size, allowing for predictable performance.

* **Security Trade-offs:** Lightweight cryptography inherently involves trade-offs between security strength and computational efficiency. The theoretical analysis of these trade-offs is crucial. For instance, the security of the Hill Cipher relies on the secrecy of the key matrix and the difficulty of inverting it. Research in linear algebra and cryptography provides tools to analyze the security margins and potential vulnerabilities [3].

* **Homomorphic Properties:** Some matrix-based cryptographic schemes can be designed with partial homomorphic properties, allowing computations to be performed on encrypted data without decryption. This is theoretically significant for enabling privacy-preserving smart contract operations, where data confidentiality is maintained even during computation.

* **Information Theory:** Information-theoretic security principles are applied to analyze the entropy of the key matrix and the amount of information leaked during encryption. Shannon's theory of perfect secrecy provides a framework for evaluating the theoretical limits of security in these schemes.

B. Multi-Signature Verification and Distributed Trust

Multi-signature (multi-sig) schemes are fundamental for establishing distributed trust in smart contracts. They rely on the concept of threshold cryptography, where a certain number of parties must cooperate to authorize a transaction.

Theoretical Basis: * **Threshold Cryptography:** The theoretical foundation of multi-sig schemes lies in threshold cryptography, which ensures that no single party can unilaterally control a transaction. The security of these schemes is based on the difficulty of solving systems of linear equations or discrete logarithm problems [10].

* **Byzantine Fault Tolerance (BFT):** In distributed systems, BFT algorithms are used to ensure consensus in the presence of malicious actors. Multi-sig schemes can be integrated with BFT protocols to enhance the resilience of smart contracts against attacks. The theoretical analysis of BFT protocols provides insights into the fault tolerance and security properties of these integrated systems.

* **Game Theory:** Game theory is used to model the interactions between multiple parties in a multi-sig scheme. It can be used to analyze the incentives and strategies of participants, ensuring that the scheme is robust against collusion and strategic behavior.

* **Digital Signature Schemes:** The underlying digital signature schemes used in multi-sig mechanisms are based on cryptographic primitives like RSA or elliptic curve cryptography. The theoretical security of these schemes is rigorously analyzed using number theory and computational complexity theory.

C. Supply Chain Finance: A Systemic Perspective

The application of key management in supply chain finance involves the integration of cryptographic techniques with business logic and distributed systems principles.

Theoretical Basis: * **Formal Methods:** Formal methods, such as process calculi and temporal logic, can be used to model and verify the correctness and security of smart contracts in supply chain finance. These methods provide a rigorous framework for analyzing the behavior of the system and identifying potential vulnerabilities [11].

* **Distributed Ledger Technology (DLT):** The theoretical properties of DLT, such as immutability and transparency, are crucial for ensuring the integrity of supply chain transactions. Research in distributed systems provides insights into the scalability, security, and performance of DLT-based systems [1].

* **Secure Multi-Party Computation (SMPC):** SMPC techniques are used to enable secure computation on sensitive data without revealing it to any single party. The theoretical security of SMPC protocols is based on cryptographic assumptions and information-theoretic principles.

* **Contract Theory:** Contract theory from economics provides a framework for analyzing the design and enforcement of smart contracts. It can be used to model the incentives and risks of participants in a supply chain and to design contracts that promote efficiency and fairness.

In essence, the theoretical underpinnings of key management in smart contracts are multifaceted, drawing from cryptography, distributed systems, formal methods, game theory, and economics. These theoretical foundations provide a rigorous framework for designing and analyzing secure and reliable smart contract systems in B2B financial ecosystems.

V. AI-POWERED FRAUD DETECTION AND PRIVACY: THEORETICAL FRAMEWORK

The convergence of AI-driven fraud detection and stringent privacy requirements in embedded finance necessitates a robust theoretical framework that balances analytical efficacy with data confidentiality [6].

A. Encrypted AI Model Training: Homomorphic Encryption and Secure Computation

Training AI models on encrypted datasets, especially using matrix-based ciphers like the Hill Cipher, leverages principles of homomorphic encryption and secure multi-party computation (SMPC). The theoretical foundation rests on the concept of homomorphic encryption, which allows computations to be performed on encrypted data without decryption. While the Hill Cipher exhibits limited homomorphic properties, its matrix structure can be adapted for specific computational tasks on encrypted data. The theoretical analysis of these properties involves exploring the algebraic structures that preserve computational operations under encryption. Training AI models on encrypted data can be viewed as a form of SMPC, where multiple parties contribute data without revealing it. The theoretical security of SMPC protocols is based on cryptographic assumptions and information-theoretic principles. This involves rigorous proofs of security against various attack models, including semi-honest and malicious adversaries. The theoretical limits of privacy are often analyzed using information-theoretic measures, such as differential privacy and mutual information. These measures quantify the amount of information leaked during the training process and provide a framework for designing privacy-preserving algorithms. The computational complexity of training AI models on encrypted data is a critical theoretical consideration. This involves analyzing the overhead introduced by encryption and decryption operations and designing efficient algorithms that minimize this overhead.

B. Secure Federated Learning: Distributed Optimization and Differential Privacy

Federated learning (FL) enables collaborative training of AI models without centralized data sharing, addressing privacy concerns. Integrating matrix-based encryption into FL enhances confidentiality during cross-institution model updates. FL relies on distributed optimization algorithms, such as federated averaging, to train models across decentralized data sources. The theoretical convergence properties of these algorithms are crucial for ensuring the accuracy and efficiency of the trained models. This involves analyzing the convergence

rates and stability of the algorithms under various data distributions and communication constraints. To ensure data privacy, FL often incorporates differential privacy mechanisms, which add noise to model updates to prevent the leakage of sensitive information. The theoretical analysis of DP involves quantifying the trade-off between privacy and accuracy and designing mechanisms that provide strong privacy guarantees without significantly degrading model performance [12].

Integrating matrix-based encryption into FL involves cryptographic aggregation techniques, which allow multiple parties to securely combine their model updates without revealing their individual contributions. The theoretical security of these techniques is based on cryptographic assumptions and protocols, such as secure aggregation and homomorphic encryption. In real-world FL scenarios, some participants may be malicious or unreliable. Byzantine resilience is a theoretical property that ensures the robustness of the FL system against these participants. This involves designing algorithms and protocols that can tolerate Byzantine failures and ensure the convergence of the model.

Use Case: AI-based Credit Risk Models and GDPR Compliance

Training AI-based credit risk models on encrypted financial records from multiple businesses involves the application of the theoretical principles discussed above. The financial records from different businesses may exhibit significant heterogeneity, which poses a challenge for training accurate and generalizable models. Theoretical analysis of domain adaptation and transfer learning techniques is crucial for addressing this challenge. GDPR and other data privacy regulations impose strict requirements on the processing of personal data. The theoretical framework for privacy-preserving AI models must incorporate these requirements and provide formal guarantees of compliance. Credit risk models are vulnerable to adversarial attacks, which aim to manipulate the model's predictions. The theoretical analysis of adversarial robustness and defense mechanisms is crucial for ensuring the security and reliability of these models. AI models used for credit risk assessment must be fair and unbiased. Theoretical analysis of fairness metrics and bias mitigation techniques is crucial for ensuring equitable outcomes [15].

VI. BLOCKCHAIN-BASED IDENTITY VERIFICATION

Secure digital identity is paramount in B2B finance, especially regarding KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance. Traditional identity verification methods are often centralized, prone to data breaches, and cumbersome, leading to inefficiencies and increased risks. Blockchain and AI offer a potent combination for creating robust and privacy-preserving identity verification systems [13].

A. Decentralized Identity Frameworks

Blockchain-based digital identity systems provide a paradigm shift from centralized identity management to decentralized, user-centric models. These systems leverage the inherent properties of blockchain technology, such as immutability, transparency, and cryptography, to create secure and verifiable digital identities. Decentralized Identifiers (DIDs) are a core component of these frameworks, serving as globally unique identifiers that do not rely on centralized registries. The theoretical foundation of DIDs lies in their ability to provide verifiable, self-sovereign identities, employing cryptographic techniques to ensure tamper-proofness and data security. Verifiable Credentials (VCs) are digital representations of identity attributes or qualifications, cryptographically signed and independently verifiable. Their theoretical basis is rooted in digital signature schemes and public-key cryptography, facilitating secure issuance and verification without centralized authorities. Zero-Knowledge Proofs (ZKPs) enable the verification of information without revealing underlying data, crucial for privacy-preserving identity verification. The theoretical security of ZKPs is based on cryptographic assumptions and computational complexity theory, ensuring information verification without compromising user privacy. Blockchain acts as a distributed ledger, providing a trust anchor for identity data. The immutability and transparency of blockchain ensure secure storage and verifiability of identity data, with theoretical analysis of blockchain's security properties providing insights into system resilience against attacks.

B. AI-Driven Verification

AI algorithms can significantly enhance the efficiency and accuracy of identity verification processes. By leveraging machine learning techniques, AI can analyze encrypted identity data and detect anomalies that might indicate fraudulent activity. AI algorithms, such as anomaly detection models, identify patterns and deviations in identity data indicative of fraudulent activity. The theoretical foundation of these models lies in statistical learning theory, which provides a framework for analyzing performance and robustness. AI algorithms can be designed to operate on encrypted data or incorporate privacy-preserving techniques like differential privacy, protecting identity data during verification. The theoretical analysis of privacy-preserving AI involves quantifying the trade-off between privacy and accuracy. AI-driven biometric verification, such as facial recognition and fingerprint analysis, enhances identity verification accuracy. The theoretical foundation of these techniques lies in pattern recognition and image processing, providing a framework for analyzing performance and robustness. Natural Language Processing (NLP) techniques analyze identity documents and extract relevant information, automating processes and improving accuracy. The theoretical foundation of NLP is computational linguistics, which provides a framework for analyzing performance and robustness.

Use Case: Automated KYC Systems in B2B Finance Automated KYC systems in B2B finance leverage blockchain and AI to securely verify suppliers, reducing onboarding time and fraud. Suppliers can use a decentralized identity framework to create and manage their digital identities, including

verifiable credentials like business registration documents, financial statements, and compliance certifications. When a B2B platform onboards a new supplier, it can request the supplier's digital identity. The platform then uses AI algorithms to verify the authenticity of the verifiable credentials and detect anomalies indicative of fraudulent activity. The platform can use zero-knowledge proofs to verify specific attributes of the supplier's identity without revealing underlying data, such as verifying registration in a specific jurisdiction without revealing full registration details. The use of blockchain ensures secure storage and verifiability of the supplier's identity data, enhancing trust and transparency. This process significantly reduces onboarding time, costs, and the risk of fraudulent activities, while ensuring compliance with KYC and AML regulations.

VII. Quantum-Resistant Encryption

Quantum computing poses a significant threat to the security of traditional encryption algorithms such as RSA and ECC, which are widely used in current B2B financial systems. This threat necessitates the development and implementation of quantum-resistant encryption solutions to ensure the long-term security of financial transactions and data [14].

A. Hybrid Cryptographic Models

Combining the Hill Cipher with post-quantum algorithms like lattice-based cryptography offers a promising approach to achieving quantum resistance in B2B finance. This hybrid model leverages the lightweight nature of the Hill Cipher for efficient encryption and decryption while incorporating the robust security of lattice-based cryptography, which is designed to withstand quantum attacks. The integration of these two cryptographic approaches allows for the creation of a secure and efficient encryption system that can protect sensitive financial data in a post-quantum future. The Hill Cipher provides a rapid, matrix based encryption layer, that can be implemented in a hybrid model, in order to reduce overhead from the more computationally expensive post quantum algorithms. This results in a system that maintains required speed for financial transactions, while still offering the required security.

B. Secure Tokenization of Assets

The tokenization of assets, such as invoices, credit, and equity, on blockchain platforms is becoming increasingly prevalent in B2B finance. These tokenized assets represent valuable financial instruments, and their ownership records must be protected from quantum attacks. Encryption of these ownership records using matrix cryptography, especially when combined with post quantum cryptographic methods, provides a robust solution. This approach ensures that the integrity and confidentiality of tokenized asset ownership are maintained, even in the face of advanced quantum computing capabilities. By encrypting ownership records, unauthorized access and manipulation of these assets can be prevented, thereby safeguarding the financial interests of all stakeholders involved.

Use Case: Trade Finance Platforms Trade finance platforms utilizing hybrid encryption models can securely tokenize and transfer digital assets even in a post-quantum future. In trade finance, where complex financial transactions and asset transfers occur between multiple parties, the security of these transactions is paramount. By implementing hybrid encryption, these platforms can ensure that all sensitive information, including asset ownership records, transaction details, and contractual agreements, are protected from quantum attacks. This allows for the continued use of blockchain technology in trade finance, enabling secure and efficient asset tokenization and transfer. The use of hybrid cryptographic systems, ensures that even as quantum computing evolves, the security and integrity of these systems are maintained. This allows for the continued growth and innovation of trade finance platforms, without fear of security breaches, and allows for global trade to continue with confidence in the security of the underlying systems.

VIII. Future Prospects and Challenges

The future of B2B embedded finance is poised to advance through trustless automation, privacy-preserving analytics, and quantum-safe infrastructure. This evolution, however, is not without its challenges. A primary hurdle lies in the standardization of AI-blockchain interoperability protocols. As AI and blockchain technologies become increasingly integrated within financial systems, establishing uniform communication and data exchange standards is crucial for seamless operation and widespread adoption. Without these standards, systems may struggle to communicate effectively, leading to inefficiencies and security vulnerabilities. Another significant challenge is the development and implementation of scalable post-quantum cryptography for real-time finance. Traditional cryptographic methods are vulnerable to quantum computing, and the need for quantum-resistant solutions that can operate at the speed required for financial transactions is paramount. This will require significant research and innovation in cryptographic algorithms and hardware [14]. Finally, cross-border regulatory harmonization presents a complex challenge. As B2B embedded finance operates on a global scale, aligning diverse regulatory frameworks across jurisdictions is essential for ensuring compliance and fostering international trust. This harmonization will require collaboration among regulatory bodies worldwide and the development of adaptable regulatory frameworks that can accommodate the rapidly evolving landscape of embedded finance.

IX. Conclusion

This paper explored the transformative potential of integrating AI, blockchain, and advanced cryptographic techniques within the B2B embedded finance ecosystem. Findings indicate that matrix-based cryptography, exemplified by the Hill Cipher, provides effective lightweight encryption solutions for secure data handling, robust identity verification, and efficient fraud detection, particularly in resource-constrained blockchain environments. The necessity of quantum-resistant

cryptographic strategies was highlighted, advocating for hybrid models combining matrix encryption with post-quantum algorithms to safeguard against future threats. Furthermore, the paper detailed the application of secure federated learning and decentralized identity frameworks to enhance privacy and compliance in AI-driven financial operations. Addressing future challenges, such as the standardization of AI-blockchain interoperability and the harmonization of cross-border regulations, is crucial for realizing the full potential of these integrated systems. Future research should focus on developing standardized frameworks that seamlessly merge AI models, secure federated learning, and permissioned blockchains to create secure, compliant, and intelligent financial ecosystems, thereby fostering trust and efficiency in B2B transactions [4].

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.

[3] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

[4] Tapscott, D., Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Portfolio Penguin.

[5] Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review.

[6] Goodfellow, I., Bengio, Y., Courville, A. (2016). Deep Learning. MIT Press.

[7] Buterin, V. (2014). Next-Generation Smart Contracts: A Survey of Technical Topics for Future Consideration. Ethereum White Paper.

[8] Cachin, C., Vukolić, M. (2016). Blockchain Consensus Protocols in the Wild. IBM Research.

[9] Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper.

[10] Shoup, V. (2000). Practical Threshold Signatures. Eurocrypt.

[11] Lamport, L. (1978). Time, Clocks, and the Ordering of Events in a Distributed System. Communications of the ACM.

[12] McMahan, H. B., et al. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS.

[13] Ferretti, S., D'Angelo, G. (2019). Decentralized Identity Management on Blockchain for Privacy and Security. IEEE Access.

[14] Bernstein, D. J., Lange, T. (2017). Post-Quantum Cryptography. Springer.

[15] Lipton, Z. C. (2016). The Mythos of Model Interpretability. arXiv preprint arXiv:1606.03490.

[16] Russell, S., Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson.

[17] Gunning, D. (2019). DARPA's Explainable Artificial Intelligence Program. AI Magazine, 40(2), 44-58.