Deep Science Publishing
https://doi.org/10.70593/978-93-49910-16-4_12

DeepScience
Open Access Books

Chapter 12: The road ahead: emerging technologies shaping the future of finance and identity protection

12.1. Introduction

The rapid rise of FinTech can be attributed to the mutual integration of cutting-edge technologies, particularly AI and Blockchain. The finance and insurance sector ranked second among the industries most targeted by cyber criminals since 2018. Malware, phishing, ransomware, and DDoS attacks are among the most disruptive threats encountered. Besides, misuse of authentication tokens like stolen passwords, access key exploitation, and use of unsecured accounts to access the clients' wallets belong to the prevailing threats. Despite industrial efforts to counter the challenges, the emergence of novel threats such as AI-generated deepfakes, social engineering, and automated account takeover attacks, outstrip the defenses and impose severe damage to various stakeholders. Like a game of cat and mouse, countermeasures and breaks are expected to continue evolving; so far, most countermeasures like source code obfuscation and metamorphic tactics have been proved effective. Due to the novelty and complexity of FinTech services, the need for manual analysis of the services have restrained the evolution of defense technologies. This introduces a novel and refined taxonomy of security threats in FinTech and conducts a comprehensive systematic review of defensive strategies. Through PRISMA methodology applied to 74 selected studies and topic modeling, this research identifies 11 central cyber threats and pinpoints 9 corresponding defense strategies. In this study, the taxonomy of cyber threats in FinTech services is enriched. Aligned with this novelty, a research gap on the preventive countermeasures is identified and an extensive survey of the defensive strategies against evolving cyber threats in FinTech is presented. The comprehensive systematic review offers invaluable insights for the academic community and other stakeholders of the FinTech industry. Available works on defending strategies are illustrated with informative materials. Similar to technologies, opponents' knowledge would be

circumvented and assembled as benign services (Rachmad, 2025; Yoganandham, 2024). Thus, academia needs to constantly enhance the defenses for competitiveness against ever-evolving cyber threats. Desiring of regulatory and preventative capability acquired through this research, we hope that practitioners become aware of the current challenges in FinTech and know it well to realize effective countermeasures. The approaches are examined as an overview of the scientific understanding of FinTech cyber threats and corresponding defenses with perspectives spanning from classic ones to novel cutting-edge technologies. The review offers novel insights into FinTech systems design and the systematic investigation of threat-vulnerability pairs of found technologies (Allioui & Mourdi, 2023; Bhati et al., 2023; Feyen et al., 2023).

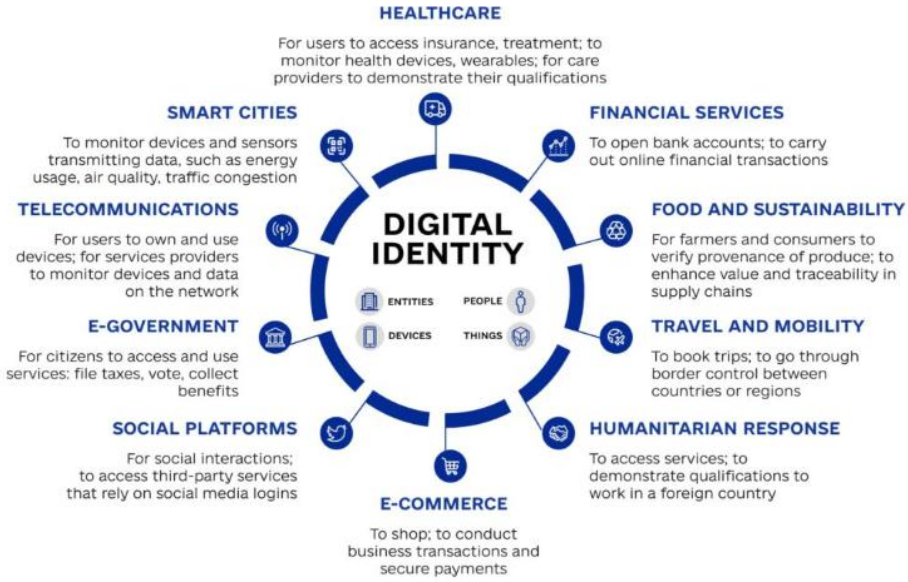

Fig 12.1: Looking Ahead Digital Identities

12.1.1. Background and Significance

Finance, Financial Technology, FinTech, Disability, Vulnerable Consumer, Cybersecurity, Identity Protection, Self-Sovereign Identity, Web 3.0, Blockchain, Decentralized Identifiers, Verifiable Credentials, Proof of Concept, User Controlled Identity.

Earlier definitions focused on the industry and the applications disrupting the financial services ecosystem, which included any firm that used technology as a tool for any financial service; for example, loans, payments, exchange of currencies. More recent definitions have considered FinTechs as a subclass of start-ups that use digital technologies as a tool for distinctly financial services and with a business model that is

either a platform or a cross-subsidized free model. This led to a trimmed definition of FinTech which still included a wide variety of companies including new banks like Revolut, business banks like Starbucks, and platforms that, as a service, allow financial services without any implication of having a credit risk. A legal and historic perspective is also useful in order to better understand the disruptive capacities of firms that have a wide gap between the financial service offerings and their activities in the real economy. The richer the offering of a FinTech platform is, in contrast to a traditional bank, the larger the challenge to law and regulation is. A very rich offering with platforming consumer protection, counterparty risk management and KYC instruments is needed.

It might also be useful to approach FinTech from a telecommunications perspective. The telecommunications infrastructure where the internet lay, allowed the bundling of a series of services that once were offered separately, first voice, fax and international money transfers, all types of media, at once. Banking and FinTech hold a service that cannot be offered as a standalone service. Standalone banking, insurance, or maintenance fund services are conspicuously money laundering suspicious, while capital movements not related to financial services are legally observed. FinTech takes advantage of Web 3.0 technologies: it offers a series of real economy services and through this partnership allows for the offering of financial services. So far, societal benefits have been obtained due to indirect competition between infrastructure-based verticals. More parochial information channels, stricter KYC, audiences' segmentation, product offering adaptations have fostered prevalence of such services to vulnerable consumers. Hence, financial malfeasance has flourished which made regulation adopt a 'whack the mole' approach in geographies out of sync with the ecosystem.

12.2. Overview of Emerging Technologies

Emerging technologies in the financial sector can be advantageous in their utilization of potential energy. The development of new technologies highlights the scintillating advancement of the financial sector in terms of competitiveness, convenience, security, and interconnections. A plethora of agencies, think tanks, and research institutes predict the effects of emerging technologies, yet the strength of the analysis is contingent on the agency's background, occupations, and advantages in different domains. This section strives to draw an analytical view of each mechanism derived from the literature collection. The section encompasses the emergence and utilization mechanisms of emerging technologies, Fintech, Artificial Intelligence (AI), Blockchain Technology, Internet of Things (IoT), the Tactile Internet, and Quantum Computing. A point worthy of note here is that, depending on the respondents' working backgrounds, actions taken for the adoption or implications of new technologies may differ.

Fintech, as a financial industry that is radically changed with technology innovations and consequently becoming new norms in economies, is an established term. The sources collection indicates that the term 'Fintech' arises from a narrow definition to produce more broad contents over time. Stakeholders gradually realize that Fintech can be embedded into every dimension of the finance ecosystem and that Fintech-related changes go beyond technical innovation and systemic change. Lately, debates on the wide ramifications of Fintech in the finance industry emerge and provoke a return of debate on the future of money and redefining of value-added services. Nevertheless, the high frequency of technologies (financial technologies) indicates that research on technologies emerges from broader categories to more individual domains. AI as a general term encompasses intelligent algorithms and devices from algorithmic concerns like neural networks and logical-based reasoning to more physical devices like robots and drones. With development over decades, AI finally comes to the finance industry and its potentials in improving efficiency, capturing profitability, and better decision-making are well understood. Among deep learning powered AI, newer generation neural networks such as Generative Adversarial Networks (GANs) and Long short term memory (LSTM) networks and their combination with finance knowledge have drawn increasing attention lately.

12.2.1. Artificial Intelligence and Machine Learning

Emerging technologies have historically transformed the landscape of nearly every industry, while at the same time creating new strategic opportunities and challenges. These emergent technologies also have the potential to threaten the future of the consumer trust and identity protection fields, forcing industry leaders to adapt their current strategies and rethink their approaches to identity protection measures. Even the most user-protective systems will face ongoing challenges as new attack means are discovered or harmfully misused approaches evolve. Without effective protections put into place against emergent technologies, the need for new trust systems based on foreknowledge of technology and guarantee of the preservation of the promise, neurally and socially.

This section explores some of the emerging technologies which are shaping the future of finance, specifically the AI and machine learning considerations thereof, as well as the implications therein for consumer trust and identity protection. These technologies are by no means a comprehensive evaluation of those which will emerge toward the future – many others could be equally or more important and impactful – but are instead an exploration of technologies viewed as among the most threatening or concerning in light of the past impact of comparable technologies as well as their current state of maturity and development. Just as past technologies would develop at a seemingly

exponential level, emerging technologies similar in form could have equally impactful effects society-wide.

12.3. Impact on Financial Services

The Financial Services Industry has changed drastically in the last two decades due to high competition and sweeping changes in technology. Continuous change of tactics has become a norm; some institutions have gone past competitors with dramatic leaps in efficiency and customer satisfaction. Mobile banking is one of the key changes in this business area. Today, mobile banking is delivered by SMS or Unstructured Supplementary Service Data, Mobile Internet Browsers or downloadable applications. On the demand side, it used to be difficult to imagine how to conduct payments with a telephone chip until 2011, when SEPA payments were officially launched across 31 countries via cell phone. Banking, money transfers and card payments can now be done by telephone.

The technology layer below Electronic Banking Services could be analyzed from two sides. On the one side, it is a multitude of cooperating financial service providers, telecommunications operators, cash register system vendors, marketplace managers, software vendors, technology providers and certification authorities. On the other side, there are not only new entrants moving into this market. Telecom operators, systems vendors and outsourcing service providers start cooperating with banks in electronic payment services. In line with this trend, payment systems integrating services across industry sectors are emerging. Yet the existing financial infrastructures and standards are mostly based on traditional banking channels making it difficult to connect from the electronic retail side.

Identity management is one of the key critical financial infrastructures. The market offers various IdM technologies, such as biometrics, smart cards, tokens, RFID, PKI and Bluetooth-based devices. In the modern world, stealing one's identity is as bad as stealing money. It is virtually impossible to steal money today without having access to the victim's identity. Hence, due to tremendous developments taking place in the ability to steal information and impersonate individuals for financial gains, the secure processing of sensitive data in e-banking is extremely important in order to avoid heavy losses and many other attacks on customer information. As recently demonstrated, it is almost impossible to have a 100% secure payment application, to send leaked information to third parties or to someone impersonate the payer. Solutions like Biometric ID, Federated ID and Mobile Transaction Authentication Numbers are currently available digital identities for additionally verifying transactions in e-banking services. The value and urgency of secure identities cannot be stressed enough when it comes to secure banking.

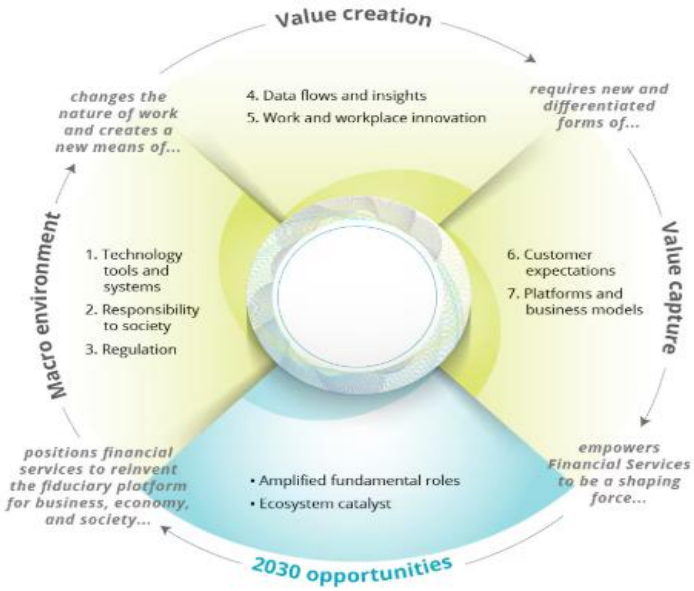

Fig 12.2: The future of financial services

12.3.1. Digital Payments and Cryptocurrencies

Digital assets, including currencies and securities, involve technology that has not been adequately considered or analyzed by policymakers. The metaverse is a prime example of an environment that is being actively constructed on a timeline that exceeds government reaction and forethought. The digital finance technologies are also under consideration on a race-to-the-bottom basis by small countries, hampered by resource constraints of understanding. A ceiling on minimum violence costs per white-collar crime, a restriction that does not apply to blue-collar crime, needs consideration in regard to the metaverse places of medium or large' harms. The second largest consumer of Fiji's energy supply has become a casino and the Stanford-destroyed value of Solana-based Metafair's $100M in Bitcoin seized.

The credibility of securities custody strategies is being reconsidered at a level higher than custodian firms collapsing. Trading firms have been cautioned that vetted participants remain legal and civil-vetted, e.g., it is not sufficient to just have exchanged funds for coins. Digital asset custodian solution analysts fear for the viability of PHV custodial contracts post-Platinum risk transfer, notwithstanding LINDD's rate-up assurances. Access provisioning undermines the security of centralized trading venues' funds and systems through exploitation of protocol vulnerabilities, and rogue insiders. FTX employee fratricide purportedly involved zero-knowledge side-channel methods, New Zealand reflecting disgruntled employee accusations.

Broad distinctions between public and private blockchain applications and the monthly custodial arms estimate decay are recognized. Insights on distributed oracle architecture balancer at exchanges and price aggregation boon at exchanges are provided, distinguishing custodial and internal restaking, along with DeFi central exhaustion models being over-crafted. Bitcoin and Ethereum custodial designs relevant to centralized exchanges are a defense tangent for semi-automated custodians. Stateless Ethereum is also examined. Performance metrics reflecting user-experience trade-offs are recognized. Concerns regarding opening up authorized chains are limited to improving competitiveness on liveness and block size.

12.4. Identity Protection in the Digital Age

As more and more of our lives become digitized, a troubling reality emerges: the risk that others will gain access to personal information regularly created and stored online. While this should always give rise to concern about identity theft and fraud, new incidents that capture the public imagination add urgency to that concern. Just this year, a data breach at Equifax exposed the personal information of 146 million consumers, including Social Security numbers, birth dates, addresses, and driver's license numbers. Just last month, Facebook disclosed that data from an estimated 49 million users had been taken without their consent. The information could include Facebook IDs, access tokens, and account usernames. This gives hackers the ability to use consumers' Facebook accounts as if they were the legitimate users. Moreover, in January, the video service Twitch reported a data breach that exposed source code, user account information, and internal details of the company. While this last hack likely does not pose a risk to consumers, it demonstrates the wide-ranging effects of data breaches in consumer settings.

The data breach at Equifax was particularly frightening, given the breadth of information that could now be used to steal or fabricate identities, a process known as "identity fraud." Once criminals gain access to a consumer's Social Security number, an identity and credit can be taken out in that consumer's name. This can be used to obtain loans, live free of charge in an apartment, or be jailed for a crime. Criminals can also use other information taken in the Equifax breach, like birth dates and surnames, to respond to knowledge-based authentication questions used to reset online bank accounts, meaning they would have access to the most sensitive and financial information available.

12.4.1. Challenges of Identity Theft

Identity theft is the impersonation of a person in order to deceive, usually for economic gain. This crime can take many forms, including obtaining false loans, checking and

credit card accounts in the name of another, and the misuse of other individuals' private data to create links with businesses such as utility companies. Theft of identity has numerous root causes, according to a recent study. A majority comes from the Internet. Hackers compromise large databases of identities and employ virus packets to search home computers for names, numbers, and passwords. Guidance cultures based offshore often lure individuals with work-from-home opportunities, then collect the victims' personal data and use it to construct fake accounts. Identity thieves also browse/search public locations, stealing bags and mail that include documentation such as a Social Security Number. Fraudulent account establishment has serious ramifications for individuals or society as a whole. Damage to credit reports will result from defaulting on loans taken out in the victim's name. Victims of such fraud would be denied loans, credit cards, housing, utilities, and employment. Aside from real economic consequences, identity theft victims also suffer emotional stress. Assessing the full extent of damage is difficult, as damaged credit reports would require years to repair. The issue of identity theft is steadily gaining significance in politics, academia, and among the general public. A sense of urgency has mounted over the last year or so, stimulated in part by ongoing media coverage of a spate of high-profile corporate scandals and events such as the hacking of a database, which exposed the information of millions of cardholders. Many are concerned that existing laws may fall short of addressing the matter, while others are doubtful about whether legislation would be successful. Many states have implemented laws addressing a variety of aspects of identity theft. A report found that 19 states have criminalized the act of stealing someone's identity, 15 included identity theft in a broader definition of fraud, and at least six prohibit computer-related identity theft. A large majority of actions performed with intent to fabricate or acquire accounts without consent are considered crimes in various states.

12.5. Case Studies

Financial institutions sometimes compete to offer financially inclusive services targeting unbanked and underbanked populations. Participants in innovation workshops proposed a Know-Your-Customer (KYC) solution that utilizes decentralized identifiers and verifiable credentials to carry out a risk-based assessment on new customers’ challenges faced. The proposed system will run as an independent identity and identification manager whose operations will be further protected by an egalitarian blockchain architecture. This case study presents the results of the team’s engineering processes, demonstrating both innovative design and regulatory compliance.

2022 saw severe conflict and ongoing shocks in global commodities. In March, sanctions on Russia prompted spikes in global commodity prices. Russia supplied an outsize share

of palladium, platinum, and crude oil. In May, war and sanctions drove price shocks, causing shifts in production away from Ukraine and confronting Western Europe with historically unprecedented price shocks in energy markets. Conflicted implementation of sanctions revealed ways the financial system created unseen cracks. The newest energy sanctions on Russia followed Russian President Putin's rejection of the G7 proposal for a price cap on oil sales to limit revenue for Russian war purposes. Regulators in the United States, United Kingdom, and European Union authorized new sanctions targeting, respectively, Russia's oil industry, ship insurers, and vessel operators in shipping sanctions on Russian crude oil.

Regulatory creation and compliance concern requirements for companies to achieve fines and penalties under antitrust, corruption, or other laws. Additionally, over the last decade, these have included the need for third-party compliance solutions for virtual currencies, non-fungible tokens, consumer data, and artificial intelligence. These technologies brought new ways to attack long-standing problems of governance and regulation, such as financial inclusion and KYC. Emerging as possible solutions are astonishing new ways to shield personal data, create second identities, verify financial account ownership, and prevent attacks on bank stability, fraud, or deception.

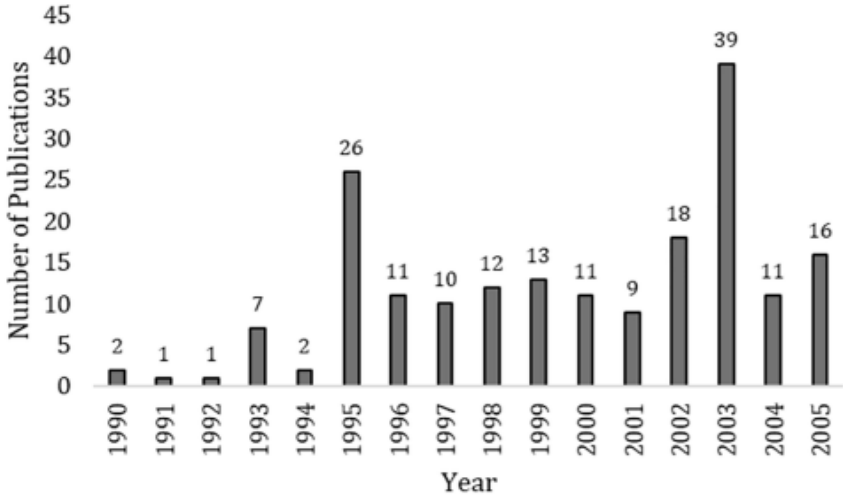

Fig : AI integration in financial services

12.5.1. Successful Implementations of Blockchain

The functionalities and characteristics of Blockchain, such as smart contracts, decentralization, verifiable immutability, fault tolerance, and security, offer meaningful use cases in many industries, including Identity Verification, Patient Health Records (PHR), and Product Provenance. Several companies have already implemented

blockchain-based solutions in these areas. Woleet sees that a tamper-proof digital signature is created whenever an asset undergoes an event. This signature is uploaded to the BlockChain, and the Hash is sent to the professional parked in BlockChain storage, allowing someone to verify that the asset hash exists on the BlockChain. In 2018, Wallet Blockchain solution was integrated into WiseKey's Identity Vaults, ensuring the immutability of data with a Bundle Digital Factory (BDF).

In order to use blockchains to verify sensitive data, a digital signature must be created that can prove that a data batch is unchanged. This ensures integrity and diminishes the risk of forgery. In collaboration with the French Interpol office, a storage implemented in ChainPoint sibling with a multi-cryptographic layer allows jurisdictions, certificate authorities, and enforcers to verify that the original certificates exist on the network. French companies like Capgemini have used Woleet's solution to store public hashes of contract agreements. These digital signatures, along with the verification scheme, allow Capgemini to offer its clients contract monitoring services. An Experiment on Anti-counterfeiting in the Art Market with the Louvre Museum is also available. Woleet clients include several organizations, and the company works with about fifteen fellow French start-ups and one in Canada.

BlockChain enables the reconciliation and exchange of information with a high level of security. French bank BNP Paribas has built a Blockchain solution for sharing information on KYC; French company Evotrust is providing a BlockChain solution for digital identity in close partnership with French authorities. French company BeezMax, in partnership with a French bank, is using a public BlockChain for the digital exchange of notary deed signatures. The Notary company adopted this solution, and one signature will validate candidates' applications in 2019.

12.6. Conclusion

The landscape of finance and identity protection is undergoing a profound transformation driven by a convergence of advanced technology, regulation, societal changes, and competition. Traditional institutions, technology firms, and startups approach this transformation differently, shaping an emerging ecosystem for the provision of identity, inclusion, and protective services and products. These institutions differ in the technological approaches they take to these services and products. This chapter has reviewed emerging technologies relevant to this future, their implications for finance and identity protection, the promises and problems they present, and policy responses to these technologies.

The most significant technological advancements are in the fields of machine learning, privacy-preserving technology, and decentralized ledgers. These technologies are

transforming how finance and identity are understood and addressed. In finance, a new technological paradigm is emerging that leverages advanced technologies to provide financial services that are effective, inclusive, and safe by compatibility with regulations. In the identity domain, as access to digital services becomes more pervasive and often necessary for participation in society, there is a need for supportive measures concerning identity. Technologies are emerging that provide trustworthy privacy-preserving answers to common identity questions in a decentralized manner while enabling customers to take greater control over their identity. New financial institutions and identity providers are appearing that understand their operation in terms of these new technologies rather than historical lineages.

The consequence of this technological evolution is the emergence of an ecosystem of institutions that are both complementary and competitive. Many complementary institutions are likely to work together in the coming years to build a new landscape of finance and identity. However, new technological approaches to the provision of finance and identity are also likely to lead to competition between, for example, traditional institutions, fintech firms, tech firms, new startups, and public actors. Examining the implications of competition and complementarity between different technological approaches to finance and identity will be crucial for future research. This is particularly important as different technological architectures appear to have different incentives for data commercialization, leading to important implications for the guarantees and practices of different systems.

12.6.1. Future Trends

A total of 241 articles published in the last decade, addressing threats and/or crimes in FinTech. Stemmed from this systematic review, valuable findings were shared, including a refined FinTech threats' taxonomy, the most central threats, a summary of the studies' findings, and a visualization of them. The implications were thoroughly discussed from both theoretical and practical perspectives. Future research directions were proposed. FinTech is an abbreviation of financial technology, which is a collection of technologies employed to provide financial services. Emerging technologies in FinTech have led to the development of novel services and products, together with new business models. As an example, previously faced with the strict control of the Central Bank and high entry barriers, with the emergence of FinTech, unlimited swelling of capital is made possible and its control by risk management is challenging. Besides FinTech services, online banking systems, broker service systems, risk managers, and anti-money-laundering systems are examples of the Bank tech domain. There are also Insure tech systems and Stock tech systems. Blockchain networks also play a vital role, recently raising great attention among researchers, providing opportunities in FinTech

services. The rapid development of smart-everything technologies has left the traditional systems and infrastructures vulnerable to unprecedented threats, giving rise to various vulnerabilities and activities. Cybersecurity threats have become extremely critical in FinTech as a data-centric sector expected to provide its services 24 h a day and 7 d a week for its clients. Cyber threats targeting FinTech are seen as a potent weapon of mass destruction as its substantial breaches in the US are categorized as an act of war.

References

Yoganandham, G. (2024). Transformative impact: The role of modern and innovative banking technologies in driving global economic growth. Tuijin Jishu/Journal of Propulsion Technology, 45(1), 2024.

Feyen, E., Natarajan, H., & Saal, M. (2023). Fintech and the future of finance: Market and policy implications. World Bank Publications.

Feyen, E., Natarajan, H., & Saal, M. (2023). Fintech and the future of finance: Market and policy implications. World Bank Publications.

Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. Sensors, 23(19), 8015.

Rachmad, Y. E. (2025). The Monetary Future: Unraveling the Complexity of Central Bank Digital Currency. The United Nations and the Nobel Peace Prize Awards.

Bhati, D., Deogade, M. S., & Kanyal, D. (2023). Improving patient outcomes through effective hospital administration: a comprehensive review. Cureus, 15(10).