

The Financial System Is Changing

What Consumers Should Know About the Infrastructure Shaping How Money Moves

UNDERSTAND • QUESTION • CHOOSE

A PLAIN-LANGUAGE ORIENTATION

About this guide

This guide explains how financial infrastructure is changing, what five major developments may mean for consumers, where risks can arise, and which questions can support more informed decisions. It is written for a general audience and does not require specialist knowledge.

Important notice

This publication is for general educational purposes. It does not provide investment, legal, tax, cybersecurity, or personalized financial advice; recommend a provider, product, asset, or technology; or describe the law of every jurisdiction. Services, protections, and regulatory requirements differ by provider and location and may change. Readers should verify current terms and protections and seek qualified advice where appropriate.

Research method

ThinkDeFi reviewed material definitions, technology descriptions, potential benefits, risks, and legal-adjacent statements against primary standards, official regulatory and multilateral publications, and authoritative consumer guidance available through 14 September 2026. Consequential claims were triangulated where appropriate. The review distinguishes documented evidence from conditional possibilities and ThinkDeFi institutional interpretation. This guide is a documentary evidence synthesis, not original empirical research, a systematic review, or jurisdiction-specific legal analysis. Source selection prioritized primary and authoritative materials; vendor marketing and unsourced statistics were excluded.

Contents

- 1 The Financial System Around You
 - 2 Why the System Is Changing
 - 3 Five Changes Consumers Should Understand
 - 4 What These Changes Could Improve
 - 5 Where Consumers Could Be Exposed
 - 6 The Human Layer
 - 7 Questions to Ask Before You Trust a Financial Service
 - 8 Consumer Readiness Checklist
 - 9 The Financial Future Is Also a Human Decision
- Sources

The Financial System Around You

Most people interact with financial infrastructure every day without seeing it. A card payment, direct deposit, money transfer, loan decision, or identity check may feel like one simple action. Behind that action, several organizations and technologies may be communicating, verifying information, moving value, and deciding whether the transaction can proceed. [6]

This infrastructure includes banks, payment networks, technology providers, identity systems, data services, regulators, and other institutions. It determines how money enters an account, how quickly a payment arrives, what information is collected, and what happens when something goes wrong. [6, 18]

Much of this system was built in separate layers over many years. Some arrangements support near-real-time processing, while others remain constrained by operating windows, manual review, or reconciliation across separate records. A service can therefore look seamless while responsibility behind it remains divided. [6, 13]

As of September 2026, several developments are advancing at different rates. Faster-payment initiatives are modernizing domestic and cross-border transfers. [13] Artificial intelligence is being used in consumer-facing and institutional financial functions. [3, 10] Digital identity tools increasingly support remote verification. [4, 11] Platform-based services are combining financial and nonfinancial activities. [15] Money and other assets are also being represented on programmable platforms. [2]

Consumers do not need to become technologists to participate. They do, however, deserve to understand the relationships that affect their identity, money, data, and choices. This guide explains five important developments, what they could improve, where consumers may be exposed, and the questions that help make an unfamiliar service easier to evaluate.

2

Why the System Is Changing

The financial system is changing in response to several forces, including changing expectations, competition, policy priorities, and infrastructure modernization. People increasingly expect services to be available through digital channels and across conventional operating hours. Businesses and institutions are seeking more efficient payments and records, stronger fraud controls, and modernized systems. [5, 6]

Technology is also making different forms of coordination possible. Cloud infrastructure and application programming interfaces can connect services and support delivery at scale. [6] Shared programmable records can coordinate information and asset transfers among participants. [2] Artificial intelligence can detect patterns and assist with decisions, while digital identity tools can support remote verification. [3, 4, 10, 11]

Competition adds another force. Technology companies, financial institutions, digital-asset businesses, retailers, and platforms are offering financial functions in new combinations. A consumer may now encounter payments, credit, insurance, or account services inside a broader commercial experience. The structures and regulatory roles within these arrangements vary. [15]

Policy priorities are changing as well. Governments and international bodies are examining payment speed, cross-border cost, financial inclusion, cybersecurity, data use, operational resilience, and the regulation of emerging assets. [6, 9, 13, 18] The rules are not identical across countries, and they continue to evolve.

These forces do not mean that every part of finance will be replaced. New systems often connect with existing institutions, laws, currencies, and payment networks. ThinkDeFi's assessment is that established and emerging infrastructure will continue to operate together in a mixed environment. [6]

For consumers, the central change is not simply that finance is becoming digital. Financial activity is becoming more connected, automated, and embedded in ordinary life. That can improve the experience, but it can also make the underlying provider, decision, or protection harder to identify.

3

Five Changes Consumers Should Understand

Five developments provide a useful foundation for understanding this changing infrastructure. Each may create benefits, but none carries the same design, protections, or level of maturity in every service or jurisdiction.

Stablecoins

Stablecoins are digital assets designed to maintain a stable value relative to a reference asset, often a national currency. The word stable describes the intended design, not a guarantee. Stabilization mechanisms, reserves, redemption terms, governance, and legal obligations vary by arrangement. International authorities focus on effective stabilization, redemption, governance, risk management, cybersecurity, and financial integrity. [1, 9]

Consumers may encounter stablecoins in wallets, digital-asset platforms, payment applications, or cross-border transfers. Some arrangements may support faster or round-the-clock transfer, including in certain cross-border uses; actual speed, cost, settlement, and redemption depend on the arrangement. Risks can include loss of value, unclear reserves, restricted redemption, or compromised custody. Protections may differ from deposit protections and vary by product, provider, and jurisdiction. [1, 9, 16] Ask who issues the asset, what supports it, how redemption works, who holds the reserves, and what happens if the issuer or platform fails.

Tokenization

Tokenization represents money, an asset, or certain rights through a digital record on a programmable platform. A token may represent an asset, a claim, or permission to act; its legal effect depends on the system, governing documents, and applicable law. A digital record does not by itself determine legally enforceable ownership. Tokenization does not remove the need for enforceable rights, custody, accurate records, or reliable valuation. [2, 14]

A consumer might encounter tokenization through different forms of investment, wallet, or digitally represented asset service; these examples may not share the same legal or technical model. Tokenization may make some assets easier to transfer, divide, or track, depending on design and law. [2, 14] Before participating, ask what the token legally represents, who controls the underlying asset, whether it can be sold or redeemed, which record establishes ownership, and what happens if the platform closes.

Artificial Intelligence

Artificial intelligence systems generate predictions, recommendations, classifications, or content using data and computational models. As of September 2026, financial organizations use or are testing these systems for functions that include fraud detection, customer assistance, application assessment, transaction monitoring, and personalization. [3, 10]

AI can improve speed and pattern detection, but outputs can be wrong, difficult to explain, or affected by incomplete or historically biased information. These risks and their severity vary by system, data, purpose, and governance. Trustworthy use requires attention to reliability, transparency, privacy, fairness, security, and accountability. [3, 10] ThinkDeFi recommends that consumers ask whether automation influenced an important outcome, what information was used, how errors can be corrected, and whether an effective review or escalation path is available.

Digital Identity

Digital identity systems help an organization determine whether a person is who they claim to be. They may combine identity proofing, credentials, devices, authentication, biometrics, and recovery processes. [4] Consumers encounter them when opening accounts, uploading identification, taking a facial image, using a passkey, or completing multifactor authentication.

Well-designed digital identity systems may improve remote access and help address some forms of fraud when assurance, accessibility, privacy, and recovery controls are effective. Poorly designed or implemented systems can create privacy, security, exclusion, and account-recovery risks. [4, 11, 12] Ask what information is collected, why it is necessary, who can access it, how long it is retained, and what alternative exists if verification fails.

Embedded Finance

Definitions of embedded finance vary. In this guide, the term describes payments, credit, insurance, savings, or other financial functions offered within a primarily nonfinancial experience. A retailer, travel application, marketplace, or software platform may present the experience while another organization provides the underlying financial service. Platform-based models differ materially in structure and oversight. [15]

Embedding may reduce friction, but it can also make the provider relationship or financial decision less visible. Depending on the design, a consumer may need to look carefully to determine whether they are borrowing, authorizing recurring payments, or sharing financial data. This is a bounded consumer-risk hypothesis rather than a claim about every embedded service. ThinkDeFi recommends asking which company provides the service, what transaction is taking place, what it costs, who receives the information, and who resolves an error or dispute. [10, 17]

4

What These Changes Could Improve

New financial infrastructure is valuable only when it solves real problems for people. When responsibly designed, it could improve speed, cost, access, responsiveness, security, records, and choice. These outcomes are possible, not automatic.

Faster movement of money could help people receive wages, family transfers, or emergency funds sooner. Modern systems may reduce reconciliation delays and allow some transactions outside traditional business hours. Some faster-payment transactions provide little time for intervention, while technical finality and legal recovery rights depend on the payment rail, authorization, transaction type, and jurisdiction. [13]

Automation and more connected infrastructure could lower administrative and intermediary costs. Consumers might see less expensive transfers or services that were previously uneconomic to provide. Lower provider cost does not necessarily produce lower consumer cost; this is an economic possibility whose outcome depends on competition, pricing, and product design. Consumers should therefore consider subscriptions, currency spreads, withdrawal charges, and the total price of the service. [5]

Digital delivery can expand access for people far from a branch or working nontraditional hours. The World Bank notes that digital financial services can lower costs and increase speed, security, transparency, and access, while also introducing privacy, predatory-lending, cybersecurity, and unequal-access risks. [5] Availability online is not true inclusion when people lack reliable connectivity, accepted identification, accessible design, or a workable alternative.

AI and data analysis may improve fraud alerts, language assistance, and customer response, depending on the model, data, and governance. [3, 10] Shared records may make some transactions easier to trace and reconcile, depending on system design and legal arrangements. [2, 6] Competition may give consumers more choices. Each benefit depends on understandable terms, reliable governance, and effective assistance when the technology does not work as intended.

5

Where Consumers Could Be Exposed

New technology can reduce certain risks while creating others or moving responsibility to places consumers may not expect. The goal is informed caution, not avoidance of innovation.

Responsibility may be divided among an application provider, bank, processor, identity company, data service, or custodian. Third-party dependencies can increase operational complexity. When roles are not clearly disclosed, consumers may struggle to identify the party able to resolve a problem. [6, 18] They should be able to identify who provides the product, who holds the money, who secures the account, and who resolves complaints and errors.

Faster and cross-border payment environments can shorten intervention time in some fraud scenarios. [13] Separately, synthetic voices and other manipulated communications can make impersonation attempts more convincing. [19] Whether a payment can be recalled or recovered depends on whether it was authorized, the payment rail, applicable rules, and jurisdiction. Urgency, secrecy, guaranteed returns, unfamiliar payment methods, and requests for passwords or verification codes should trigger a pause and independent verification. [8]

Protections can vary among a bank deposit, payment account, wallet balance, stablecoin, and tokenized asset, depending on the product, provider, transaction, and jurisdiction. Insurance, redemption, reversibility, complaint rights, and governing law should never be assumed from a familiar interface or brand. [9, 16]

Depending on the service and permission structure, digital providers may collect identity, device, location, spending, or behavioral information and may infer additional information. Data can support security and personalization, but it can also be breached, shared, retained, or misinterpreted. [3, 4, 10] ThinkDeFi recommends clear information about collection, use, correction, sharing, and retention; applicable privacy rights vary by jurisdiction.

Automated decisions can rely on inaccurate or incomplete data and may be difficult to explain. [3, 10] ThinkDeFi considers notice, correction, explanation, and a practical escalation path important safeguards when automation materially affects a consumer. Applicable legal rights vary by use case and jurisdiction. [20]

Digital systems can exclude people who lack current devices, accepted documents, stable connectivity, or digital confidence. [5, 12] They can also fail through outages, software errors, cyberattacks, or concentration among third-party providers. [6, 18] ThinkDeFi considers accessible alternatives, recovery procedures, timely communication, and clear accountability important safeguards for essential services.

6

The Human Layer

Financial infrastructure is often described through networks, ledgers, algorithms, assets, and platforms. Yet every system is built, governed, and experienced by people. ThinkDeFi defines the Human Layer as the point where financial infrastructure meets human life and proposes it as an evaluative framework.

The framework asks whether people can understand what is happening, make a meaningful choice, identify responsibility, obtain help, challenge a consequential decision, and recover access to their identity or money. It is a ThinkDeFi institutional framework, not yet an empirically validated scholarly construct. A system may be technically advanced and still perform poorly against these proposed criteria.

As a proposed design principle, the Human Layer treats agency as more than clicking 'I agree.' Financial moments should remain visible when money moves, credit is offered, automation influences a decision, personal information is shared, permission continues, or an action may be difficult to reverse. Good design helps people understand an action before completing it. [3, 10]

Dignity requires recognizing the person behind the transaction. A frozen or restricted account may interrupt access to money needed for food, housing, work, or family support. Official consumer-protection analysis has documented the importance of timely access and effective error resolution. [21] People are not complete data profiles, and needing assistance is not a consumer failure.

ThinkDeFi's framework holds that technology does not remove organizational responsibility. Organizations choose the systems, data, standards, and actions that follow, although specific legal duties vary. Consumers should be able to learn what materially influenced an outcome, who can correct an error, and what remedy exists. Complex systems require clearer accountability, not less. [3, 10]

For consequential disputes involving identity, money, rights, or participation, ThinkDeFi treats effective recourse as a core test. Effective recourse should be accessible and timely, reach a party with authority to act, provide an understandable explanation, and offer an appropriate remedy or escalation route. Human review may be important in some cases, but well-designed nonhuman remedies can also resolve routine problems effectively.

The future should be measured not only by what systems can do, but by what people become more capable of doing. If forced to choose between making a financial system more impressive and making it more human, choose human.

7

Questions to Ask Before You Trust a Financial Service

Trust should be supported by clear information rather than dependence on what consumers cannot see. Before opening, connecting, or funding a service, ask the following questions.

This question set synthesizes guidance from financial, identity, cybersecurity, and consumer-protection authorities. It is general educational guidance, not a statement of universal legal rights. [1-21]

Who provides the service

What company presents the product? Is another bank, lender, insurer, processor, custodian, or technology provider delivering the financial function? Who is responsible when it fails?

Who holds or controls the money

Where will the funds or assets be held? Does the consumer retain control, or does a provider control access? What happens if the provider becomes insolvent, closes, or loses access?

What protections apply

Are funds insured or otherwise protected? Can an unauthorized or mistaken transaction be disputed or reversed? What redemption, complaint, and escalation rights exist, and which jurisdiction governs them?

What will it cost

Consider the full cost: fees, interest, subscriptions, withdrawal charges, currency conversion, expedited service, and penalties. Are costs presented before commitment?

What happens to identity and data

What information is required, why is it collected, who receives it, and how long is it kept? Can inaccurate data be corrected? What recovery path exists if a device or credential is lost?

Does automation influence the outcome

Does an automated system affect approval, pricing, fraud decisions, or account access? Can the main reason be explained? Can a person review or change an incorrect result?

What happens when something goes wrong

Is support reachable through a verified channel? Who has authority to act? How quickly will the organization respond, and what further escalation is available?

8

Consumer Readiness Checklist

Use this checklist before opening, connecting, or funding an unfamiliar financial service, and return to it periodically after enrollment. These steps can reduce exposure but cannot substitute for provider duties, effective regulation, or access to remedy.

Before you begin

- ☐ Understand what the service does and does not do.
- ☐ Identify the provider and independently verify its contact information.
- ☐ Confirm who will hold or control your money, assets, and personal information.

Understand the terms

- ☐ Review total cost, including fees, interest, subscriptions, withdrawals, and currency conversion.
- ☐ Determine whether funds or assets are insured, protected, redeemable, or reversible.
- ☐ Identify the governing jurisdiction and the process for closing the account.

Protect your access

- ☐ Use a unique, strong password and multifactor authentication when available. [7]
- ☐ Protect verification codes, recovery phrases, and backup information.
- ☐ Keep devices and applications updated. Never move money to protect it at an unexpected caller's instruction. [8]

Start carefully and monitor

- ☐ As a general risk-management practice, test an unfamiliar service with limited exposure before depending on it.
- ☐ Confirm that transfers, withdrawals, or redemption work as expected.
- ☐ Review transactions, connected applications, recurring permissions, and security alerts.

If something goes wrong

- ☐ Stop further transactions and contact the provider through a verified channel.
- ☐ Preserve messages, receipts, transaction identifiers, screenshots, and dates.
- ☐ Change compromised credentials and report suspected fraud to the appropriate institution or authority.

9

The Financial Future Is Also a Human Decision

A payment made from a phone may appear simple. Depending on the service, it may involve an identity check, automated fraud review, several providers, a payment network, and rules determining whether the transaction can be stopped or corrected. [6, 13]

Consumers do not need to understand every technical layer. They deserve enough information to know what is happening, make meaningful choices, and seek help when something goes wrong.

From ThinkDeFi's perspective, the financial future is being shaped by decisions about access, privacy, control, responsibility, and whose needs the system serves. Institutions, developers, policymakers, and technology providers make many of these decisions. Consumers may also influence the future through the services they choose, questions they ask, permissions they grant, and standards they expect.

Innovation should make people more capable, not merely make systems more powerful. Progress should be measured by whether people can understand, trust, challenge, and recover from the infrastructure around them.

The defining question is not simply, What can this technology do? It is: What should people become more capable of doing because this technology exists?

ThinkDeFi Public Guides will continue exploring that question, helping readers understand the systems shaping financial life and the human choices embedded within them.

EVIDENCE BASE

Sources

Sources support the definitions and factual statements identified in the text. ThinkDeFi analysis and the Human Layer framework are presented as institutional interpretation.

1. Financial Stability Institute. Stablecoins: regulatory responses to their promise of stability. FSI Insights No. 57, 9 April 2024, especially executive summary and sections 2-4.
<https://www.bis.org/publications/fsi-insight-57-stablecoins-regulatory-responses-their-promise-stability.pdf>. Accessed 14 September 2026.
2. Bank for International Settlements. Tokenisation in the context of money and other assets: concepts and implications for central banks. 2024, especially sections 2-4.
<https://www.bis.org/publications/tokenisation-context-money-and-other-assets-concepts-and-implications-central-banks.pdf>. Accessed 14 September 2026.
3. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework. NIST AI 100-1, January 2023, sections 3-5. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>. Accessed 14 September 2026.
4. National Institute of Standards and Technology. Digital Identity Guidelines. NIST SP 800-63-4, July 2025, sections 3-5.
<https://pages.nist.gov/800-63-4/sp800-63.html>. Accessed 14 September 2026.
5. World Bank Group. Financial Inclusion. Institutional topic summary and linked Global Index materials.
<https://www.worldbank.org/ext/en/topic/financial-sector/financial-inclusion>. Accessed 14 September 2026.
6. Bank for International Settlements. Digitalisation of finance. 2024, chapters on digital intermediation, data, operational risk and policy. <https://www.bis.org/publications/digitalisation-finance.pdf>. Accessed 14 September 2026.
7. Cybersecurity and Infrastructure Security Agency. Secure Our World. Guidance on strong passwords, multifactor authentication, phishing and software updates. <https://www.cisa.gov/secure-our-world>. Accessed 14 September 2026.
8. Federal Trade Commission. Never move your money to protect it. That is a scam. 6 March 2024.
<https://consumer.ftc.gov/consumer-alerts/2024/03/never-move-your-money-protect-it-thats-scam>. Accessed 14 September 2026.
9. Financial Stability Board. High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements. 17 July 2023, Recommendations 2-9. <https://www.fsb.org/uploads/P170723-3.pdf>. Accessed 14 September 2026.
10. Organisation for Economic Co-operation and Development. Artificial intelligence and personal finance. OECD Business and Finance Policy Papers, September 2026.
https://www.oecd.org/en/publications/artificial-intelligence-and-personal-finance_2858fdf4-en.html. Accessed 14 September 2026.
11. Financial Action Task Force. Guidance on Digital Identity. March 2020, especially sections II-IV.
<https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html>. Accessed 14 September 2026.
12. World Bank. Principles on Identification for Sustainable Development: Toward the Digital Age. First edition, 2021, principles on inclusion, design, privacy and grievance mechanisms. <https://documents1.worldbank.org/curated/en/614981614634836160/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age-First-Edition.pdf>. Accessed 14 September 2026.
13. Committee on Payments and Market Infrastructures. Enhancing cross-border payments: addressing fraud in cross-border payments. 2026, sections on fraud typologies, intervention and payment-chain controls.
<https://www.bis.org/pages/cpmi-cross-border-payments-programme/pietf-fraud-report-2026.pdf>. Accessed 14 September 2026.
14. UNIDROIT. Principles on Digital Assets and Private Law. 2023, Principles 3-10 and commentary.
<https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>. Accessed 14 September 2026.

15. Bank for International Settlements. Platform-based business models and financial inclusion. BIS Working Papers No. 986, December 2021.
<https://www.bis.org/publications/working-paper-986-platform-based-business-models-and-financial-inclusion.pdf>. Accessed 14 September 2026.
16. Federal Deposit Insurance Corporation. What the Public Needs to Know About FDIC Deposit Insurance and Crypto Companies. 28 July 2022. United States example only. <https://www.fdic.gov/sites/default/files/2024-03/crypto-fact-sheet-7-28-22.pdf>. Accessed 14 September 2026.
17. Organisation for Economic Co-operation and Development. Consumer Finance Risk Monitor 2026. September 2026, sections on digital financial services and consumer conduct.
https://www.oecd.org/en/publications/consumer-finance-risk-monitor-2026_61f7dbe0-en.html. Accessed 14 September 2026.
18. CPMI and IOSCO. Financial market infrastructures' reliance on third-party service providers: challenges and risks. 2026, sections on concentration, cyber risk and operational dependency.
<https://www.bis.org/publications/cpmi-iosco-fmis-reliance-third-party-service-providers-challenges-and-risks.pdf>. Accessed 14 September 2026.
19. Federal Trade Commission. Fighting back against harmful voice cloning. April 2024.
<https://consumer.ftc.gov/consumer-alerts/2024/04/fighting-back-against-harmful-voice-cloning>. Accessed 14 September 2026.
20. Consumer Financial Protection Bureau. Circular 2022-03: adverse action notification requirements in connection with credit decisions based on complex algorithms. 19 May 2022. United States credit context only. <https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/>. Accessed 14 September 2026.
21. Consumer Financial Protection Bureau. Protecting people's access to their money. 26 June 2023. United States consumer-protection context. <https://www.consumerfinance.gov/archive/blog/protecting-peoples-access-to-their-money/>. Accessed 14 September 2026.

About ThinkDeFi

ThinkDeFi is an independent research and convening institution advancing the future of financial infrastructure. Through independent research, executive dialogue, and strategic collaboration, ThinkDeFi works to strengthen human agency and institutional resilience as financial systems evolve.

Advancing the future of financial infrastructure.

thinkdefi.org