

Building Financial Resilience at HBCUs through Generative AI, FinTech, Blockchain, and Cybersecurity Education

Weizheng Gao¹

Department of Business and Technology, Elizabeth City State University

wegao@ecs.u.edu

Shanzhen Gao

Reginald F. Lewis College of Business, Virginia State University

sgao@vsu.edu

<https://doi.org/10.68414/MMET5997>

Abstract

Financial resilience has become an urgent educational priority as individuals face increasingly complex decisions involving budgeting, debt, credit, retirement planning, digital payments, online fraud, artificial intelligence tools, and rapidly changing financial technologies. Historically Black Colleges and Universities are well-positioned to advance financial security education by integrating financial literacy, FinTech, blockchain, cybersecurity, and generative artificial intelligence into interdisciplinary learning experiences. This paper proposes a human-centered framework for building financial resilience at HBCUs through technology-enhanced financial security education. The framework is organized around six connected pillars: financial foundations, FinTech literacy, blockchain and digital trust, generative AI-supported decision learning, cybersecurity and fraud prevention, and community-centered financial resilience. Using a conceptual design-science methodology, the paper synthesizes literature on financial literacy, digital financial capability, AI risk management, cybersecurity education, and HBCU-centered pedagogical innovation. It also builds on prior work in AI-supported learning, investment decision-making, blockchain education, and human-centered cybersecurity. The paper contributes a scalable curriculum model, sample learning modules, implementation strategies, and assessment measures for HBCU programs in business, computer information systems, cybersecurity, data science, and interdisciplinary fields. The framework positions financial resilience as a lifelong learning outcome and connects HBCU-centered

¹ Corresponding Author: Weizheng Gao

financial education with digital trust, cybersecurity awareness, and responsible use of emerging financial technologies.

Keywords: HBCUs, financial resilience, generative AI, FinTech, blockchain, cybersecurity, financial security education, digital trust

Introduction

Financial resilience is the ability of individuals, families, and communities to make informed financial decisions, manage financial shocks, protect assets, use financial technologies safely, and pursue long-term economic goals. In the current digital economy, financial resilience requires more than basic knowledge of budgeting or saving. Individuals must understand credit, debt, student loans, retirement planning, investment risk, insurance, taxes, digital payments, cybersecurity threats, online misinformation, and the growing use of artificial intelligence in personal finance.

The rapid expansion of FinTech, blockchain, digital assets, online banking, mobile payments, and generative artificial intelligence has created new opportunities for financial access and education. Digital financial platforms can help users monitor spending, compare financial products, transfer funds, invest, and access information. Blockchain technologies can support transparency, traceability, decentralized verification, and new forms of digital value exchange. Generative AI tools can explain complex financial concepts, simulate scenarios, help draft budgets, and support personalized learning. However, these same technologies can produce inaccurate information, encourage overconfidence, expose sensitive personal data, support scams, or widen inequalities when users lack the knowledge to evaluate them critically (Lo & Ross, 2024; National Institute of Standards and Technology [NIST], 2024a).

Historically Black Colleges and Universities are uniquely positioned to respond to this challenge. HBCUs have long served as engines of educational opportunity, community leadership, social mobility, and professional preparation. In the generative AI era, HBCUs can also lead in financial security education by preparing learners to understand both the promise and the risks of emerging financial technologies. A human-centered approach is especially important. Financial education should not blame individuals for financial hardship. Instead, it should recognize structural barriers, unequal access to trustworthy advice, increasing complexity in financial systems, and the need for practical, culturally responsive, and technology-supported learning.

This paper proposes a conceptual framework for building financial resilience at HBCUs through generative AI, FinTech, blockchain, and cybersecurity education. The framework is designed for use in business, computer information systems, cybersecurity, data science, finance, economics, entrepreneurship, general education, faculty development, staff training, and community outreach. It connects financial literacy with digital trust and treats cybersecurity as an essential part of financial well-being. It also emphasizes responsible use of generative AI: AI can support learning and decision analysis, but it should not replace professional financial, legal, tax, or investment advice.

The central contribution of this paper is the HBCU Financial Resilience Education Framework, a scalable conceptual model that integrates financial foundations, FinTech literacy, blockchain-based digital trust, generative AI-supported decision learning, cybersecurity awareness, and community-centered financial resilience. The paper addresses three research questions: (a) What core competencies are needed for financial resilience in the generative AI and FinTech era? (b) How can HBCUs integrate generative AI, FinTech, blockchain, and cybersecurity into financial security education? and (c) What curriculum modules, safeguards, and assessment strategies can support scalable implementation of financial resilience education at HBCUs?

Literature Review

Financial Literacy, Financial Capability, and Financial Resilience

Financial literacy is commonly understood as the knowledge and skills needed to make informed financial decisions. Foundational research emphasizes concepts such as inflation, interest rates, risk diversification, compounding, borrowing, saving, and retirement planning. Lusardi and Mitchell (2014) argue that financial literacy has important economic consequences because individuals are increasingly responsible for complex financial decisions over the life course. Atkinson and Messy (2012) similarly describe financial literacy as a combination of awareness, knowledge, skills, attitudes, and behaviors needed to make sound financial decisions and achieve financial well-being.

Recent evidence suggests that financial literacy remains a persistent challenge. The 2026 TIAA Institute-GFLEC Personal Finance Index reported that U.S. adults correctly answered only 47% of its 28 financial literacy questions on average, the lowest result in the index's 10-year history (Yakoboski et al., 2026). The Board of Governors of the Federal Reserve System (2026)

reported that 73% of adults were doing at least okay financially and that 63% could cover a \$400 emergency expense with cash or its equivalent. These statistics show both resilience and vulnerability: many adults report stability, yet substantial numbers remain exposed to emergencies, debt pressure, price increases, and uncertainty.

The Consumer Financial Protection Bureau (2015) defines financial well-being as a condition in which individuals can meet current and ongoing financial obligations, feel secure in their financial future, and make choices that allow them to enjoy life. This definition shifts the focus from isolated financial facts to lived financial experience. For HBCUs, financial resilience education should therefore include budgeting, debt management, credit, insurance, investing, retirement planning, tax awareness, emergency savings, and the ability to evaluate financial products and advice.

Digital Financial Literacy and FinTech Education

FinTech refers to the use of technology to deliver, improve, automate, or transform financial services. It includes mobile banking, peer-to-peer payments, budgeting apps, robo-advising, digital lending, credit scoring, digital wallets, blockchain systems, cryptocurrency, smart contracts, crowdfunding, and AI-supported financial services. FinTech can reduce barriers to access, but it can also create new vulnerabilities. Users may face hidden fees, privacy risks, biased algorithms, identity theft, phishing, scams, price volatility in digital assets, and misleading financial information.

The OECD/INFE international survey emphasizes the importance of digital financial literacy. Across participating countries and economies, the average digital financial literacy score was 53 out of 100, and only 29% of adults reached the minimum target score of 70 out of 100 (Organisation for Economic Co-operation and Development [OECD], 2023). Digital financial literacy levels were higher among adults with higher incomes and higher education levels (OECD, 2023). These findings support educational programs that help learners develop both technical and financial judgment.

For HBCUs, FinTech education should not be limited to preparing students for careers in financial technology. It should also prepare students, faculty, staff, and community members to navigate digital financial systems safely in daily life. A student who understands mobile payments, credit card interest, student loan repayment, online fraud, and AI-generated financial advice is better prepared for personal financial resilience. A business student who understands

FinTech platforms and cybersecurity risks is better prepared to make professional decisions. A computer information systems student who understands finance and digital trust is better prepared to design responsible systems.

Blockchain, Digital Trust, and Financial Security

Blockchain technologies are relevant to financial resilience education because they introduce new ways of thinking about trust, verification, transparency, decentralization, and digital ownership. A blockchain is a distributed ledger that records transactions across a network and uses cryptographic mechanisms to support integrity and verification (Nakamoto, 2008). In financial education, blockchain concepts can be used to teach authentication, immutability, consensus, transparency, smart contracts, tokenization, digital assets, and governance.

Blockchain education must be balanced and critical. Students should learn both potential benefits and risks. Benefits may include transparency, auditability, programmable transactions, and reduced reliance on centralized intermediaries. Risks may include volatility, scams, private key loss, smart contract vulnerabilities, regulatory uncertainty, speculative behavior, and irreversible transactions. A financial resilience curriculum should therefore present blockchain as one component of digital trust education, not as a guaranteed path to wealth.

Blockchain education can also help students compare financial trust models. Learners can examine the difference between bank accounts, payment app balances, cryptocurrency wallets, and tokenized assets; discuss how ownership and transactions are verified; and consider user responsibilities when private keys, irreversible payments, and decentralized governance are involved. These questions connect technical literacy with financial decision-making.

Cybersecurity, Privacy, Fraud Prevention, and Human Factors

Cybersecurity is central to financial security. Even a financially knowledgeable individual can suffer harm if they fall victim to phishing, identity theft, account takeover, payment fraud, investment scams, tax scams, ransomware, or social engineering. Many financial threats are not purely technical; they involve human factors such as urgency, trust, fear, social pressure, unfamiliar terminology, and cognitive overload.

The NIST Cybersecurity Framework 2.0 organizes cybersecurity outcomes around the functions Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024b). These functions can be translated into personal financial security education. Learners can govern their financial security by setting rules for password management, account monitoring, and

information sharing. They can identify financial assets and risks, protect accounts with multifactor authentication, detect suspicious activity, respond to fraud attempts, and recover through reporting, freezing credit, changing credentials, and documenting incidents.

Human-centered cybersecurity research emphasizes that security systems must account for human behavior, organizational culture, trust, communication, and practical constraints (Malomo et al., 2025). A human-centered financial resilience curriculum should avoid blaming victims of scams. Instead, it should teach learners how scams work, how emotions are manipulated, how to verify information, how to pause before acting, and how to seek help.

Generative AI in Financial Security Education

Generative AI can support financial education by explaining concepts, generating examples, simulating scenarios, translating technical language into accessible language, creating practice quizzes, helping learners compare repayment options, and supporting reflection. For example, a student could ask an AI tool to explain compound interest using a simple example, generate a monthly budget template, or compare the long-term effects of minimum payments versus larger credit card payments.

However, generative AI introduces serious risks in financial contexts. AI tools may generate inaccurate, incomplete, outdated, or overly confident responses. They may fail to account for personal circumstances, tax rules, legal constraints, or institutional policies. Lo and Ross (2024) show that generative AI can be considered a promising yet limited tool for financial advice, underscoring the need for verification and human judgment. The NIST AI Risk Management Framework emphasizes trustworthy AI characteristics such as validity, reliability, safety, security, resilience, accountability, transparency, explainability, privacy enhancement, and fairness (NIST, 2023). NIST's Generative AI Profile also highlights risks involving information integrity, cybersecurity, privacy, and misuse (NIST, 2024a).

The present framework uses generative AI for educational and decision-support purposes, not as a substitute for licensed financial, legal, tax, or investment advice. Learners should be taught to verify AI outputs, compare AI-generated explanations with reliable sources, avoid entering sensitive personal data, recognize hallucinations, and understand the limits of AI-generated financial guidance.

HBCU-Centered Pedagogical Innovation

HBCU-centered financial security education should be practical, interdisciplinary, inclusive, and empowering. It should recognize that financial learning occurs across academic programs, workplaces, families, and communities. Students may need help understanding student loans, credit cards, budgeting, internships, entrepreneurship, taxes, insurance, and entry-level retirement benefits. Faculty and staff may need continuing education on retirement planning, cybersecurity, digital financial tools, and AI-assisted financial information. Community members may need accessible workshops on fraud prevention, credit, online banking, and safe use of digital tools.

Prior related work has emphasized AI-supported learning, blockchain and generative AI education at HBCUs, investment decision-making, business analytics, Google Colab, computational thinking, and human-centered cybersecurity (Gao, 2025; Gao & Gao, 2025; Gao et al., 2026; Malomo et al., 2025). The present paper extends that work by focusing specifically on financial resilience and financial security education.

Methodology

This paper uses a conceptual design-science methodology. Design-science research is appropriate when the goal is to create and justify an artifact, model, method, or framework that addresses a relevant problem (Hevner et al., 2004). In this paper, the artifact is the HBCU Financial Resilience Education Framework. The goal is not to test a single intervention with experimental data, but to design a practical, research-informed framework to guide future curriculum development, classroom implementation, faculty development, and empirical assessment.

The methodology includes four phases: problem identification, literature synthesis, framework design, and implementation planning. First, the problem is defined as the gap between the complexity of modern financial systems and the financial security preparation available to many learners. Second, the literature synthesis draws from financial literacy, digital financial literacy, FinTech education, blockchain and digital trust, cybersecurity and human factors, and generative AI in education. Third, the framework is designed using principles of human-centeredness, practicality, digital trust, AI responsibility, cybersecurity integration, scalability, and measurable learning outcomes. Fourth, implementation planning translates the framework into six curriculum modules, sample activities, classroom safeguards, and an

assessment plan that HBCU programs can adapt to existing business, computer information systems, cybersecurity, data science, and interdisciplinary courses.

The architectural design of the HBCU Financial Resilience Education Framework (HBCU-FREF) is fundamentally grounded in Design Science Research (DSR) theory (Hevner et al., 2004). Rather than serving as a purely descriptive model, the framework operates as an instructional artifact developed through iterative, socio-technical design cycles. By anchoring our six core pillars in the NIST Cybersecurity Framework 2.0 and the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) (National Institute of Standards and Technology [NIST], 2024), the model systematically justifies the intersection of technical risk mitigation with systemic consumer asset protection.

Because this is a conceptual paper, the quality of the contribution depends on relevance, theoretical grounding, internal coherence, practical utility, and potential for future evaluation. The design artifact is therefore presented with competency maps, modular learning activities, technology-use safeguards, and assessment measures that can be tested through pilot workshops, course modules, pre- and post-assessments, student reflections, and community outreach studies.

Proposed Framework: The HBCU Financial Resilience Education Framework

This paper proposes the HBCU Financial Resilience Education Framework, abbreviated as HBCU-FREF. The framework integrates six pillars: financial foundations, FinTech literacy, blockchain and digital trust, generative AI-supported decision learning, cybersecurity and fraud prevention, and community-centered resilience. The framework treats financial resilience as the central outcome. Each pillar contributes a different competency set, and the combined model emphasizes secure, ethical, and informed participation in modern financial ecosystems. Figure 1 illustrates the conceptual structure of HBCU-FREF.

Figure 1

Conceptual Structure of the HBCU Financial Resilience Education Framework

Financial Foundations
FinTech Literacy <-> Blockchain and Digital Trust
Generative AI-Supported Decision Learning
Cybersecurity, Privacy, and Fraud Prevention
Community-Centered Financial Resilience
Outcome: Financial Resilience and Digital Trust

Framework Pillars

The framework is organized around six pillars. Financial foundations provide essential knowledge about budgeting, debt, credit, savings, investing, retirement, taxes, and risk. FinTech literacy prepares learners to evaluate digital banking, mobile payments, online lending, robo-advising, digital wallets, and AI-enabled financial services. Blockchain and digital trust introduce ledgers, hashing, consensus, wallets, private keys, smart contracts, tokenization, and the limits of technological trust. Generative AI-supported decision learning teaches learners to use AI for explanation, practice, and reflection while verifying outputs and protecting privacy. Cybersecurity and fraud prevention prepare learners to recognize phishing, identity theft, account takeover, investment scams, and AI-enabled social engineering. Community-centered resilience extends the learning model to workshops, outreach, student research, faculty development, staff training, alumni engagement, and local community education.

A simple classroom rule for AI-supported financial learning is Ask, Verify, Protect, Reflect. Learners may ask AI for explanations, examples, or questions; verify outputs using reliable sources and calculations; protect private financial data; and reflect on what is useful, risky, or still uncertain. This rule positions generative AI as a learning partner rather than a substitute for qualified financial, legal, tax, or investment advice.

Results / Findings: Curriculum Model, Competency Map, and Learning Outcomes

Because this is a conceptual design paper, the findings are presented as design rather than empirical. The central design finding is that financial resilience education can be strengthened when financial literacy, digital trust, AI literacy, cybersecurity, and community engagement are taught together rather than separately. Table 1 maps the six framework pillars to competencies, outcomes, and sample learning activities.

Table 1*Competency Map for Financial Resilience Education*

Framework Pillar	Core Competency	Sample Learning Outcome	Example Activity
Financial foundations	Budgeting, debt, credit, investing, retirement	Compare short-term and long-term financial tradeoffs.	Build a monthly budget and debt repayment plan.
FinTech literacy	Digital payments, apps, online banking, robo-advising	Evaluate benefits and risks of FinTech tools.	Compare digital payment apps using security and fee criteria.
Blockchain and digital trust	Ledgers, consensus, wallets, smart contracts	Explain how blockchain systems attempt to create trust.	Simulate a blockchain ledger in a spreadsheet or Python.
Generative AI decision learning	AI prompting, verification, privacy, reflection	Use AI to support financial learning while checking accuracy.	Ask AI to explain compound interest, then verify calculations.
Cybersecurity and fraud prevention	Phishing, identity theft, account security, recovery	Recognize scams and identify safe responses.	Analyze suspicious messages and create a fraud response plan.
Community resilience	Outreach, peer education, lifelong learning	Translate financial security knowledge into community education.	Design a one-page guide or mini-workshop.

Table 2 translates the competency map into a sample six-module curriculum that can be adapted for a course unit, a workshop series, a first-year experience module, a business analytics project, a cybersecurity lab, or a community outreach program.

Table 2*Sample Six-Module Curriculum*

Module	Topic	Key Concepts	Technology Integration	Assessment
1	Financial resilience basics	Budgeting, savings, emergency funds, inflation	Spreadsheet or Python budget model	Budget scenario and reflection
2	Debt, credit, and student loans	Interest, credit scores, repayment plans	Loan calculator in Google Colab	Debt comparison worksheet
3	Investing and retirement	Risk, diversification, compounding, retirement accounts	AI-assisted explanation plus manual verification	Investment myth analysis
4	FinTech and digital payments	Mobile payments, fees, privacy, account security	App comparison matrix	FinTech evaluation report
5	Blockchain and digital trust	Ledgers, hashes, wallets, smart contracts	Simple blockchain simulation	Concept map and quiz
6	Cybersecurity and AI safety	Phishing, scams, AI hallucinations, privacy	AI-generated scam detection activity	Fraud response plan

Expected Learning Outcomes

- Explain key financial concepts such as interest, inflation, debt, credit, savings, investment risk, and retirement planning.
- Use basic quantitative tools to compare financial decisions.
- Evaluate FinTech tools in terms of usability, cost, privacy, and security.
- Explain the role of blockchain in digital trust and identify risks associated with digital assets.
- Use generative AI responsibly for financial learning while verifying outputs.
- Recognize common financial scams and cybersecurity threats.
- Develop a personal financial security checklist.
- Communicate financial security concepts to peers and community members.

Sample Learning Activities

Four classroom-ready activities can operationalize the framework. In an AI-assisted credit card repayment activity, students calculate repayment time and total interest, then compare their work with an AI-generated explanation. In a blockchain ledger simulation, students create a

simple transaction ledger and observe how changes to a record affect trust and integrity. In an AI-generated scam-detection activity, students classify fake bank alerts, investment messages, and student-loan scams, then write safe responses. In a retirement-planning reflection, learners compare early and delayed contributions and discuss uncertainty, inflation, risk, and the need for professional advice when personal decisions become complex.

Discussion

The proposed framework aligns with the themes of blockchain, FinTech, AI, cybersecurity, digital trust, financial inclusion, and education. It treats blockchain as part of a broader trust ecosystem, FinTech as both opportunity and risk, generative AI as a learning support tool, and cybersecurity as a core component of financial security. In this sense, the framework supports engineering trust: secure financial systems require robust technology, responsible institutions, and informed users who can verify claims, protect data, and manage risk.

The HBCU context is central to the framework. HBCUs can connect classroom learning with workforce preparation, faculty development, staff training, student research, alumni engagement, and community outreach. Students can learn to manage credit, loans, digital payments, salaries, and early retirement decisions. Faculty, staff, alumni, and community members can benefit from accessible education on retirement planning, fraud prevention, credit, digital payments, and safe use of AI-supported financial information.

To solidify the model's scholarly positioning, a formal comparative analysis distinguishes the HBCU-FREF from traditional literacy frameworks. Legacy benchmarks—such as the OECD/INFE International Survey configurations—evaluate financial budgeting behaviors independently from technical data protection protocols (OECD, 2023). This isolation leaves minority consumers structurally vulnerable to automated transaction fraud and algorithmic vector scams. The HBCU-FREF fills this gap by executing an analytical system where technological evaluation criteria directly govern deployment decisions, shifting student actions from passive conceptual literacy into proactive risk mitigation.

The framework is intentionally non-stigmatizing. It does not assume that financial challenges result from lack of effort or intelligence. Instead, it recognizes that financial systems are complex and that many people, including highly educated professionals, may need support

with debt, retirement, digital tools, and cybersecurity. A respectful approach can reduce shame, encourage help-seeking, and promote lifelong learning.

A major contribution of the framework is the integration of cybersecurity into financial education. Traditional financial literacy programs may teach budgeting and credit, but omit phishing, account takeover, identity theft, social engineering, and scam recovery. In the digital economy, multifactor authentication, password management, scam detection, and incident response are financial resilience skills.

Implementation and Assessment

The framework can be implemented in several formats: a course unit, a workshop series, a first-year experience module, a business analytics project, a cybersecurity lab, a financial literacy outreach program, or an interdisciplinary certificate component. A practical initial implementation could use a six-week sequence, a two-day workshop, or six embedded activities across an existing course. Suggested tools include spreadsheets, Python or Google Colab notebooks, AI prompt templates, mock financial scenarios, and scam-analysis exercises. To protect learners, activities should use fictional or anonymized data rather than personal financial records.

Assessment should measure knowledge, behavior, confidence, and applied judgment. Suggested measures include a pre- and post-financial literacy quiz, a digital financial literacy self-assessment, a cybersecurity behavior checklist, an AI verification assignment, a scenario-based fraud detection task, a student reflection, a final project, and an optional follow-up survey after three to six months. A minimum evaluation package should include one objective knowledge measure, one applied scenario task, one AI-output verification rubric, and one reflective action plan. This operational matrix establishes a concrete, replicable path for future multi-institutional validation studies, enabling researchers to compile quantitative self-efficacy indices alongside empirical scenario accuracy scores to track long-term instructional efficacy. Assessment should not shame learners; instead, it should help them identify growth, build confidence, and develop practical plans.

Limitations and Future Research

This paper presents a conceptual framework rather than empirical results from a completed intervention. The framework should therefore be tested through pilot workshops, classroom implementations, pre- and post-assessments, qualitative student reflections, faculty

interviews, and community outreach studies. Financial decisions are also highly personal and context-dependent, so educational examples cannot replace professional financial, legal, tax, or investment advice.

Future research can measure changes in financial knowledge, digital financial literacy, AI literacy, cybersecurity awareness, confidence, and behavior. Researchers can compare lecture-based learning, AI-supported tutoring, scenario-based learning, and project-based learning. Future work can also develop open educational resources, Google Colab notebooks, AI prompt libraries, scam detection exercises, and blockchain simulations for HBCUs and other minority-serving institutions.

Conclusion

Financial resilience is a critical educational outcome in the generative AI and FinTech era. Students, faculty, staff, and community members face complex decisions involving debt, credit, budgeting, retirement, digital payments, online fraud, blockchain systems, and AI-generated financial information. HBCUs can lead in this area by developing practical, human-centered, and technology-enhanced financial security education.

This paper proposed the HBCU Financial Resilience Education Framework, which integrates six pillars: financial foundations, FinTech literacy, blockchain and digital trust, generative AI-supported decision learning, cybersecurity and fraud prevention, and community-centered resilience. The framework supports interdisciplinary teaching, faculty development, student research, and community engagement. It emphasizes responsible AI use, verification, privacy protection, and practical cybersecurity behaviors.

The central message is that financial resilience education should not be limited to facts about personal finance. It should prepare learners to navigate digital financial systems securely, evaluate emerging technologies critically, and make informed decisions across the life course. By integrating generative AI, FinTech, blockchain, and cybersecurity education, HBCUs can help build more financially resilient individuals, institutions, and communities.

Data availability

No new datasets were generated or analyzed in this conceptual paper.

Funding statement

This research received no direct external funding.

Conflict of interest

The authors declare no conflict of interest.

Acknowledgment

This paper was inspired by the Fifth and Sixth Annual National HBCU Blockchain, FinTech, and AI Conferences. The authors' research, teaching, and service have benefited greatly from the insights, collaborations, and professional engagement fostered by these conferences.

Part of this research was conducted while the second author was a visiting scholar at the Institute for Mathematical and Statistical Innovation (IMSI) at the University of Chicago, which is supported by the National Science Foundation under Grant No. DMS-2425650.

References

- Atkinson, A., & Messy, F.-A. (2012). Measuring financial literacy: Results of the OECD/International Network on Financial Education pilot study. OECD Working Papers on Finance, Insurance and Private Pensions, No. 15. OECD Publishing.
<https://doi.org/10.1787/5k9csfs90fr4-en>
- Board of Governors of the Federal Reserve System. (2026). Economic well-being of U.S. households in 2025. <https://doi.org/10.17016/8960.2>
- Consumer Financial Protection Bureau. (2015). Financial well-being: The goal of financial education.
https://files.consumerfinance.gov/f/201501_cfpb_report_financial-well-being.pdf
- Gao, S. (2025). A framework for integrating blockchain, AI, and generative AI into computer programming education at HBCUs. *Journal of Technology Research*, 13, Article 254038.
<https://www.aabri.com/manuscripts/254038.pdf>
- Gao, W., & Gao, S. (2025). Integrating generative AI and foundational skills for investment and financial decision-making. In H. R. Arabnia, L. Deligiannidis, F. Shenavarmasouleh, S. Amirian, & F. Ghareh Mohammadi (Eds.), *Computational science and computational intelligence (Communications in Computer and Information Science, Vol. 2504)*, pp. 182–191). Springer. https://doi.org/10.1007/978-3-031-94943-2_14
- Gao, W., Gao, S., Allagan, J. D., Su, J., McClinton, B., Eyob, E., & Strevel, H. B. (2026). Investment decision-making in the AI era. In H. R. Arabnia, L. Deligiannidis, S. Amirian, F. Ghareh Mohammadi, & F. Shenavarmasouleh (Eds.), *AI revolution: Research, ethics and society (Communications in Computer and Information Science, Vol. 2722)*, pp. 499–511). Springer. https://doi.org/10.1007/978-3-032-12930-7_35

- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Lo, A. W., & Ross, J. (2024). Can ChatGPT plan your retirement? Generative AI and financial advice. *Harvard Data Science Review*, Special Issue 5. <https://doi.org/10.1162/99608f92.ec74a002>
- Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. *Journal of Economic Literature*, 52(1), 5–44. <https://doi.org/10.1257/jel.52.1.5>
- Malomo, O. O., Gao, S., Adekoya, A. A., Donald, A. M., Andrews, T., Jr., Allagan, J. D., Gao, W., Su, J., & Eyob, E. (2025). Toward human-centric cybersecurity: Case study insights and the HuCRAF model. *International Journal of Cybersecurity and Risk Assessment*, 1(1), 1–61. <https://doi.org/10.4018/IJCRA.389592>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>
- National Institute of Standards and Technology. (2024a). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.600-1>
- National Institute of Standards and Technology. (2024b). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Organisation for Economic Co-operation and Development. (2023). OECD/INFE 2023 international survey of adult financial literacy. OECD Publishing. <https://doi.org/10.1787/56003a32-en>
- Yakoboski, P. J., Lusardi, A., Sticha, A., & Mastry, F. (2026). A decade of tracking financial literacy in America: Findings from the 2026 TIAA Institute-GFLEC Personal Finance Index. TIAA Institute and Global Financial Literacy Excellence Center. <https://www.tiaa.org/public/institute/publication/2026/tiaa-gflec-personal-finance-index>