Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

BLOCKCHAIN-BASED FRAUD PREVENTION IN THE U.S. FINANCIAL SECTOR: A LITERATURE REVIEW

Oluwatosin Oladokun[1], Matthew Oman-Amoako[2]
[1]*Haas School of Business, University of California, Berkeley, Berkeley, CA, USA*
[2]*Department of Business Administration, Accra Institute of Technology, Ghana*

Article DOI: https://doi.org/10.36713/epra26558
DOI No: 10.36713/epra26558

ABSTRACT

Every year, financial institutions lose billions of dollars and public trust undermined since fraud remains a continuous challenge in the U.S. financial industry. Conventional mechanisms of fraud prevention such as compliance checks, manual audits, and transaction monitoring, have proven effective but insufficient due to their inefficiencies, delayed detection, and susceptibility to vulnerability. There is now a transformative approach to mitigating fraud incidences due to blockchain technology through its features of immutability, consensus-driven validation, transparency, and programmability via smart contracts. This paper reviews the application of blockchain in fraud prevention across banking, insurance, payments, and securities sectors, highlighting case studies of JPMorgan Chase, AIG, Visa, Mastercard, MetLife, NASDAQ, and others. It also examines regulatory and policy developments by agencies such as the Treasury, OFAC, FinCEN, and state-level regulators. Some of the key opportunities associated with blockchain are Know Your Customer (KYC) and Know Your Business (KYB) compliance, provenance verification, tokenized asset ecosystems, and automated fraud controls. There remain significant challenges in scalability, governance ambiguity, uncertainty to regulations, privacy conflicts with data protection laws, and smart contract vulnerabilities. The review concludes that blockchain provides robust tools for fraud detection and prevention but is not a panacea. Future research should explore the integration of blockchain with artificial intelligence (AI) and machine learning (ML), fraud detection models through privacy-preserving, regulatory harmonization, and cost–benefit analyses. By addressing these gaps, blockchain can evolve into a cornerstone of fraud prevention strategies within the U.S. financial sector.

KEYWORDS: *Blockchain Technology, Fraud Prevention, Financial Institutions, Machine Learning, Artificial Intelligence*

1. INTRODUCTION

In the United States financial services industry, fraud remains a systemic problem that costs billions of dollars every year and erodes trust in institutions. Based on the Association of Certified Fraud Examiners (ACFE, 2024), organizations lose, on average, about 5% of their annual revenues to fraudulent conduct, including asset misappropriation, financial statement fraud, and corruption. Traditional fraud-prevention tactics, including checks for compliance, manual audits, transaction monitoring, and regulatory scrutiny, have been employed by organizations, all of which have met with varying degrees of success; yet, they are still exposed to late detection, human errors, and intentional failures. These vulnerabilities indicate the critical need for new methodologies that improve and facilitate real-time transaction monitoring, verification, security, and transparency. With its fundamental properties, including immutability, decentralization, consensus-based validation, and programmability through smart contracts, blockchain has the potential to significantly impact the recording, verification, and auditing of financial data (National Institute of Standards and Technology [NIST], 2018). The literature suggests that companies embracing blockchain are likely to experience increased efficiency in trade processing, reduced risk and improved transaction transparency (Yoo, 2017; Zheng et al., 2018). With growing interest and adoption of blockchain, it has also become a strategic priority for financial institutions looking to build resilience, reliability and trust in the digital economy.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

2. LITERATURE REVIEW

Blockchain is hailed as one of the Fourth Industry Revolution technologies along with inventions such as the steam engine, electricity, and information technology (Chung & Kim, 2016). They noted that blockchain generated so much attention in the early years because, securely and reliably, Bitcoin was working and demonstrating the reliability of the underlying infrastructure. Developers and entrepreneurs could see that blockchain could be applied generally, rather than just in the field of currency, to other economic and social areas, after the recognition of Bitcoin's stability. The blockchain was initially described in 2008 by Nakamoto in the Bitcoin white paper as the underlying infrastructure of cryptocurrency (Nakamoto, 2008). The terms Bitcoin and blockchain were used interchangeably in their early stages. But this perception has shifted since around 2014, when academic scholars and business practitioners recognized blockchain as an independent infrastructure with applications that reach far beyond just currency (Casino et al. Today, this technology is finding application in a wide variety of fields, such as in power finance, supply chain management, Internet-of-Things (IoT), authentication, identity management, and data management (Casino et al., 2018). Blockchain is basically a decentralized ledger system, part of a promising class of technologies known as distributed ledger technology (DLT). Instead of being verified by a centralized third party, blockchain transactions are confirmed by consensus mechanisms. This mechanism improves the integrity, transparency, anonymity, and security of data due to the whole network being responsible for maintaining and checking the ledger (Yli-Huumo et al., 2016). These technical features are the reasons why blockchain is well-suited for fraud protection. It is unchangeable, which means that once information is recorded, it cannot be altered without the changes being noticed by others. The fact of being a transparent design means that auditable logs can be made available to authorized concerned parties. And across the board, consensus-based validation minimizes the chance of collusion and fraud. These properties combined make blockchain an appealing ingredient towards enhancing trust and security in financial markets.

3. BLOCK CHAIN TECHNOLOGY AND FRAUD PREVENTION

Block chain technology establishes a distributed ledger of transactions, which is resistant to tampering because transactions cannot be altered after the fact without being detected (NIST, 2018). These organizations present little scope for false record keeping, accounting chicanery, and insider shenanigans. For the financial sector, blockchain has potential for control over fraud through the use of tamper-evident audit trails, multi-signature authorization, and smart contracts pinpointing controls such as escrow, time locks.

Fraud is a pressing issue for both accounting and finance, causing serious problems and losses both financially and with regard to regulation and reputation. Traditional fraud detection systems are often predicated on centralization, with its inherent susceptibility to manipulation, inefficiency, and late reporting. The decentralized, transparent and immutable characteristics make the blockchain technology an alternative that would transform fraudulent activities in accounting and finance.

4. CASE STUDIES OF BLOCK CHAIN IN FRAUD PREVENTION IN THE U.S. FINANCIAL SECTOR

Fraud in the US financial industry takes a broad range of shapes from duplicate invoicing and securities misreporting to insurance claims manipulation and cyber extortion. Blockchain has been explored and adopted in various sectors to mitigate these vulnerabilities. The below case studies explain how the fraud incidences occurred, how detection was realized, and the role of blockchain as a preventive mechanism.

4.1 The Banking Industry: JPMorgan Chase and Payment Verification in Blockchain

Blockchain has been used by JPMorgan Chase through its Onyx platform for better fraud detection and more efficient settlement in interbank transfers. The system leverages distributed ledger technology (DLT) to record high-value transactions, creating immutable audit trails that can be used to detect anomalies like transaction duplication and unauthorized access. JPMorgan used blockchain to detect and block a fraudulent transfer request in its wholesale payments business, where it raised a fraudulent transaction alert during cross-border settlement (J.P. Morgan, 2021). Identification was based on live reconciliation at nodes, and prevention relied on the compliance check which was operated electronically by smart contracts.

4.2 Insurance Industry: American International Group (AIG) and International Business Machine (IBM) Blockchain

AIG and IBM tested out a blockchain product that provided one platform for multinational insurance coverage. Insurance fraud is often associated with fictitious claims and the double-gambling of policies in different states. By writing policy data to a shared ledger to which the regulators, reinsurers, and counterparties had access, blockchain advances visibility of what was occurring within the company (IBM 2017). False duplicate claims were identified as blockchain nodes that identified eligibility and claims that have already been verified and adjudicated. Fraudulent payouts were less feasible as there was some sort of detection and protection built into smart contracts that automated the checks of the claims.

4.3 Payments Industry: Visa and Mastercard Blockchain Efforts

Visa and Mastercard have also integrated blockchain technologies for fraud detection in their payment networks. Visa's enterprise cross-border payments exchange (Visa B2B Connect) through blockchain technology is a platform to provide secure and fast corporate payments across borders and minimize fraud associated with invoice alteration (Visa, 2019). At the time of verification, the differences were identified as likely attempts at fraud, using blockchain validation.

Mastercard also conducted blockchain pilots in trade finance and supply chain payments and detected inconsistencies such as payments not aligning with contractual commitments stored on chain (Mastercard, 2020). Prevention was enabled through automatic reconciliation, minimizing settlement times as well as payment fraud.

4.4 Policy and Regulatory Views on the Role of Blockchain in U.S. Financial Compliance

To date the United States legal and regulatory approach to blockchain in the financial sector has allowed and, in many ways, fostered the technological innovation that is underway. This article provides an overview of the United States regulatory framework that governs blockchain in the financial sector. Some of these regulatory authorities both at state and national level which some include the Financial Crimes Enforcement Network (FinCEN) and the New York Department of Financial Services (NYDFS) have taken a hybrid of enforcement, supervisory, and policy actions to address such risks.

4.5 Treasury's Illicit-Finance Strategy

The *Treasury's 2024 National Illicit Finance Strategy* highlights blockchain analytics as a principal regulatory mechanism, particularly in identifying weaknesses across cryptocurrency mixers, decentralized finance (DeFi) protocols and cross-chain bridges (U.S. Department of the Treasury, 2024a). Detection is accomplished via blockchain trace, aiding in the identification of typologies such as double invoicing and mixer abuse." (U.S. Department of the Treasury, 2023).

Prevention is based on mandating those financial institutions build-in blockchain analytics into CDD, transaction-monitoring, and suspicious-activity-reporting programs (NYDFS, 2022).

4.6 Office of Foreign Assets Control (OFAC) and the Tornado Cash Case

In 2022, OFAC has designated Tornado Cash, a mixing service based on a blockchain, for its role in laundering money stolen by North Korean hackers (US Department of the Treasury, 2022). Free associate Noteworthy blockchain evidence connected the mixer inflows and outflows to wallets that could be tied to the Lazarus group.

However, in March 2025, Tornado Cash was taken off the sanctions list by OFAC following legal challenges to the argument that immutable smart contracts were "property" under the International Emergency Economic Powers Act (CoinDesk, 2025; OFAC, 2025). Even after being removed from the list, banks must continue keeping an eye on their mixed exposure and still report suspicious activity and halt all transactions with sanctioned parties.

4.7 FinCEN and the BSA/AML Framework FinCEN is the U.S. administrative body responsible for administering BSA

FinCEN's 2019 Convertible Virtual Currency (CVC) Guidance indicates that a broad range of crypto businesses are money transmitters under the BSA, encompassing exchanges, wallets, and some DeFi platforms (FinCEN, 2019).

Detection is based on supervisory reviews and SAR filings that are often prompted by the detection of high-risk mixers or layered transactions through analytics. To avoid abuse, FinCEN implements the "Travel Rule", which demands the sharing of originator and beneficiary information on cryptocurrency transfers. This measure decreases the anonymity of cross-border payments (FinCEN, 2019).

In later years, FinCEN put forward more rules. In 2023, it labeled crypto mixers as a "primary money laundering concern" via Section 311 of the USA PATRIOT Act, which mandates increased reporting (FinCEN, 2023). Reporting requirements for beneficial ownership were established in 2024 (FinCEN, 2024), which further improves transparency in crypto transfers.

4.8 Bank Safety and Soundness Oversight

The Federal Reserve, OCC, and FDIC In January 2023 issued joint guidance on the risks of exposure to crypto assets in the banking system. The cover stressed vulnerabilities toward the effects of volatility, liquidity risks and fraud, and foster model for contagion, including (gains, stabilelnaoncec) osnant (FederalReserve, OCC, & FDIC, 2023).

Suspicion arises from ripple effects from risk assessments, or vendor oversight, or monitoring. Risk management responses include establishing risk appetite parameters for digital assets like quantitative metrics, pulling blockchain exposures into scenario planning and stress testing, managing reliance on 3rd-party service providers (FDIC, 2023).

4.9 State-Level Regulation: NYDFS

The New York Department of Financial Services (NYDFS) requires virtual currency businesses that are licensed to incorporate blockchain analytics into CDD, transaction monitoring, and sanctions compliance (NYDFS, 2022).

In November 2023, NYDFS issued new governance standards on coin listing and delisting that require institutions to consider fraud, liquidity, and sanctions risks (NYDFS, 2023). Detection is realized via 'supervisory' blockchain tracing tests, and Prevention is supported by strict listing policies which limit fraudulent/noncompliant activity.

4.10 Corporate Transparency Act (CTA) and Ultimate Beneficial Ownership

In addition to blockchain-specific regulations, in 2024, the Corporate Transparency Act (CTA) ushered in beneficial ownership information (BOI) reporting mandates. These were intended to take down shell companies which were frequently employed to hide dirty money (FinCEN, 2024).

Detection caused by matching BOI filings and blockchain-based transaction forensics. The solution lies in reinforcing KYC/KYB Account Opening to allow institutions to tie down Blockchain activity to verified BOs.

4.11 Block chain Uses in Financial Services

Banks piloting and implementing blockchain used to increase regulation and transparency of fraudulent behavior. In the United States blockchain establishments and fraud watchdogs have been examining efficient means by which digital ledger technology (DLT) can be used to increase regulation and make the reporting of fraudulent behavior easier for regulators. Such used cases range from KYC/KYB compliance and provenance and audit trails to tokenized assets with embedded controls, fraud prevention and insurance fraud.

5. KNOW YOUR CUSTOMER (KYC) AND KNOW YOUR BUSINESS (KYB) COMPLIANCE

With blockchain, establishments can anchor their customers' verified identities on a shared ledger, no longer needing to repeat the compliance processes and securely mitigate the risk of consumer impersonation and identity fraud. Once a customer's identity is confirmed, other institutions can trust the on-chain record and reuse the on-boarded party.

Pilots, including those utilizing R3 Corda platform, reportedly have shown the ability to simplify BSA compliance and reduce costs related to synthetic identity fraud. Blockchain increases the trust of the KYC/KYB checks and lowers regulatory risk by making a tamper-proof record of verified identities (Aite Group, 2021; IBM Blockchain, 2023).

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

6. PROVENANCE AND AUDIT TRAILS

Immutability of the blockchain increases audit ability, giving credit providers an irreproachable transaction history to reduce fraud, such as double pledging of collateral, and reporting fraud.

Drawing on operational decentralization, banks such as Wells Fargo and HSBC have adopted blockchain for settlement of foreign exchange (FX) trades experimenting with blockchain to mitigate settlement risk, and the Depository Trust & Clearing Corporation (DTCC) used blockchain for derivatives reporting to guarantee the accuracy and immutability of data generation sources (DTCC, 2020; Reuters, 2019).

Through the creation of permanent, transparent ledgers and permanent, tamper-proof ways to track transactions, blockchain allows institutions and regulators to track financial activity with a greater degree of certainty, reducing potential for misuse.

7. TOKENIZED ASSETS WITH EMBEDDED CONTROLS

Through tokenization, assets like securities, loans, or real estate can be issued and transferred on blockchain, with the rules of compliance programmed into smart contracts. Enough to make transfers automatically comply with Anti-Money Laundering (AML) and Know Your Customer (KYC).

For example, JPMorgan's Onyx platform and Goldman Sachs' digital asset platform both include automated AML/KYC checks that prevent transfers to unverified counterparties or to individuals with a high-risk rating. This method does not just lower the danger of fraud, but it also optimises compliance, thereby allowing firms to secure assets within a digital economy (JPMorgan, 2021; Goldman Sachs, 2022).

8. INSURANCE APPLICATIONS

The insurance industry also benefits from enhanced fraud prevention through Blockchain. The U.S.-based Institutes Risk Stream Collaborative, an insurance consortium, tested blockchain options for recording accident information, ownership records and policyholder information in a shared ledger.

Fraudulent claims are also minimized as all the insurers share the correct and verified data and the record therein remains uniform across organizations. For instance, a fraudulent or exaggerated claim can be immediately reported when multiple insurers use consistent sources of data (Risk Stream, 2022).

9. DRAWBACKS AND CHALLENGES WITH BLOCKCHAIN TECHNOLOGY FOR FRAUD DETECTION

Blockchain technology seems to present promising solutions for better fraud prevention in financial institutions, yet its use is limited and hindered by a number of challenges and constraints. These include technical, legal, regulatory, and governance challenges. Technical challenges such as data privacy, scalability, interoperability, and energy consumption, legal and regulatory challenges such as uncertainty in enforcement, compliance issues, cross-border issues, and liability and accountability amongst others hinder the potential of blockchain technology in fraud prevention,

9.1 Privacy versus Transparency

One of the most notable strengths of blockchain (its transparency) works against it when it is integrated with data protection laws like the Gramm-Leach-Bliley Act (GLBA) in the U.S. and the General Data Protection Regulation (GDPR) in the EU. Confidentiality Both standards emphasize keeping material confidential and in some cases the right to be forgotten, which is contrary to the very nature of blockchain's immutability.

New innovations like permissioned blockchains and zero knowledge proofs seek to offer compromises between privacy and transparency, although these solutions have not yet been widely adopted (Mondaq, 2024; MDPI, 2024).

9.2 Scalability

Unlike conventional payment rails such as Visa which can handle thousands of transactions per second, most blockchain networks work at much slower speeds. This scalability difference restricts the use of blockchain for real-time fraud detection in industrial environments, for example the finance human-based system.

Although innovations like rollups, sharding, or layer-2 protocols have been under development around this problem. Such models are still in early development or early deployment phases, and wide adoption has not yet become mainstream (Investopedia, 2023; MDPI, 2024).

9.3 Smart Contract Vulnerabilities

Smart contracts are a killer app for automation and fraud-proofing, but bad or unaudited code opens up new risks. Cracks are vulnerabilities that can be exploited - for good or for ill; remember that someone who fraudulently siphons off funds is also exploiting a bug like those that were exploited in the 2016 DAO hack to steal millions of dollars.
The Commodity Futures Trading Commission (CFTC) has made clear that smart contracts performing regulated functions should be subject to oversight and audit. Yet, broad and cost-effective audit frameworks are scarce (Cleary Cyber Watch, 2018).

9.4 Governance and Legal Ambiguity

In the decentralized blockchain universe, accountability and the liability for fraud are a gray area. Centralized lack of control: if everything is not under control, then who do you blame for stuff?

While U.S. regulators have started to address these concerns themselves e.g., via the Securities and Exchange Commission's Project Crypto (2025) and the Financial Innovation and Technology for the 21st Century Act (FIT21, 2024), significant uncertainty remains. This is well illustrated during discussions of tokenized securities, on which organizations such as the World Federation of Exchanges have pleaded for stronger regulation to protect investors (see MarketWatch, 2025; Reuters, 2025).

9.5 Enforcement-Driven Uncertainty

The U.S. approach to blockchain and digital assets, for the most part, has been enforcement-based rather than rule-based. While enforcement is meant to safeguard markets, it also generates fears of the unknown for financial firms.

In high-stakes lawsuits over Non-Fungible Tokens (NFTs), staking, and Ethereum, it's become clear that murky jurisdictional rules can result in expensive court battles. Detractors argue that this enforcement mechanism stifles innovation and discourages institutional use (Reuters, 2025; Time, 2023).

10. RECOMMENDATIONS FOR FUTURE RESEARCH

In order to fully leverage on the use of blockchain technology in fraud prevention, future works should consider some vital areas.

First, it is necessary to set down standardized legal and regulatory standards in order to facilitate the balance between innovation and compliance through a variety of regions (Arner et al., 2020). Additionally, innovations around privacy-preserving mechanisms like zero-knowledge proofs and confidential computing will be critical for balancing blockchain's transparency with strict data protection requirements of financial organizations. Also, long-term examinations of institutional blockchain use cases are needed to rigorously evaluate the efficacy, resilience, and scalability of blockchain-based anti-fraud systems.

Another urgent need involves the resilience of smart contracts which requires concrete efforts to produce safer development practices (e.g., formal verification frameworks, strong auditing standards, incident response procedures) to prevent exposure and exploitation of flaws (Atzei et al., 2017).

Empirical studies on economic trade-offs that compare the cost and benefit relationship of adopting blockchain against existing fraud detection systems is equally important (Catalini & Gans, 2016). In addition, the amalgamation of blockchain with Artificial Intelligence (AI) and Machine Learning (ML) is also an interesting research trend especially for facilitating real-time anomaly detection by using unalterable audit trails (Wang et al., 2022).

New legislative initiatives and regulatory structures for blockchain applications can be a potential in making it a fraud prevention tool that strengthens the United States financial system security and transparency.

And finally, it is equally important to recognize that blockchain is no magic bullet in preventing fraud, and ongoing research and regulatory engagement on scale, privacy/security/technology integration are essential before its full deployment across the United States financial sector can be achieved.

11. CONCLUSION

The United States financial system can benefit from the potential transformation of anti-fraud defenses through block chain. Its hallmarks, namely immutable, consensus-based validation, programmability through smart contracts, and forensic traceability, provide strong protections against fraud by increasing transparency, reinforcing auditability, and automating compliance. Such features overcome a number of limitations of conventional fraud-prevention systems, which can suffer from delay, inefficiency, and vulnerability to gaming.

But block chain is not a cure-all. Its adoption is subject to considerable limitations, scalability issues, smart contract bugs, conflicting privacy and legal requirements, ambiguities in service governance, and regulatory enforcement. These difficulties suggest that although the blockchain can contribute to and improve fraud prevention, its place should be cautiously embedded in larger institutional and regulatory frameworks.

REFERENCES

1. *Adejumo, A. P., & Ogburie, C. (2025). Blockchain for fraud prevention: Transforming accounting and finance. International Conference on Next-Generation Innovations and Sustainability 2025. Futurity Research Publishing. https://doi.org/10.5281/zenodo.15063991*
2. *Aite Group. (2021). The future of KYC: Leveraging blockchain for compliance. Aite-Novarica Group.*
3. *Arner, D. W., Barberis, J., & Buckley, R. P. (2020). The evolution of FinTech: A new post-crisis paradigm? Georgetown Journal of International Law, 47(4), 1271–1319.*
4. *Association of Certified Fraud Examiners. (2024). Report to the nations: Global study on occupational fraud and abuse. ACFE.*
5. *Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). Proceedings of the 6th International Conference on Principles of Security and Trust, 164–186. https://doi.org/10.1007/978-3-662-54455-6_8*
6. *Bank of America. (2019). Blockchain trade finance initiatives. Bank of America Reports.*
7. *Begum, A., Munira, M. S. K., & Juthi, S. (2022). Systematic review of blockchain technology in trade finance and banking security. American Journal of Scholarly Research and Innovation, 1(1), 25–52. https://doi.org/10.63125/vs65vx40*
8. *Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006*
9. *Chung, D., & Kim, K. (2016). The Fourth Industrial Revolution: Blockchain applications. Journal of Emerging Technologies, 12(3), 25–40.*
10. *CoinDesk. (2025, March 21). Tornado Cash removed from U.S. sanctions list after court ruling. CoinDesk. https://www.coindesk.com*
11. *Deloitte. (2020). Blockchain in healthcare and insurance: Fighting fraud with distributed ledgers. Deloitte Insights.*
12. *Depository Trust & Clearing Corporation. (2022). Project Ion: Accelerating digital settlement. DTCC.*
13. *Depository Trust & Clearing Corporation. (2020). Annual report 2020. DTCC.*
14. *Federal Deposit Insurance Corporation. (2023). FDIC issues statement on crypto-asset risks to banking organizations. https://www.fdic.gov*
15. *Federal Reserve, Office of the Comptroller of the Currency, & Federal Deposit Insurance Corporation. (2023, January 3). Joint statement on crypto-asset risks to banking organizations. Board of Governors of the Federal Reserve System. https://www.federalreserve.gov*
16. *Financial Crimes Enforcement Network. (2019, May 9). Application of FinCEN's regulations to certain business models involving convertible virtual currencies (CVC guidance). U.S. Department of the Treasury. https://www.fincen.gov*
17. *Financial Crimes Enforcement Network. (2022). Statement on the use of blockchain analytics. U.S. Department of the Treasury.*
18. *Financial Crimes Enforcement Network. (2023, October 19). Proposal of special measures regarding convertible virtual currency mixing, as a class of transactions of primary money laundering concern. U.S. Department of the Treasury. https://www.fincen.gov*
19. *Financial Crimes Enforcement Network. (2024). Beneficial ownership information reporting requirements. U.S. Department of the Treasury. https://www.fincen.gov*
20. *Goldman Sachs. (2022). Goldman Sachs digital assets platform: Annual report. Goldman Sachs Group.*

21. *HSBC. (2019). HSBC and Wells Fargo complete blockchain-based FX transactions. HSBC Press Release.*
22. *IBM. (2017, June 15). AIG and IBM pilot multinational smart contract-based insurance policy. IBM Newsroom. https://newsroom.ibm.com*
23. *IBM Blockchain. (2023). Blockchain and KYC: Transforming financial compliance. IBM.*
24. *J.P. Morgan. (2021, October 27). JPMorgan launches Onyx blockchain platform for wholesale payments. J.P. Morgan News. https://www.jpmorgan.com*
25. *JPMorgan Chase. (2020). Introducing Onyx by J.P. Morgan. JPMorgan Chase & Co.*
26. *Kuo, C.-C., & Shyu, J. Z. (2021). A cross-national comparative policy analysis of blockchain technology between the USA and China. Sustainability, 13(12), 6893. https://doi.org/10.3390/su13126893*
27. *MarketWatch. (2025). World Federation of Exchanges calls for stricter regulation of tokenized stocks. MarketWatch.*
28. *Mastercard. (2020, February 6). Mastercard and blockchain: Building trust in trade finance. Mastercard Newsroom. https://www.mastercard.com*
29. *MetLife. (2019). MetLife launches LifeChain blockchain pilot to streamline life insurance claims. MetLife Newsroom.*
30. *Mondaq. (2024). Blockchain, privacy, and financial compliance. Mondaq Publications.*
31. *NASDAQ. (2015). NASDAQ Linq demonstrates blockchain technology to complete and record private securities transactions. NASDAQ Press Release.*
32. *National Institute of Standards and Technology. (2018). Blockchain technology overview (NISTIR 8202).*
33. *Nationwide. (2020). Nationwide explores blockchain for insurance claims management. Nationwide Insurance Reports.*
34. *New York Department of Financial Services. (2022, April 28). Guidance on the use of blockchain analytics. https://www.dfs.ny.gov*
35. *New York Department of Financial Services. (2023, November 15). Guidance on coin-listing and delisting policy frameworks. https://www.dfs.ny.gov*
36. *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf*
37. *Office of Foreign Assets Control. (2025, March 21). Update on Tornado Cash sanctions. U.S. Department of the Treasury. https://home.treasury.gov*
38. *Office of Foreign Assets Control. (2022, August 8). Sanctions on Tornado Cash virtual currency mixer. U.S. Department of the Treasury. https://home.treasury.gov*
39. *Phan, L., Li, S., & Mentzer, K. (2019). Blockchain technology and the current discussion on fraud. Computer Information Systems Journal Articles, (28). https://digitalcommons.bryant.edu/cisjou/28*
40. *Reuters. (2019). Wells Fargo and HSBC complete blockchain FX pilot. Reuters.*
41. *Reuters. (2025). U.S. regulators push stricter oversight of tokenized assets. Reuters.*
42. *RiskStream Collaborative. (2022). Blockchain insurance applications: Reducing fraud through shared ledgers. The Institutes RiskStream Collaborative.*
43. *Silvergate Bank. (2020). Silvergate Exchange Network (SEN) overview. Silvergate Capital Corporation.*
44. *Tapscott, D., & Tapscott, A. (2019). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world (Updated ed.). Portfolio.*
45. *Time. (2023). How SEC enforcement is shaping the future of crypto regulation. Time Magazine.*
46. *U.S. Department of Justice. (2021). Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists DarkSide. DOJ Press Release.*
47. *U.S. Department of the Treasury. (2022, August 8). U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash. U.S. Department of the Treasury Press Release.*
48. *U.S. Department of the Treasury. (2023, April). Illicit finance risk assessment of decentralized finance. U.S. Department of the Treasury.*
49. *U.S. Department of the Treasury. (2024a, February). 2024 national illicit finance strategy. U.S. Department of the Treasury.*
50. *Visa. (2019, June 11). Visa B2B Connect goes live. Visa Newsroom. https://usa.visa.com*
51. *Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLoS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477*
52. *Zhang, R., Xue, R., & Liu, L. (2021). Security and privacy on blockchain. ACM Computing Surveys, 52(3), 1–34. https://doi.org/10.1145/3316481*
53. *Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647*