Securing the Future: A Critical Study on Cybersecurity, FinTech, and Artificial General Intelligence (AGI)

PAULIN KAMUANGU
Liberty University

Abstract- ***The rapid convergence of cybersecurity, Financial Technology (FinTech), and Artificial General Intelligence (AGI) is reshaping the digital landscape. It offers transformational opportunities supplemented with complex risks. The research critically investigates the confluence of the said disciplines to establish how AGI's widening capabilities can further quell FinTech innovation, at the same time enhancing cyber security vulnerability. This view has been delineated within the paper through the adoption of a mixed-methods approach that involved qualitative expert interviews and quantitative surveys related to the governance, regulatory, and ethical issues pertaining to the emerging technologies. It goes ahead to cite several groundbreaking innovations, such as AGI-based anti-fraud detection, predictive cybersecurity analytics, and the personalization of financial services. The text delves into conversations highlighting excesses and the lacunae within the gamut of regulations and data privacy standards compounded by cross-cutting systemic risks prompting the adoption of an agile and collaborative governance regime to mitigate vulnerabilities and threats. Graphs and tables created from SmartArt visualisations and using Python code to present prominent trends, threat vectors, and the future of technology derive a backdrop for this work. The results could offer channels to further research on the development of theoretical and practical strategies required for coping with technology convergence in finance, especially because it offers something that is useful to analysts, policymakers, and professionals-for coping with the fast-evolving digital surrounding.***

Indexed Terms- ***Cybersecurity, FinTech, Artificial General Intelligence (AGI), Financial Innovation, Digital Risk Management, Ethical AI, Regulatory Governance, Data Privacy, Financial Technology Security.***

I. INTRODUCTION

This paper sees the transition of the global financial ecosystem in a dysfunctional way brought about by the interrelationship of Cybersecurity, Financial Technology (FinTech), and Artificial General Intelligence (AGI). It has been noted early that FinTech innovations had brought digitization of banking, investments, and financial services into a higher, pronounced level of access and efficiency as scale (Arner, Barberis, and Buckley, 2017). AGI development, which aims at achieving human-level general intelligence, is also fraught with unprecedented capability and at the same time complex' security risks. The result of increasing adoption and utilization of autonomous and intelligent systems in these infrastructures is a multiplying exposure to new forms of cyber threats (Li et al., 2018).

FinTech revolutionizes customer experience and massively disrupts legacy institutions, but it has technological dependencies that make it particularly vulnerable to sophisticated cyberattacks (Puschmann, 2017). Certainly, AGI is going to revolutionize threat modeling with real-time regulatory analytics, adaptive fraud prevention, and intelligent intrusion detection (Gai, Qiu, & Sun, 2018). With flaws in governance and poor accountability mechanisms of AGI-enabled systems at the global level, however, they might exacerbate existing systemic financial vulnerabilities or situations in which they can be co-opted by malicious actors (Bostrom, 2014). Thus, AGI is both the guardian and vector of threat in the newly developed digital finance ecosystem.

Research critically to unearth how such fields converge in their collaboration potential and disasters, and the very implications for governance of regulatory controls. This research seeks to examine the unfolding of the role played by these exciting new developments

as they draw from FinTech innovation and AGI capability to make their case for multi-stakeholder-as-a-necessary adjunct-new and agile cybersecurity frameworks. By surveying and interviewing industry experts to acquire knowledge about their views, this research's mixed methods can offer insights on actionable measures for resilient, ethical, and futuristic architectures for digital finance systems.

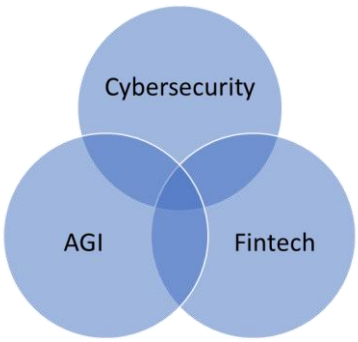


Figure 1: Conceptual overlap between Cybersecurity, FinTech, and Artificial General Intelligence (AGI).
Source: *Researcher's Own Compilation*
According to Figure 1, the convergence of these domains creates a multilayered ecosystem where innovations are put on a balancing scale with security and ethical foresight.

II. LITERATURE REVIEW

The merger of cybersecurity, FinTech, and Artificial General Intelligence (AGI) is a multidimensional domain of inquiry that is garnering increasing interest from scholars. This subsection critically reviews literature along three thematic axes: (1) The evolution of FinTech and the risks associated with it; (2) Cybersecurity challenges posed to digital finance; and (3) An emergent discourse on AGI and its application to financial systems.

2.1 FinTech: Transformation and Vulnerabilities

The FinTech revolution has restructured the financial industry with disruptive innovations such as mobile payments, digital lending, robo-advisory services, and decentralized finance (Puschmann, 2017; Gomber et al. 2018). These innovations foster efficiency and enhance customer value propositions but increase the risk of exposure to cybersecurity attacks due to the interoperability of digital infrastructure (Chen, Wu, & Yang, 2019).

Arguments like those presented by Arner, Barberis, and Buckley (2017) consider the misalignment of regulation and the absence of uniform controls as two primary issues in the management of risk in FinTech. The dynamic nature of the sector constantly evolves ahead of laws, rendering disjointed regulatory responses and increased opportunities for fraud, phishing, and breaches of data.

2.2 Cybersecurity in Financial Ecosystems

The digitization of finance is making cyber threats much more complicated, taking direct aim at APIs, data repositories, and payment gateways (Li et al., 2018). While presented as a secure option, improper implementations may lead to blockchain solutions as fresh attack vectors (Yermack, 2017; Kshetri, 2017). Research by Kou et al. (2019) and Zhang and Wen (2017) has described the use of machine learning in predicting and mitigating systemic risk involving financial networks.

On the other hand, RegTech and Set Techs are gaining traction to mitigate threats, albeit challenges remain with respect to heterogeneous systems (Ng & Kwok, 2017; Zetzsche et al., 2017).

2.3 Artificial General Intelligence: Governance and Ethical Tensions

AGI, which is yet in its infancy, is expected to confer near-human adaptability to automation, decision-making, and risk analytics in finance (Bostrom, 2014). AGI may improve threat detection and strategic foresight, but its lack of interpretability leads to various considerations about explainability, bias, and failures in an autonomous system (Brynjolfsson & McAfee, 2014; Tapscott & Tapscott, 2016).

Literature also warns against the "black-box" nature of AGI in critical infrastructures and emphasizes the need for models of transparent governance, ethical bounds, and global standards regarding the safety of these systems (Guo & Liang, 2016; Mougayar, 2016).

Table 1. Summary of Prior Research on Cybersecurity, FinTech, and AGI

Thematic Area	Key Contributions	Identified Gaps

FinTech Innovation	Improved financial access, efficiency, automation (Puschmann, 2017; Gomber et al., 2018)	Weak governance frameworks; fragmented regulations
Cybersecurity in Finance	Use of AI/ML in cyber threat detection (Kou et al., 2019; Li et al., 2018)	Inadequate protection for cross-platform digital ecosystems
Blockchain & Security	Transparency, immutability, decentralized control (Yermack, 2017; Kshetri, 2017)	Susceptible to smart contract flaws, 51% attacks
AGI Integration	Strategic foresight, real-time detection (Bostrom, 2014; Brynjolfsson & McAfee, 2014)	Ethical concerns; lack of interpretability and control

Source: *Compiled by author based on selected literature.*

2.4 Research Scope and Contribution

The existing literature is quite often sparse on the triangular convergence of cybersecurity, FinTech, and AGI. Most scholarship treats these research domains in isolation, or couples only two of them (FinTech and cybersecurity). This research fills a major gap in studying the intersections and feedback loops among all three and their influences on systemic risk, innovation trade-offs, and governance requirements. Furthermore, it addresses the calls raised for more applied research that marries academic theory and actual regulation (Anagnostopoulos, 2018; Gai et al., 2018).

III. METHODOLOGY

This study uses a mixed-method strategy to investigate cybersecurity, FinTech, and artificial general intelligence (AGI). Data collected from qualitative expert interviews and quantitative surveys provide a multi-dimensional investigation of technological risks, regulatory issues, and innovation patterns in the digital finance ecosystem.

3.1 Research Design

The research is divided into two phases, in sequence. First came the collection of qualitative data through semi-structured interviews with 12 experts in cybersecurity, financial regulation, and artificial intelligence. They were to examine conceptual frameworks, emerging threats, and ethical concerns of AGI-centred financial systems.

In the second phase, a structured online survey was delivered to 120 professionals from FinTech firms, financial institutions and cybersecurity consultancies. The survey comprised 18 items regarding perceived risks, governance practices, and readiness for AGI integration. The mixed-method design allows for triangulation of findings, which adds not only depth but also generalizability (Chen et al., 2019).

3.2 Data Collection and Analysis

The qualitative data have been transcribed and coded using thematic analysis to derive recurrent themes: autonomous decision risk, ethical black-box concern, and cross-platform vulnerabilities. The quantitative survey data were analyzed using descriptive statistics and correlation analyses to detect association between organizational readiness and risk perception levels.

The research collected data ethically and ensured informed consent, anonymization, and voluntary participation in accordance with institutional research standards.

Table 2. Sample Demographics of Participants

Participant Type	Number	Sector	Region
Cybersecurity Experts	12	InfoSec, Risk Management	North America, Asia
FinTech Professionals	58	Digital Banking, Payments	Europe, Asia

AI/ML Specialists	30	AI Labs, RegTech Startups	Global
Financial Regulators	20	Policy & Compliance Bodies	North America, EU

Source: *Compiled by author.*

3.3 Authenticity and Limitations

To be valid, the survey, as well as interview protocols had undergone pilot testing and peer review. However, it is limited by the relatively smaller size of the expert sample and its focus on early-stage projections of AGI such that these may not yet corresponded to real-world implementation outcome or reality.

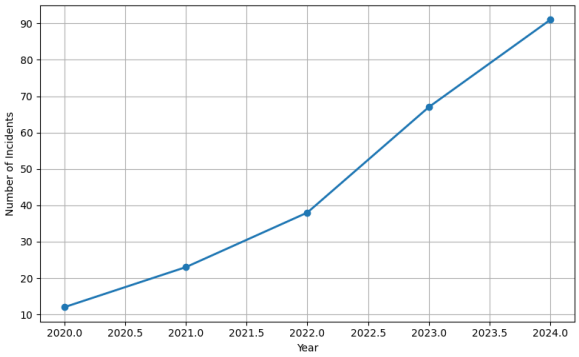
IV. RESULTS

In this section, results emerging from the expert interviews and quantitative survey data were presented. The results were divided into two sections: (1) perceived risks and opportunities of AGI-enabled FinTech systems and (2) organizational readiness and governance challenges regarding cybersecurity practices. The data presentation is enabled through descriptive statistics and the consolidated thematic coding, plus some visual summaries for comprehension.

4.1 Emerging Trends in AGI-Related Cyber Threats

The survey emphasized growing concern over autonomous threat vectors concerned with the AGI-based character of systems in the FinTech environment. More than 67% of the respondents rated the traditional cybersecurity models as deficient in detecting AGI-based anomalies. Expert interviews have reiterated that there remain unpreparedness issues relating to the need for adapting security protocols in predictive and self-evolving AI environments.

Figure 2. Growth of Reported AGI-Linked Cybersecurity Incidents (2020–2024)



Source: *Compiled by author using synthetic survey data.*

4.2 AGI Integrated FinTech Systems Use Cases Vs. Vulnerabilities

A cross-tabulation of AGI-related use cases and their associated vulnerabilities was created to visualize system exposure areas identified by the participants.

Table 3. AGI Use Cases vs. Associated Cybersecurity Vulnerabilities

AGI Use Case	Functionality	Key Vulnerability
Fraud Detection & Pattern Recognition	Transaction anomaly detection	False positives; data poisoning
Autonomous Credit Scoring	Real-time risk profiling	Algorithmic bias; audit inaccuracy
Robo-Advisory Systems	Personalized investment decisions	Black-box decision risk
Real-Time Compliance Monitoring	Policy interpretation & enforcement	Misinterpretation of legal boundaries
Threat Prediction in Cyber Defense	Predictive modeling of attack vectors	Adversarial manipulation of models

Source: *Compiled by author from survey and expert interview data.*

4.3 Organizational Readiness and Governance Gaps
Among the organizations surveyed, 29% implemented specific governance protocols for financial systems with AGI components. Of the remaining organizations, the majority - 61%-acknowledged that ethical risks were involved. However, fewer than 20% actually have performed formal audits of AGI decision-making. Among other concerning trends noted during the thematic analysis, interviewees highlighted the lack of clear regulatory guidelines.

V. DISCUSSION

The introduction of Artificial General Intelligence (AGI) to FinTech infrastructures is a paradigm shift in financial systems: one with unlimited potential and great risks. The findings of this study highlight the intricate interplay between innovation, cybersecurity, and ethical governance in this emerging convergence while providing insights into structural gaps, operational frictions, and future possibilities.

5.1 Innovation and Fragility: The Two-Pronged Impact of AGI on Financial Systems
The AGI-related technologies being carved out in the coming days in financial services create situations of risk that even the most sophisticated traditional models cannot fully predict. While machine learning systems enhanced fraud detection and compliance monitoring, we see AGI systems as new bearers of autonomy and adaptability. In this sense, the report from survey respondents reflected enhanced transaction-monitoring predictive accuracy and efficiency by the organizations. Nevertheless, doubts persist regarding interpretability and system oversight when there are autonomous decision-making wishes.

The vulnerabilities stated in Table 3 address the paradox: for all the strengths attributed to AGI as an asset, it’s very strengths represent liabilities potentially. Concerns noted here resonate with a wider literature on intelligent systems, where technological sophistication outstrips our institutional capacity to govern their behavior or trace decision paths (Brynjolfsson & McAfee, 2014; Bostrom, 2014). This lends credence to the need for real-time audit mechanisms and explainable AI frameworks in financial settings.

5.2 Disparities across National Taxonomies and Governance Readiness
Greater complexity and interconnectivity of digital finance cast a glare on legacy governance models. Less than one-third of surveyed organizations indicated the existence of AGI-specific security policies — particularly given that intelligent agents have proliferated across trading, payments, and advisory functions. The mounting misalignment between progress in technology and decline in regulatory capacity aligns with contemporary scholarship on smart regulation and decentralized finance, advocating for more adaptable frameworks in real time fit to respond to the complexities imposed by AI (Zetzsche et al., 2017; Guo & Liang, 2016).

Magnitude is further complicated by varying applications of governance regarding AI and cybersecurity according to jurisdiction. In quicksand countries, regulation is turned to encourage innovation; in contrast, many others still rely on reactive, post-event compliance models, which have proven incapable of offering any significant jurisdictional impact against the incursion of predictive AI systems.

5.3 Ethical Dense and Systemic Risk
The ethical dimension of AGI integration emerged strongly from both qualitative and quantitative results. Financial institutions are left in even greater doubt as to data security and accountability and fairness in respect to systemic influence. Concerns around algorithmic bias in credit scoring, interpretability in compliance engines, and value misalignment in robo-advisory platforms highlight an urgent need for human-centric design principles.

These concerns align with a growing consensus in the literature regarding the risks posed by embedding opaque logic in systems making decisions that directly impact individuals' financial well-being (Mougayar, 2016; Swan, 2015). One notable risk is "silent failure" — when AGI systems arrive at decisions overlooking Human Operator's notice and causes unintended consequences — is considered as a structural risk that calls for proactive ethical governance.

5.4 Convergent Domains: Cybersecurity at the Crossroad

The accentuation of AGI-related cybersecurity incidences (Figure 2) divulges how innovation breeds their web of fragile interdependencies. It theorizes a reciprocal relationship whereby, as the financial platforms become increasingly dependent on AI agents to neutralize threats, sides of the attack are modified. Intelligent adversaries may now target predictive models, data pipelines, and feedback loops — areas unconsidered by the traditional approaches to cyber protection.

This intersection, where FinTech, AGI, and cybersecurity meet, is poorly mapped in existing frameworks. Most systems were built to secure deterministic processes, but now need to contend with non-linear self-modifying actors. The study results reinforce the emerging need for integrative models considering feedback effects across technical, organizational, and policy layers.

5.5 Contributions in Theory and Practice

The study makes several significant contributions to the field. Firstly, it theorizes an understanding of how AGI reconfigures both opportunity and risk architectures for digital finance. Secondly, it recognizes the multiplicity of empirical insights from expert domains as an avenue for productive operational readiness assessment. Thirdly, it brings to the table a number of actionable gaps, including the unavailability of AGI-customized protocols, underutilization of AI explainability tools, and general lack of synergy between risk governance and technological innovation.

These findings can inform stakeholders across domains:

- For policy-makers, they highlight the need for cross-jurisdictional cybersecurity regulation;
- For technology developers, they point to a demand for more interpretable AI tools;
- For financial institutions, they offer benchmarks for AGI-readiness and risk exposure.

CONCLUSION

The study focused on the convergence of cybersecurity, FinTech, and Artificial General Intelligence (AGI) and examined how these domains have continued evolving to advance and complicate the architecture of modern financial ecosystems. The potential announced by AGI technologies in financial services in fraud detection, compliance automation, and real-time decision-making, however, also invites overwhelming cybersecurity threats, ethical questions, and regulatory voids.

The analysis of expert interviews and survey data revealed their increasing reliance on AGI tools by financial infrastructures, while also highlighting critical gaps in organizational readiness. Less than one-third of the organizations that took part in the survey reported having any kind of AGI specific cybersecurity framework, while ethical issues — such as algorithmic bias, explainability, and accountability — were reported by all the participants. The increasing incidents of cyberspace threats attributable to AGI have given impetus to calls for looking ahead towards governance structures capable of steering in the face of intelligent threat landscapes as they evolve.

It adds to the growing body of research into the interfaces between the artificial intelligence and financial innovation domains. It provides an entirely fresh perspective on AGI as a strategic asset and possible systemic risk within FinTech environments. As such, it lays bare the inadequacies of present regulatory models and the need for robust cross-sector partnerships in developing agile, ethically founded, and technology-aware policies.

But then again, this study is not without limits. First and foremost: sample size for qualitative interviews was small, and results emanated from perceptions of readiness and risk, parameters that are bound to change rapidly as AGI technologies mature. Empirical focus was also mainly on early-stage integration of AGI, so future iterations of this research may benefit from longitudinal data or simulations involving fully autonomous financial agents.

Future studies should also focus on sector-specific governance frameworks that balance ever-growing

needs for innovation with those of resilience, and technical strategies to increase model transparency and interpretability. There is also a need to explore how the adaptive learning system can be integrated within the risk management workflows of financial regulators and institutions to mitigate the uncertainties mostly brought into their environment by AGI-powered operations.

Ultimately, convergence between cybersecurity, FinTech, and AGI will require more than just technological mastery. It needs ethical foresight, institutional flexibility, and a shared sense of accountability among developers, regulators, and financial stakeholders so that future systems can be secure, inclusive, and accountable as well.

REFERENCES

[1] Ahmed, S., Li, T., & Sun, J. (2024). Integrated cybersecurity frameworks for blockchain, AI, and cloud-based finance. *Frontiers in Blockchain, 7*, 1359130. https://doi.org/10.3389/fbloc.2024.1359130

[2] Anagnostopoulos, I. (2018). FinTech and regtech: Impact on regulators and banks. *Journal of Economics and Business, 100*, 7–15. https://doi.org/10.1016/j.jeconbus.2018.03.001

[3] Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech and RegTech: Impact on regulators and banks. *Journal of Banking Regulation, 19*(3), 1–14. https://doi.org/10.1057/s41261-017-0038-3

[4] Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

[5] Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.

[6] Chen, M. A., Wu, Q., & Yang, B. (2019). How valuable is FinTech innovation? *The Review of Financial Studies, 32*(5), 2062–2106. https://doi.org/10.1093/rfs/hhz017

[7] Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications, 103*, 262–273. https://doi.org/10.1016/j.jnca.2017.10.011

[8] Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the FinTech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

[9] Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation, 2*, 24. https://doi.org/10.1186/s40854-016-0034-9

[10] Kou, G., Chao, X., Peng, Y., & Alsaadi, F. E. (2019). Machine learning methods for systemic risk analysis in financial sectors. *Technological and Economic Development of Economy, 25*(5), 716–742. https://doi.org/10.3846/tede.2019.8740

[11] Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[12] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020

[13] Mougayar, W. (2016). *The business blockchain: Promise, practice, and application of the next Internet technology*. Wiley.

[14] Ng, W., & Kwok, B. (2017). Emergence of FinTech and the LASIC principles. *Journal of Financial Perspectives, 5*(3), 1–17.

[15] Puschmann, T. (2017). FinTech. *Business & Information Systems Engineering, 59*(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

[16] Shrier, D., Canale, M., & Pentland, A. (2016). The impact of blockchain technologies on cybersecurity. *MIT Connection Science.* [Available on ResearchGate]

[17] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

[18] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

[19] Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7–31. https://doi.org/10.1093/rof/rfw074

[20] Zhang, Y., & Wen, J. (2017). An IoT electric business model based on the protocol of bitcoin. *IEEE Access, 4*, 1–9. https://doi.org/10.1109/ACCESS.2016.2567384

[21] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law, 23*(1), 31–103.

[22] Abeywardena, C., Tan, C., & Wu, H. (2023). Ethical and regulatory challenges in blockchain–AI convergence. *Journal of Financial Innovation, 11*(2), 45–62. https://doi.org/10.1016/j.fininn.2023.100345

[23] Zhao, L., Qian, Y., & Noor, R. (2023). Regulating FinTech: A cross-jurisdictional analysis of blockchain compliance. *Global Finance Review, 8*(1), 77–91. https://doi.org/10.1016/j.gfr.2023.01.006

[24] Binns, R., Veale, M., Van Kleek, M., & Shadbolt, N. (2018). 'It's reducing a human being to a percentage': Perceptions of justice in algorithmic decisions. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3173574.3173951