Monetary and Economic Studies

Vol. 44 November 2026

Monetary Policy from New Perspectives
A Conference Organized by
the Institute for Monetary and Economic Studies,
Bank of Japan, Held in Tokyo on May 27–28, 2026

Summary ····· Yusuke Oh, Daisuke Ikeda, and Yojiro Ito

Opening Remarks ····· Kazuo Ueda

The Mayekawa Lecture: Challenges to Independence:
How should Central Banks Respond—Lessons from History ····· Donald Kohn

The Presence of Foreign Open–End Funds in Japan's Financial Markets ····· Kenta Yamamoto, Tomohiro Okubo, Nobuhiro Abe, and Yukio Minoura

A Technical Examination of Non-Ledger-Based Payment Systems ····· Yuko Tamura, Masayuki Abe, Tetsuya Okuda, Hiromasa Tsugawa, Toshiyuki Miyazawa, Kazuki Yamamura, Yoshiharu Akahane, Tomoki Taguchi, Yuto Hirakuri, Hiroto Masuda, and Kento Yamada

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

Institute for Monetary and Economic Studies, Bank of Japan

Chief Councillor
Takeo Hoshi
Emeritus Professor, The University of Tokyo

Councillors
Hideki Kanda
Emeritus Professor, The University of Tokyo
Atsuko Miyaji
Professor, The University of Osaka
Makoto Nirei
Professor, The University of Tokyo
Kazuhiko Ohashi
Professor, Hitotsubashi University and Institute of Science Tokyo
Etsuro Shioji
Professor, Chuo University

Honorary Advisers
Markus K. Brunnermeier
Edwards S. Sanford Professor of Economics, Princeton University
Athanasios Orphanides
Professor of the Practice, Global Economics and Management, Massachusetts Institute of Technology

Director-General
Shingo Watanabe

Monetary and Economic Studies (ISSN 2759-5102) is published by the Bank of Japan's Institute for Monetary and Economic Studies (IMES). In line with IMES policy, the publication seeks to provide information on monetary and economic issues to the general public. Articles include research achievements by the staff and visiting scholars, and contributions to conferences sponsored by IMES.

The views expressed in *Monetary and Economic Studies* are those of the authors and do not necessarily reflect those of the Bank of Japan or IMES.

Comments on articles are welcome. All correspondence, including requests for subscriptions, queries about delivery, notice of change of address, and inquiries concerning reprint and translation rights, should be sent to:

Institute for Monetary and Economic Studies (IMES)
Bank of Japan
2–1–1, Nihonbashi-Hongokucho,
Chuo-ku, Tokyo 103–8660, Japan
E-mail: imes.journals-info@boj.or.jp

©2026 by the Institute for Monetary and Economic Studies, Bank of Japan

Monetary and Economic Studies

Vol. 44 November 2026

Contents

1	Monetary Policy from New Perspectives A Conference Organized by the Institute for Monetary and Economic Studies, Bank of Japan, Held in Tokyo on May 27–28, 2026	
1	Summary	Yusuke Oh, Daisuke Ikeda, and Yojiro Ito
29	Opening Remarks	Kazuo Ueda
35	The Mayekawa Lecture: Challenges to Independence: How should Central Banks Respond—Lessons from History	Donald Kohn
47	The Presence of Foreign Open–End Funds in Japan's Financial Markets	Kenta Yamamoto, Tomohiro Okubo, Nobuhiro Abe, and Yukio Minoura
77	A Technical Examination of Non-Ledger-Based Payment Systems	Yuko Tamura, Masayuki Abe, Tetsuya Okuda, Hiromasa Tsugawa, Toshiyuki Miyazawa, Kazuki Yamamura, Yoshiharu Akahane, Tomoki Taguchi, Yuto Hirakuri, Hiroto Masuda, and Kento Yamada
125	General Information	

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

Monetary Policy from New Perspectives:

Summary of the 2026 BOJ-IMES Conference

by Yusuke Oh, Daisuke Ikeda and Yojiro Ito

I. Introduction

The Institute for Monetary and Economic Studies (IMES) of the Bank of Japan (BOJ) held the 2026 BOJ-IMES Conference, entitled "Monetary Policy from New Perspectives," on May 27–28, 2026.[1] This year marked the 31st edition from its start in 1983, and participants discussed a wide range of topics from the conduct of monetary policy to economic analyses.

The conference began with the opening remarks delivered by Kazuo Ueda (BOJ). Next, Donald Kohn (The Brookings Institution) gave the Mayekawa Lecture. Markus Brunnermeier (Princeton University) delivered a keynote speech. Also, Philip Jefferson (Federal Reserve Board), Philip R. Lane (European Central Bank: ECB), and Ryozo Himino (BOJ) had a fireside chat on monetary policy and supply shocks. In the paper presentation sessions, four papers were presented on the theoretical and empirical analyses of monetary policy, by David López-Salido (Banco de España), Şebnem Kalemli-Özcan (Brown University), Iván Werning (Massachusetts Institute of Technology), and Daisuke Ikeda (BOJ).

The conference had two policy panel discussions. The first one was moderated by Takeo Hoshi (The University of Tokyo) and the four panelists, Pierre-Olivier Gourinchas (International Monetary Fund: IMF), Andrew Hauser (Reserve Bank of Australia), Lorie Logan (Federal Reserve Bank of Dallas), and Eli Remolona Jr. (Bangko Sentral ng Pilipinas), discussed monetary policy and imbalances. The second one was moderated by Athanasios Orphanides (Massachusetts Institute of Technology), and the five panelists, Piti Disyatat (Bank of Thailand), Austan Goolsbee (Federal Reserve Bank of Chicago), M. Ayhan Kose (The World Bank Group), Clare Lombardelli (Bank of England: BOE), and Koji Nakamura (BOJ), discussed monetary policy in a changing world economy.

Yusuke Oh: Deputy Director, Institute for Monetary and Economic Studies, Bank of Japan
(E-mail: yuusuke.ou@boj.or.jp)
Daisuke Ikeda: Head of Economic and Financial Studies Division, Institute for Monetary and Economic Studies, Bank of Japan (E-mail: daisuke.ikeda@boj.or.jp)
Yojiro Ito: Director, Institute for Monetary and Economic Studies, Bank of Japan
(E-mail: youjirou.itou@boj.or.jp)

The conference organizers wish to express their sincere gratitude to conference participants for the thought-provoking presentations and discussions. The views expressed throughout this summary are those of the attendants and do not necessarily reflect those of their respective institutions. All remaining errors are the authors' responsibility.

1. See Appendix 1 for the program. See Appendix 2 for a list of participants; their affiliations are as of May 27–28, 2026.

II. Opening Remarks

Ueda shared some thoughts on Japan's experience with major energy shocks over the past five decades.[2] He said that supply shocks loomed large in everyone's mind and that revisiting past experience was an indispensable starting point for discussions. He identified five notable spikes in energy prices since the 1970s and noted that the impact on inflation in Japan was different in each case.

Beginning with the first oil shock of 1973, he noted that the economy had been already overheated when the shock hit, leading to a typical wage-price spiral, and stressed that wages were the most important transmission channel. He added that monetary tightening came after high inflation dynamics had already developed. He contrasted the second oil shock of 1979–80, which led to far more moderate inflation. He pointed out that not only a monetary policy response was more prompt but initial conditions were more favorable: inflation was lower; wages were more restrained; firms and labor unions learned from the first shock; earlier yen appreciation cushioned import prices; and firms had begun to improve energy efficiency and reduce oil dependence.

He noted that oil prices rose substantially in the mid- to late-2000s, but this resulted little change in underlying inflation because the Japanese economy had fallen into a deflationary equilibrium by this time. He added that higher oil prices mainly operated as a tax on real income, raising costs for firms and prices for consumers, but they did not generate a sustained rise in wages or expectations.

He turned to the recent episode, beginning around 2021, noting that an external cost shock was not temporary: price increases broadened, firms became more willing to pass on higher costs, and wage growth and inflation expectations moved up. However, he pointed out that this did not bring about an early-1970s-style wage-price spiral, with medium- to long-term inflation expectations rising only modestly from near zero to around 1.5–2%.

He noted the implication that central banks should not view oil prices in isolation, since their effects depend on wages, expectations, demand, and exchange rates, adding that the boundary between temporary and persistent inflation was not mechanical. He summarized that oil price shocks were tests of the entire inflation regime. Noting that the fifth of these significant energy price spikes was currently under way, he concluded by hoping to hear participants' views on initial conditions, inflation regimes, and the best policy response from central banks around the world.

III. The Mayekawa Lecture: Challenges to Independence: How Should Central Banks Respond—Lessons from History

Kohn delivered the Mayekawa Lecture on central bank independence, drawing on his own experience and the lessons history offers for protecting it.[3] He observed that threats to central bank independence in the United States had risen to levels not seen since the Fed-Treasury accord of 1951. He noted that these concerns extended beyond the United

2. For details, see Ueda (2026).
3. For details, see Kohn (2026).

States, emphasizing that preserving independence had become one of the defining institutional challenges of the moment.

He first explained the meaning of independence. He noted that elected representatives, recognizing that electoral incentives make it difficult to sustain a credible commitment to price stability, had delegated authority to independent central banks with clearly defined objectives. He stressed that this authority had limits in a democracy, with accountability maintained through the give and take between the central bank and elected representatives, while its independence rested on both laws and norms. He noted that protecting independence required that policy disagreement not be grounds for dismissal by the appointing authorities.

He then documented that the political pressure on the Federal Reserve had increased to levels that are unusual in scale and intensity. He added that under the broader economic environment, including rising public, fading disinflationary forces, and adverse supply shocks, the case for independence was likely to become stronger, since political incentives to demand short-run relief grows just as the need for disciplined policy becomes greater.

He explained how central banks found themselves in this situation. He said that across many democracies, populist movements had drawn strength from dissatisfaction with economic outcomes and distrust of technocrats, making central banks particularly vulnerable because they are technocratic institutions by design and their independence constrains elected leaders. He acknowledged that economic events over the past two decades—the Global Financial Crisis and the inflation surge of 2021–23—had reinforced these pressures.

He then turned to what central banks can do despite the challenges they face, focusing on three themes: focus, success, and communication. He argued that central banks should be as successful as possible, focusing on their core legal objectives while avoiding peripheral or politically contested objectives, with accountability underpinned by good communication. Drawing on the three chairs with whom he had worked most closely—Paul Volcker, Alan Greenspan, and Ben Bernanke—he emphasized that successful policy required a disciplined narrative grounded in evidence and essential policymaking virtues: flexibility and humility.

He next addressed two especially difficult challenges. First, on unsustainable fiscal trajectories, he warned that rising debt and persistent deficits could threaten independence well before outright fiscal dominance emerged, and argued that central banks should explain the economic consequences clearly while avoiding prescriptions about how elected officials should close fiscal gaps. Second, on financial stability, he argued that while responsibility is often shared across agencies, central banks should articulate their independent assessment of systemic risk candidly, bringing a distinctive system-wide perspective, even when it differs from the administration's view.

Finally, he concluded that these were difficult times for central banks, but that history offered an encouraging lesson: independence had endured because experience repeatedly demonstrated its value. He emphasized that this insulation could not be taken for granted and must be earned and re-earned through disciplined focus, institutional competence, humility about uncertainty, and a willingness to explain difficult choices clearly.

Neel Kashkari (Federal Reserve Bank of Minneapolis), as chair of the session, asked several questions before opening the floor for discussion. He first asked about accountability after five years of elevated inflation. **Kohn** answered that accountability came from institutions holding themselves to be accountable, adding that such cases included the removal of what he saw as an inflation bias in the 2020 strategic framework and the FOMC's subsequent rapid tightening once it recognized the mistake, while pointing out that the 2025 strategic review fell short of examining the tools used, in particular forward guidance and asset purchases. Asked how candidly experts should admit uncertainty without damaging credibility, he saw a balance, with holding honesty about uncertainty, could be sustained while keeping focus on long-term goals. On whether a single mandate would simplify communication, he disagreed, arguing that price stability was the path to maximum employment, in line with the pre-crisis approach of Volcker, Greenspan, and early Bernanke. On reforming the system so that only monetary policy is formally independent, he said the US was largely there already, but he expressed the need for more evidence that the Fed considers financial stability issues such as deregulation, taking a system-wide macro perspective.

Kashkari opened the floor discussion. **Lombardelli** asked how to reconcile looking through temporary supply shocks with shifting inflation expectations and credibility concerns. **Kohn** responded that price-level changes could be looked through as long as second-round effects are avoided, adding that after five years of above-target inflation, more attention should be given to the risks of second-round effects. **Hauser** asked whether central banks' communication about the economic consequence of fiscal trajectories had had a meaningful impact, even when it was clearly stated. **Kohn** acknowledged that it often did not, but added that it was the only available path, arguing that failure could erode public support for central bank independence. **Kashkari** followed up on how forcefully to communicate given uncertainty about fiscal situations. **Kohn** suggested that one could, for instance, highlight evidence showing how rising debt-to-income ratios increase interest rate burdens, crowd out private investment, and shrink fiscal space. **Gourinchas** raised the issue of potential conflicts between monetary policy and financial stability, adding that regulations might weaken ex-ante if regulatory authorities rely on central bank interventions during crises. **Kohn** expressed support for maintaining the separation principle between monetary policy and financial stability, admitting that there is no easy answer. However, he observed that conflicts were unlikely to emerge during crises, as they are typically accompanied by recessions. **Brunnermeier** asked how to balance central bank communication to the general public and to financial markets. **Kohn** emphasized the importance of keeping trying to reach out to the general public, adding that reaching legislators matters most and public outreach should continue without overreacting. He wondered if the Fed Listens events of 2018–19 had led the Fed to over-weight employment. **Kashkari** responded that they were effective and eye-opening for Washington, though whether the Fed over-learned was debatable. **Lane** asked about the idea of enshrining Fed independence in the Constitution, while commenting that ECB communication on climate was largely positive economics. **Kohn** responded that constitutional change would not happen, so institutions must build support within the present system, while commenting that although the link between climate and financial stability was a legitimate subject, the ECB appeared

to go further to support climate policy. **Remolona** raised the issue of many emerging economies' tendencies to lean on central bank financing of deficits. **Kohn** noted that this lesson had largely been learned through separating fiscal and monetary policy, and mentioned an analogy to the US, warning that calls to lower rates to ease budget pressure were dangerous. **Kose**, citing recent work quantifying the costs of a lack of independence, asked whether those costs were nonetheless under-communicated. **Kohn** said the evidence was nearly self-evident, acknowledging that there is no silver bullet to addressing communication to the general public, with focus, success and communication the only durable answer. Finally, **Åsa Olli Segendorf** (Sveriges Riksbank) asked whether data dependence monetary policy could conflict with forward guidance. **Kohn** replied that data mattered but had to be folded into a broader narrative rather than overreacting to the latest release.

IV. Keynote Speech: The AI Transformation: Implications for Finance, Money and Policy

Brunnermeier set out five "AI-forces" and discussed how they could reshape money, finance, and policy. The first force is a delegation and alignment challenge, as software moves from human-written code to large language models whose outputs are self-verified, creating a principal-agent problem marked by asymmetric understanding and asymmetric information. The second is speed, which obliges humans to delegate tasks to AI agents, leading to loss of control by humans. The third is a widening span of control that flattens hierarchies and hollows out the middle-manager pipeline. The fourth is hyper-personalization of goods, services, and prices, raising questions about how aggregate price indices are measured and what will happen to price stickiness. The fifth is "moat rupture risk," as AI erodes switching costs, weaking incumbents, and increases idiosyncratic risk.

Turning to the implications for money, finance, and policy, he argued that asymmetric execution speed, wider delegation to AI trading agents, and shared models and data would change the market structure, making regulation even more difficult. He expected fewer self-directed retail investors, more AI-managed strategies replacing static ETFs, reputation-building by those strategies, possible front-running of black-box advice, and common-mode failures—many AI strategies relying on similar models and data breaking down together—that raise systemic risk. He emphasized that regulation would become harder, mentioning the unresolved question of how to require disclosure for black-box, model-driven products.

He argued that a high-speed world would need tokenized digital money, since slow money would be driven out, and asked whether fast money would be private, such as stablecoins and tokenized deposits, or public, such as a CBDC. Drawing on Brunnermeier and Payne (2026), he set out a payment-credit-privacy trilemma in which only two of perfect credit, perfect payments, and cash-like privacy can be achieved, with the choice shaped by interoperability, ledger design, and privacy guarantees.

He then examined the big AI bet. He noted that the US financed AI innovations through capital markets, China through state-directed credit. He pointed out that the

AI-related investment of near 2.8% of GDP in the US was large but not unprecedented, and gains had been concentrated in a few stocks, as in past innovation cycles. He continued that financing was shifting to debt such as private credit, with data-center financing structures being reminiscent of special purpose vehicles observed in the run-up to the global financial crisis of 2007–09.

On repricing of AI technologies, he contrasted a foundation-model scenario, where a few firms become dominant and earn rents, with a commodification scenario, where many firms compete with rents broadly shared, followed by a major repricing. He also mentioned the possibility of a slow productivity gain scenario, and discussed its implications for US fiscal sustainability and US safe-asset status, adding that AI technologies could segment the finance world by building digital currency areas. He concluded that in this challenging time the only way to have a resilient outcome was to stay agile and maintain the reputation of institutions such as central banks.

From the floor, **Gourinchas** asked two questions. First, he asked why competition among AI firms could be disruptive instead of leading to more efficient investment and allocation. **Brunnermeier** replied that the main threat was asymmetry, since some actors will gain large advantages in analysis, information, and speed. Second, **Gourinchas** asked about the risk of AI being weaponized to attack the financial system. **Brunnermeier** agreed that cyber risk was enormous and under-emphasized, warning that institutions must be ready.

Lane asked whether rents were more likely to accrue to foundation-model firms or to those applying AI across business lines. **Brunnermeier** responded that the distribution of rents was largely up to regulators, who could enforce commodification of foundation models, for example, through qualified public procurement.

Building on Brunnermeier's observation that slower money might be displaced by faster, tokenized money, **Tao Zhang** (Bank for International Settlements) asked, about the implications for central banks. In particular, he asked whether central banks—especially those in medium-sized economies that are largely adopters of AI technologies—risk becoming less relevant if public money cannot keep pace with private-sector innovation. **Brunnermeier** replied that CBDC arrangements could keep private money efficient, with public money prepared to address a fallback against cyber risks.

Lombardelli returned to inflation and the value of money, asking what happens to inflation indices and to inflation expectations if agents trade highly personalized goods at personalized prices. **Brunnermeier** responded that price discrimination could grow, reducing price stickiness, with caveats that these were speculative and meant to stimulate discussion.

V. Fireside Chat

Himino hosted the fireside chat and welcomed Jefferson and Lane as guest speakers. He invited each speaker to make brief remarks on monetary policy response to supply shocks, after which he asked about the lessons learned from past episodes and about central bank communication.

Jefferson first flagged three global developments: rising energy prices, the rapid

advances in AI, and trade disruptions. He noted that elevated energy prices weighed heavily on net importers such as Japan, while less on net exporters such as the US. He saw US growth as solid but moderating, the labor market as broadly stable with risks skewed somewhat to the downside, and disinflation as stalled largely because of tariffs. He reaffirmed his commitment to returning inflation to the 2% target, adding that the current policy stance was well positioned to respond to economic developments.

Lane argued that supply shocks were not a one-size-fits-all category, distinguishing anticipated trends such as demography, the green transition, and future AI gains, which affect demand today with supply capacity changing in the future, from disruptions in the energy sector, which affect both demand and supply immediately. Even if the acute phase of such disruptions passed, he cautioned, repositioning around inventories and energy diversification might persist, and near-term supply capacity could fall well below long-term potential, which is one of the lessons from the 1970s.

Regarding the question about the lessons learned from past episodes, **Jefferson** pointed out the importance of anchored inflation expectations, policy credibility, and economic structure, noting that lower energy intensity and exporter status made the current shock milder than in the 1970s in the US. **Lane** compared the current shock with past episodes, including 2022 and the 1970s, and emphasized a nonlinear inflation response in which larger shocks have disproportionately stronger effects, adding that the current shock could be less acute as it could be smaller than that of 2022.

Regarding the questions about central bank communication, **Lane** stressed an overriding medium-term commitment to returning inflation to the target, staying adaptive meeting by meeting, and avoiding both complacency and overreaction. **Jefferson** added that policymakers should remain humble with regard to first-round effects, which monetary policy cannot offset, while acting to prevent second-round effects and a wage-price spiral.

From the floor, **Orphanides** pointed out that the effect of supply shocks on consumption would differ substantially between exporting and importing countries and asked how to deal with communication and policy. **Lane** replied that granular data and targeted fiscal support for the lowest-income households were key, while acknowledging that communicating distributional issues is challenging; **Jefferson** noted that the US faced not only an energy shock but also AI-driven investment, emphasizing on monitoring the second-round effects while keeping eye on the surge in investment demand. **Brunnermeier** asked whether policymakers differentiated supply shocks by upstream or downstream position in the production network, by the pricing power of the sector hit, and by supply-side uncertainty. **Lane** replied that the ECB used a production-network approach, while pointing to differences in energy pricing such as short-term or long-term contracts, noting that uncertainty was pushing firms toward larger inventories. **Ueda** asked whether repeated food and energy shocks, each a temporary price-level move but cumulatively lifting average inflation, might justify targeting a core rate slightly below 2% to allow for upward shifting, and what the welfare and communication implications would be. **Lane** replied that the ECB's strategy review last year had focused on various supply shocks and concluded that inflation volatility would rise, with no conclusion about the average inflation; **Jefferson** added that price stability at 2% was itself a source of broad-based, inclusive growth.

Olli Segendorf asked whether the less flexible European labor market warranted different policies and more severe second-round effects. **Lane** replied that second-round effects were not only about inflation expectations but about readjustment in wages that could take place when an increase in the cost of living due to external factors is not felt fair; **Jefferson** said that the resilience of the US labor market made returning inflation to 2% the appropriate focus.

VI. Paper Presentation Sessions

A. Optimal Monetary Policy with Uncertain Private Sector Foresight[4]

To motivate his research, **López-Salido** highlighted the risk of de-anchoring inflation expectations against the backdrop of persistent post-pandemic inflation, the energy price shock following the Ukraine conflict, and renewed fears about medium-to-longer run expectations drifting from target. He noted that inflation scares, episodes in which long-run inflation expectations drift away from target, were an old topic usually analyzed under rational expectations, but argued that models placing expectation formation at the center of the transmission mechanism offered a fresh angle. He then posed a question of how a central bank should conduct monetary policy when facing uncertainty about expectation formations in the private sector and the risk of inflation scares.

To address the question, he embedded finite-horizon planning by private agents into an otherwise standard three-equation New Keynesian model. In the model, households and firms plan a fixed number of periods ahead and, beyond that horizon, form beliefs through adaptive learning from past data. The planning horizon is heterogeneous, either four quarters or 32 quarters, with their relative shares varying over time. In addition, agents perceive that the central bank has the same planning horizon, even though it actually has an infinite planning horizon. Because of adaptive learning and the misperception, agents use realized inflation, rather than the announced target, to form long-term inflation expectations. Using the model estimated using the US data, he studied optimal discretionary policy.

He presented three findings. First, the model fits US data well on several dimensions. It captures the gradual decline in the underlying trend of inflation over the 1980s and early 1990s and reproduces the documented pattern of inflation forecast errors, which under-react to shocks on impact and over-react thereafter. Second, the optimal targeting rule—the condition relating optimal policy to inflation and the output gap—contains the familiar leaning-against-the-wind term plus an additional preemptive term, reflecting the incentive to prevent long-term inflation expectations from de-anchoring. This makes policy more aggressive on average and reverses the Brainard attenuation principle, the classic result that uncertainty should make policy more cautious. Third, simulations calibrated to the March 2023 FOMC projections showed that the optimal discretionary policy that guards against inflation scares would have anchored inflation more tightly around 2% with less dispersion.

As a discussant, **Olli Segendorf** praised the paper for elegantly combining rationality, learning, and optimal policy under uncertainty and for speaking directly to post-

4. For details, see Gust, Herbst, and López-Salido (2025).

pandemic concerns. She observed that central bank forecasting frameworks typically assumed inflation returns to target, and valued the paper for forcing policymakers to take alternative, de-anchoring inflation regimes more seriously. From a practical central banking perspective, she asked whether aggressive policy stance is the only way for preventing inflation scares, noting that Swedish long-run expectations had stayed anchored despite large shocks. She pointed out that communication, including published policy-rate paths and alternative scenarios, had already served as a complementary anchoring device in Sweden. She cautioned that precautionary tightening may generate non-linear risks to the real economy and lead central banks to underweight recession risk, especially when inflation is supply-driven, since tightening could produce large output losses. She further suggested distinguishing informed from uninformed expectations, since households often report high inflation expectations with limited forecast accuracy, and asked whether monetary policy should respond symmetrically to the two. She noted that the frequency of firms' price changes varied over time in practice, which could be taken into account. She also pointed to a tension in the model's estimate of longer planning horizons during the high-inflation 1970s: if higher inflation made agents more attentive, she questioned why their expectations would not by the same logic have become better anchored.

López-Salido agreed that the issues warranted further work. He added that he was now trying to connect inflation expectations with attention by endogenizing the planning horizon through state-dependent cognitive costs, emphasizing the need to identify the mechanism that drives inflation expectations by combining expectations data with micro price data. He agreed that household and firm expectations should be distinguished, and noted that the exercise was deliberately simple, relying on static discretion rather than commitment, which he hopes to address in future work, while reiterating that the framework calls for a tighter policy on average.

From the floor, **Orphanides** commented that the paper valuably revived Goodfriend's (1993) insight on anchoring inflation expectations. He asked whether communicating an inflation target could improve anchoring, citing learning models in which a known target delivers significant benefits over an unknown one—one of the theoretical cases for an inflation-targeting framework. **López-Salido** replied that in his setting agents already know the target but, beyond their planning horizon, rely on realized inflation to gauge how far it has drifted from 2%, adding that the central bank does not know how agents assess the target's credibility given their limited foresight, so a lack of credibility about the long-run target would generate similar preemptive incentives. He also noted that this result had emerged naturally in a setting that formalized Goodfriend's ideas.

B. Global Networks, Monetary Policy and Trade[5]

Kalemli-Özcan examined how monetary policy should be conducted in this geopolitically fragmented, interdependent world, where protectionist tools such as tariffs, subsidies, industrial policy, and trade and investment restrictions have risen sharply since 2020. Invoking the Kindleberger stabilizer view and the Hirschman weaponizer

5. For details, see Kalemli-Özcan Soylu, and Yildirim (2026).

view, she argued that global trade and finance networks could deliver stabilization and weaponization at the same time. She continued that a central question was whether geopolitics change how central bankers think about monetary policy, with an answer hinging on how trade and financial portfolios reshape in a fragmented world, how they affect currencies and exchange rates, and how they alter the international transmission of shocks.

To address these challenges, she built an N-country, J-sector global New Keynesian open economy model that incorporates trade, production, and financial networks, nominal rigidities, and incomplete markets with non-zero net international investment positions. The model features two analytical objects. The first is a risk-sharing wedge—the departure from full international risk-sharing—whose sign determines whether a tariff-imposing country gains or loses. The second is a New Keynesian open economy propagation matrix, a dynamic analogue of the Leontief inverse, that governs inflation persistence through real marginal costs. She incorporated tariffs implemented as of March 2026 into the model that is calibrated using data on firm-level trade, investment, and supply chains.

She explained that tariffs act as triple shocks—demand, supply, and financial wealth-transfer shocks, so whether a country gains or loses is a general equilibrium outcome of these effects. She argued that with global trade and finance networks central banks would face a greater tradeoff between inflation and output stabilization in response to an increase in tariffs, adding that even a look-through stance—premised on a one-time price-level jump that would quickly subside—would increase inflation persistently.

Turning to actual tariff data, implemented March 2026 tariffs are modest, raising inflation about 0.4 percentage points and persistently lowering output in the US. She discussed why the dollar depreciated after "Liberation Day," arguing that a rise in tariff volatility exerted depreciation effects that are greater than the direct appreciation effects of tariffs. She further showed that the general-equilibrium adjustment produced substantial trade diversion toward Europe, and a counterfactual in which the full Liberation Day tariffs took effect would have produced a global stagflation. She concluded that heterogeneous central bank responses reopened the case for international coordination, since national policies and endogenous exchange rates cannot fully offset network-borne distortions.

As a discussant, **Ippei Fujiwara** (Keio University/The University of Tokyo) praised the paper for its relevance to the current policy debate about tariffs, inflation, exchange rates, and monetary policy spillovers as well as its rich global New Keynesian open-economy model with input-output linkages and incomplete markets. He asked what determines the risk-sharing wedge, which determines which country gains or loses in response to a tariff shock. He added that estimating the response of the economy including the wedge to a tariff shock would be useful to discipline the model, and also asked whether the paper's conclusions would change if the wedge were instead generated by explicit financial frictions as in the previous literature. He further questioned if the model produces realistic exchange rate and UIP dynamics after a monetary shock. In closing, he said that the paper would become a benchmark for studying the effects of tariffs at business cycle frequencies, integrating monetary

policy, international finance, and global trade linkages.

In response, **Kalemli-Özcan** noted that the model matched the 2018 dollar appreciation, adding that to fit the 2025 depreciation as well, the UIP wedge, microfounded by tariff volatility in a companion paper, was needed. She emphasized that the New Keynesian and balance-of-payments blocks of the model could be solved separately by taking portfolio costs to zero, which eventually pins down the risk-sharing wedge, a key variable that determines the winner and loser of a tariff shock.

From the floor, **Lane** confirmed from ECB modeling that networks amplify and prolong supply shocks while diminishing demand shocks, but emphasized that the network was both opportunity and risk, since Europe could substitute away from Russian gas in 2022 whereas a truly global shock leaves nowhere to turn. **Kalemli-Özcan** responded that her model allowed substitution at the final-good layer and complementarity among inputs but did not easily capture extensive-margin production shifts such as Germany's rapid LNG buildout. **Gourinchas** asked whether the trade network or the financial network matters most, noting that the paper's own results suggested non-zero net foreign asset positions were quantitatively important, yet the model traded only US bonds on the financial side. He suggested testing the model against the empirical responses of the components of net foreign assets. **Kalemli-Özcan** replied that the model emphasized both the trade and financial networks but the financial side was kept simple, adding that the trade network was retained because the risk-sharing wedge has a trade component as well as a valuation component, and the two can move in opposite directions, so a purely financial formulation would miss the trade channel that matters especially under sectoral tariffs. **Etsuro Shioji** (Chuo University) asked about the pricing currency of traded goods and of international liabilities and whether the results are sensitive to them. **Kalemli-Özcan** answered that the model used hybrid currency pricing disciplined by dollar- and producer-pricing shares with sectoral retail heterogeneity, and that the net international investment position was effectively in dollars alongside a local-currency bond, yielding realistic and well-disciplined valuation effects.

C. Global Price Shocks and International Monetary Coordination[6]

Werning examined the optimal monetary policy response to global supply shocks, motivated by the post-COVID inflation in which goods price surges spread to services and wages across many countries. He framed a puzzle as why economies fare worse under global supply shocks than under comparable local ones, and posed two questions: Is uncoordinated policy really too contractionary, as the traditional view suggests, once accounting for the endogeneity of world commodity prices? Is there a case for international coordination?

To address these questions, he built a deliberately simple small open-economy model, consisting of a continuum of symmetric, price-taking small open economies, with a non-labor input labeled as "oil" that enters production with limited substitutability. He explained that nominal rigidities were introduced in both non-traded prices and wages to break divine coincidence: the property that stabilizing inflation automatically closes the output gap, leaving no policy trade-off. He noted that the steady state was ef-

6. For details, see Guerrieri, Lorenzoni, and Werning (2025).

ficient, and terms of trade effects were assumed away so that coordination gains could not stem from that channel. He then compared an uncoordinated Nash equilibrium, in which each country takes the world oil price as given, with a coordinated world planner who internalizes the endogeneity of the oil price.

As a main result he highlighted an expansionary bias: uncoordinated policy is too loose rather than too tight, leaving the world with excess inflation and output. He explained that each country perceived a flatter Phillips curve than the planner because it ignores the endogeneity that a decrease in global demand due to monetary tightening lowers oil prices, overturning the traditional wisdom that non-cooperative monetary policy is excessively contractionary. He added that the oil wedge arising from wage rigidity also generated inefficiency that can be addressed by the planner. He stressed that a distortion in the world Phillips curve and the oil wedge gave rise to an expansionary bias under the same plausible condition: low substitution between oil and labor. Drawing an analogy with optimal currency area arguments, he noted that dollarization or a currency union pools monetary policy, automatically internalizing the oil price externality, and thus would be welfare-improving.

As a discussant, **Kosuke Aoki** (The University of Tokyo) praised the paper as clean and insightful, emphasizing that it overturned two conventional views: the look-through prescription for commodity shocks and the presumed contractionary bias. He focused on how to implement the planner's outcome in practice when coordination at business cycle frequency is difficult. He proposed three options within the framework of a loss function: targeting a broader CPI measure rather than core inflation, appointing conservative central bankers in the spirit of Rogoff (1985), and a Pigouvian tax on oil. He showed that a broader CPI mandate can replicate the planner's outcome only for an optimally chosen output weight, and that a conservative central banker does so precisely when each country perceives a flatter Phillips curve. He noted that the Pigouvian tax fails under the loss function but might work under the full welfare analysis. He cautioned that each proposal would merely relocate the coordination problem to another dimension.

Werning welcomed these ideas, noting he had not thought enough about achieving coordination through the back door, which might prove easier than coordinating after every shock. He acknowledged that the Pigouvian option was likewise new to him, and expressed interest in developing it further. He cautioned that reweighting mandates or appointing conservative bankers would help against global shocks but could worsen responses to domestic shocks, likely leaving policymakers at a second best, and stressed that even setting coordination aside, the framework explained why a global shock is inevitably worse than a domestic one.

From the floor, **Hibiki Ichiue** (Keio University) asked why both price and wage rigidities are needed to break divine coincidence, whereas a simple New Keynesian model breaks it under a cost push shock with price rigidity alone. **Werning** replied that an oil or productivity shock, unlike a cost-push shock, reflects genuine resource scarcity rather than an artificial distortion; with price rigidity alone it therefore creates no policy trade-off, so wage rigidity is needed to introduce the additional wedge that breaks divine coincidence. **Goolsbee** asked whether positive supply shocks such as new technologies are symmetric and whether the implication is that policy would be

too tight. **Werning** answered that the model was formally symmetric so all signs invert, though he viewed negative supply shocks as sharper in practice, and summarized the message as policy reacting too little absent coordination. **Gourinchas** agreed with the conclusion and asked how fiscal policy interacts, observing that energy subsidies mute domestic price responses, export the adjustment abroad, and, by suppressing headline inflation, can lead central banks to tighten even less, deepening the expansionary bias. He suggested that the combined implication was for monetary policy to act more forcefully while fiscal energy support is scaled back. **Werning** agreed that subsidizing oil would discourage tightening, making world oil demand elevated and its price high, adding that if all countries subsidize simultaneously, everyone would worse off. **Kose** asked how asymmetry in country size would affect the main result. **Werning** replied that larger countries or coordinating blocs would partially internalize the externality, moving closer to the optimum, much like a currency area.

D. Monetary-Fiscal Nexus and Unintended Equilibria[7]

Ikeda observed that inflation had remained persistently above target in many countries despite inflation targeting frameworks, while government debt had risen worldwide. He mentioned that reflecting this development recent work had turned to heterogeneous agent New Keynesian (HANK) models with non-Ricardian households, because government bonds are net wealth for such households so that rising debt is expansionary. Noting that the literature had mostly focused on targeted equilibria with inflation fluctuating around 2%, he posed the question of whether monetary-fiscal interactions can generate unintended, non-targeted equilibria that push inflation away from a target persistently.

To explore the question, he built an analytically tractable perpetual youth overlapping generations (OLG) version of the New Keynesian model with non-Ricardian households and monetary-fiscal interactions. He explained that the model abstracted from nominal rigidities and fundamental shocks for simplicity, adding that the model nests the representative agent model as a special case.

Analyzing the model, he reported the following results. First, with non-Ricardian households, multiple steady states may prevail. A targeted steady state always exists, but a high inflation steady state can emerge when the stabilization stance of monetary or fiscal policy is relatively weak. The high-inflation outcome is driven by a self-reinforcing cycle: a rise in inflation prompts the central bank to raise interest rates, inducing the fiscal authority to issue more debt, and households who find government bonds as net wealth increase consumption, putting upward pressure on inflation. Second, analyzing local dynamics, he showed that when a high inflation steady state emerges, it exhibits determinacy while a targeted steady state loses determinacy, so that the economy might settle persistently at elevated inflation. Highlighting these two results, he argued that there might be a risk of persistently high inflation depending on monetary-fiscal interactions. Third, he examined the existence of self-fulfilling deflationary steady state, showing that with non-Ricardian households it exists with determinacy—a result that contrasts with standard New Keynesian models, where such

7. For details, see Ikeda (2026).

states are always indeterminate. He argued that this model had the potential for explaining Japan's low inflation experience from the late 1990s to early 2020s.

As a discussant, **Fernando Martin** (Federal Reserve Bank of St. Louis) praised the timely paper and offered a simplified analytical representation of the model. Showing the various models of non-Ricardian households, he pointed out that non-Ricardian households were necessary but not sufficient, and that what matters is the steady state real interest rate that depends on the quantity of debt. He also noted that monetary policy stance still matters: a sufficiently aggressive monetary policy response keeps the economy in the stable region around the targeted equilibrium. Examining US data, he argued that expansive and unresponsive fiscal policy combined with a monetary policy that has been slow to respond could pose a risk of persistently high inflation according to the model. He acknowledged that central bank accommodation and fiscal expansions during the global financial crisis of 2007–09 and the COVID-19 pandemic had supported the economy, but stressed that inflation was ultimately the cost of deficits not financed by taxes. He concluded that restoring fiscal responsiveness was an open question for the future.

Ikeda welcomed the simpler analytical representation and agreed that non-Ricardian households were necessary but not sufficient for the existence of multiple steady states. He raised a further case in which both policy responses were weak yet the targeted steady state stayed determinate, adding that inflation becomes fiscally driven so that inflation and output respond more strongly to debt.

From the floor, **Werning** asked how much the result depends on HANK rather than merely turning Leeper's (1991) previously ignored explosive region into a finite steady state, and urged care on income effects since debt held by foreigners or wealthy low MPC agents might reverse the consumption response. **Ikeda** replied that he studied only local dynamics, viewing the high inflation steady state as intermediate between the targeted state and explosive hyperinflation. He conceded that higher debt might not stimulate consumption in practice, as Japan's experience suggests, adding that a natural next step would be to examine whether quantitative OLG and HANK models exhibit non-targeted equilibria. **Brunnermeier** asked how critical the zero lower bound is, whether the intuition for the deflationary steady state parallels Benhabib, Schmitt-Grohé, and Uribe (2001), and whether an R-versus-G (the real interest rate versus the growth rate of the economy) connection applies. **Ikeda** noted that the paper focuses exclusively on R greater than G, and that while the deflationary steady state shares the same intuition as Benhabib, Schmitt-Grohé, and Uribe (2001), non-Ricardian households make it determinate rather than indeterminate as in standard New Keynesian models. **Fujiwara** asked whether any monetary policy rule, such as a history dependent one, could avoid the multiplicity. **Ikeda** replied that he had not explored whether any rule could eliminate deflationary or high-inflation steady states, and expected multiple equilibria to persist under alternative specifications. **Shioji** questioned the realism of a low survival probability assumed in the model, and asked whether a discontinuous monetary rule could avoid multiplicity. **Ikeda** acknowledged that only a simple rule had been studied and whether a richer specification could eliminate multiplicity remained open, while noting that the OLG framework can be interpreted as a model of heterogeneous agents subject to borrowing constraints.

VII. Policy Panel Discussion 1

In the Policy Panel Discussion 1, moderated by Hoshi, four panelists, Gourinchas, Hauser, Logan, and Remolona, discussed monetary policy and imbalances.

A. Remarks by Moderator and Panelists

Hoshi opened the policy panel discussion by noting that global imbalances, prominent before the global financial crisis and largely quiet since, had returned to the agenda of the G7, the G20, and the IMF. He argued that the underlying economics remained unchanged, with saving and investment still the analytical anchor, even as the world had grown more financially integrated, more capital-mobile, and more shaped by geopolitical tension and industrial policy. Drawing a parallel with the 1980s, he cautioned that China was now far larger relative to the world than Japan ever was, and that external imbalances reflected deeper domestic conditions rather than bilateral trade and could not be resolved by the exchange rate alone. He invited the panelists to consider how monetary policy should respond to such structurally and geopolitically driven imbalances, how resilient markets can be, and whether the international monetary system is fragmenting.

Gourinchas reported that global imbalances have been rising at an increasing rate since the pandemic, and that today's episode carried a concern absent from the pre-crisis debate: growing evidence that surpluses, particularly from China, reflect industrial policies that have distorted the manufacturing sector beyond efficient scale—producing the overcapacity that China itself acknowledges—and providing one rationale for the recent US turn to tariffs. Using the saving minus investment framework, he stressed that global imbalances were not inherently undesirable and that the relevant unit was national rather than bilateral balances. On the drivers, he found tariffs to have very limited durable effects on current accounts and micro industrial policy—subsidies to particular firms or sectors—to show little systematic link to balances. He continued that what can generate sizeable surpluses was macro industrial policy: financial repression, forced savings, and FX intervention deployed to compress domestic consumption and channel resources into the export sector. On rebalancing, he argued that coordinated adjustment would be best but unlikely, and that unilateral action by one large economy would raise global real interest rates and create adjustment incentives elsewhere. On monetary policy, he aligned himself with Hoshi: engineering a nominal currency appreciation would only generate deflation without resolving the underlying imbalances. Venturing beyond current-account imbalances, he drew attention to imbalances in control over critical resources, noting that the global economy had choke points such as rare earths and the Strait of Hormuz. He cited an IMF study finding that a disruption to rare earth supply, with mining, refining, and processing all heavily concentrated in China, could have sizeable effects on other economies given the low substitutability of these inputs.

Hauser recalled that there had been many prior attempts to identify the causes of, and possible solutions to, global imbalances. To take one important example, the multilateral consultation on global imbalances coordinated by the IMF in 2006 had produced commitments from the major players—US fiscal consolidation, Chinese re-

balancing toward consumption with greater exchange rate flexibility, and European structural reform—that closely resembled today's prescriptions. Imbalances, he observed, were not necessarily malign in themselves: indeed they could deliver genuine benefits through efficient capital allocation and risk sharing. But excessive imbalances risked a disorderly unwind. The question then was what should count as 'excessive.' He pointed out that the scale of the risk was elevated: imbalances were closed to 150-year highs, financial stock effects now matter more than trade flows, and markets have proved willing to fund large debt stocks well past thresholds once considered dangerous, raising the danger of a non-linear adjustment triggered by a loss of confidence or a reappraisal of the AI boom. Speaking for a small open economy (SOE) central bank such as the RBA, he said Australia sat in the front row as a major beneficiary of globalization, but was relatively powerless to address the factors underpinning excess imbalances. In that light, the priority for SOE central banks was primarily to build resilience through better modelling, smarter strategy in the face of uglier trade-offs, and stronger domestic crisis tools.

Logan began with energy markets and shared views on global oil imbalances. She noted that the closure of the Strait of Hormuz had cut global oil supply by more than 10%, nearly 13 million barrels per day, with inventory drawdowns and rising US exports filling much of the shortfall so far, adding that in the last week of April the US had become a net exporter of oil for the first time since 1943. Mentioning the Dallas Fed's latest survey, she said that industry leaders saw little scope to increase oil production because of capital discipline, tight labor, and limited gas pipeline capacity. She then pointed out that with supplies highly constrained, if the shipping through the strait would not return to the original level, world oil and natural gas consumption would fall. She turned to financial imbalances, noting that, unlike energy where physical limits force a rough rebalancing, financial imbalances can persist for years. She pointed out that Treasury issuance had greatly outpaced dealer capacity since the global financial crisis, making the markets vulnerable to shocks as evident in the March 2020 Dash for Cash. She welcomed steps to strengthen Treasury market resilience while urging a richer toolkit and clearer separation of market-functioning support from monetary accommodation. Finally, she mentioned a slower force, the global decline in fertility to below replacement across major regions, which she said would reshape labor markets, fiscal positions, the neutral rate, and the meaning of a balanced economy as growth approaches zero.

Remolona observed that the current oil price shock exacerbated the current account deficit of the Philippines while raising inflation. He noted that the peso was overvalued a few years ago with the adjustments of the exchange rate toward depreciation being frustratingly slow. He pointed out that exchange rate adjustment alone might prove insufficient to address the current account deficit. Invoking Dornbusch's law and recalling the 1997 Asian crisis, he voiced concern that the current shock could become a tipping point. He shifted attention from the trade component to saving and investment, noting that with a very young population (median age 26) the Philippines had low saving and strong investment needs, which are eventually financed by borrowing abroad, leading to the current account deficit. He added that higher interest rates might eventually help, though the central bank's policy rate had focused on price stability rather than on the

current account deficit.

B. Discussion between the Moderator, Panelists and Floor Participants

Hoshi opened the discussion by returning to the point, made by both Gourinchas and Hauser, that imbalances are not necessarily harmful. He asked why deficit countries often see imbalances problematic.

Gourinchas replied that the main reason would be an asymmetric perception that surpluses and strong currencies are good while deficits and weak currencies are bad, adding that the pressure to adjust falls disproportionately on deficit countries, which risk losing market financing as they accumulate debtor positions, whereas surplus countries face no comparable imminent pressure beyond the possibility of lending into investments that are never repaid. Reflecting on Logan's point about demographics, he added that demographic divergence would be shrinking as a driver of imbalances because the world is becoming more like Japan, leaving less asymmetry to generate surpluses and deficits.

Hoshi then asked in which areas the greatest risk of a sudden, non-linear adjustment lies, for example, in sovereign bond markets or non-bank finance. **Logan** identified sovereign bond markets as a chief concern, given rising government debt and limited dealer intermediation capacity, noting progress on transparency and central clearing but much more work to be done. She also flagged stretched asset valuations, especially if AI productivity assumptions do not realize. **Hauser** said it was hard to explain why markets continued to fund some of sovereign debt stocks at the prices seen recently, with rises in term premia muted. He mentioned the Bank of England's intervention during the 2022 liability-driven investment (LDI) crisis as a possible toolkit, while questioning whether constructive ambiguity still works, that is, whether a central bank should leave deliberately unspecified whether and when it would step in to support markets. **Remolona** stressed that the biggest threat is to central bank independence, since it is challenging to convince the general public that financing projects through money creation eventually brings inflation, a danger especially acute for emerging economies. **Gourinchas** echoed concern about worsening fiscal trajectories and the eroded willingness to consolidate since the pandemic, and pointed to the erosion of the US exorbitant privilege. Reflecting on Hauser's point, he noted that despite Treasuries come to be seen as no longer uniquely safe but merely one safe asset among others, investors kept buying them as a second-best alternative. Regarding non-linearities, he argued that the deepest danger is a financial risk event that is unaccompanied by the usual flight to the dollar.

Asked by **Hoshi** whether declining the exorbitant privilege means the world must contemplate a post-dollar system, **Gourinchas** responded that no sudden displacement was in prospect and that the dollar-based system remained strong, adding nonetheless that risk scenarios were worth exploring, since a typical financial stress event features a dollar shortage that the dollar liquidity swap lines are designed to fill, but a different pattern would require rebuilding global liquidity provision.

Hoshi next asked Logan about energy and the investment needs of the AI industry, including their implications for interest rates and imbalances. **Logan** responded that US power demand had risen sharply, with electricity growth of 2% in 2025 af-

ter two essentially flat decades, driven by data centers and electric vehicles, and that this was lifting investment demand. She pointed out that the significant demand suggested a higher neutral rate, with financial conditions appearing to be somewhat loose. **Remolona** added that AI has been a powerful force behind stock market gains across the value chain in Taiwan, Korea, and elsewhere in Asia, more than offsetting the oil price shock for those economies.

From the floor, **Kalemli-Özcan** asked about an emerging view that multinational firms and sectoral imbalances, particularly in energy and semiconductors, are now the more important driver of global imbalances. **Gourinchas** responded that he doubted the view since any sectoral or multinational effects must ultimately show up in national saving and investment. While multinationals and the location of FDI might shape the macroeconomic variables of some small countries, he argued that they would not account for the imbalances of large economies.

Kose asked whether the case for cooperative solutions could lead to an orderly resolution of imbalances and what might prompt such cooperation. **Gourinchas** clarified that a coordinated solution would be best but that he was skeptical of significant progress, adding that unilateral adjustments such as US fiscal consolidation, although not as good as coordination and not necessarily favorable for growth, would generate spillovers in the right direction by lower global interest rates increasing the pressure on China to adjust. Progress, he argued, should not wait for an unattainable joint agreement but can begin when countries act on their own domestic interest.

Brunnermeier asked whether increasing returns to scale might justify China building imbalances strategically. **Gourinchas** acknowledged the validity of the argument and pointed to Chinese successes in electric vehicles and solar panels, but noted that aggregate TFP had grown slowly and the marginal return to capital had collapsed, signs of resources being misallocated at scale.

Disyatat questioned how to move away from the IMF external balance assessment and the associated US currency-manipulator framework, given that the exchange rate is not the main corrective instrument. **Gourinchas** agreed to the point and explained that the external sector report first assesses excess current account positions and then translates them into estimates of currency over- or undervaluation, with this second step regarded as insufficiently robust, although the assessment remains part of its mandate.

Kazumasa Iwata (Japan Center for Economic Research) asked whether removing China's capital mobility restrictions—which, like Japan's in the 1980s, are tighter on outflows than on inflows—might widen global imbalances rather than narrow them, and how the US prohibition of a central bank digital currency affects demand for safe assets in light of concerns about the sustainability of the US external position. **Gourinchas** responded that if China lifted all controls, capital would flow out, the currency would depreciate sharply, and the surplus would grow even larger.

VIII. Policy Panel Discussion 2

In the Policy Panel Discussion 2, moderated by Orphanides, five panelists, Disyatat, Goolsbee, Kose, Lombardelli, and Nakamura, discussed monetary policy in a changing

world economy.

A. Remarks by Panelists

Disyatat argued that supply shocks now defined the policy environment. He identified three features of the shocks: they are sectoral, implying relative price changes rather than generalized inflation; they are persistent because structural trends such as AI, demographics, and the climate transition feed through production networks; they arrive as a confluence that complicates signal extraction. He argued that central banks therefore had a more limited ability to steer inflation within narrow targets, pointing out the risk of excessively fine tuning to hit narrow targets as inflation deviates from targets more often and more persistently both upward and downward, even while staying anchored within the low inflation regime. In such situations, he argued that central banks would face communication difficulties and political pressure that can undermine central bank independence, mentioning the experience of Thailand where inflation peaked at 8% in August 2022 but fell below 1% within a year and had since been close to zero. He supported inflation targeting with greater flexibility and more tolerance for the size and duration of deviations, stressing that anchoring occurs at the regime level rather than at a precise numerical rate.

Goolsbee reflected on the implications of stronger productivity growth, drawing on analysis at the Chicago Fed. He observed that US productivity had run substantially faster than the pre-COVID trend, adding that, interpreted broadly, the acceleration appeared concentrated in industries that develop and use AI. He cautioned that the 1990s intuition, in which higher productivity permits lower inflation and lower rates, applies when productivity gains are unanticipated, whereas anticipated future productivity gains can raise the optimal rate today through a wealth effect that pulls future demand and stimulates the economy. He pointed out that central bankers should monitor activity premised on future growth, such as consumer borrowing, elevated equity valuations, and large data center investment that drives up the cost of electricity, chips, and construction. He added that because general purpose technologies eventually spread beyond the country of origin, the same dynamics would become more pronounced in Japan and Europe, and that negative supply shocks would compound it by reducing potential output in the near term.

Kose reflected on the implications of the changing nature of shocks for monetary policy, drawing on recent work with Kristin Forbes and Jongrim Ha (Forbes, Ha, and Kose 2026). He recalled that during the Great Moderation domestic demand shocks dominated, where stabilizing inflation also contributes to stabilizing output, but during the past two decades the succession of global shocks had created sharp swings and difficult trade-offs between stabilizing inflation and output. He argued that global shocks increasingly shaped domestic monetary policy, stressing that they differ fundamentally from domestic shocks. Using an econometric decomposition across 13 advanced economies, he reported that global shocks now accounted for roughly half of the variation in policy rates, up from less than a fifth in earlier decades, and that they were more supply driven, more volatile, more frequent when large, and more persistent and more asymmetric upward in their effects on inflation. Echoing Kohn, he urged humility and suggested that policy design would benefit from giving global shocks greater attention

in models and communication, including through scenario analysis.

Lombardelli emphasized the supply-based character of the current shocks, pointing out the frequency of such supply shocks: the next arrives before the previous shock has subsided. She noted that UK inflation had averaged above target for five years and had peaked near 11%, and she stressed the persistent impact of repeated shocks on real incomes and the resulting damage on aggregate demand. She observed that as a medium-sized open economy and net energy importer with a very large financial sector, the UK had been hit hard, and she described uncertainty over prices set by firms facing squeezed margins and weak demand. She highlighted the BOE's growing use of scenarios following the Bernanke review, noting that in April it had published scenarios without a central forecast, and she flagged three financial stability risks as potential future shocks, namely stretched AI-related equity valuations, the rapid and less transparent growth of non-bank intermediation, and the large size of government bond markets together with the volatility introduced by hedge funds.

Nakamura posed the question of whether the recent series of once-in-a-lifetime events represent bad luck or a new normal, suggesting that the post-Cold War euphoria of globalization was itself an exceptional period and that supply shocks might now be more systematic, reinforced by income and wealth polarization, populism, geopolitical risk, and climate change. He argued that while the basic idea is to look through supply shocks, frequent shocks should not be treated as transitory because they can lift underlying inflation and inflation expectations. In addition, he pointed to a slow-moving demographic shock in Japan, with a shrinking pool of potential labor supply exerting structural upward pressure on wages, as a structural factor that cannot be dismissed as temporary. He noted the difficulty of capturing underlying inflation with any single indicator and the resulting challenge of communicating with the public, citing the BOJ's use of multiple measures. He turned to the deteriorating quality of official statistics, driven by budget cuts and privacy concerns, and argued that they might not accurately capture the actual state of the economy, which poses a threat to data dependent monetary policy.

B. Discussion between the Moderator, Panelists and Floor Participants

Orphanides asked the panelists how they would adjust monetary policy strategy in their own economies given the supply shock environment.

Disyatat replied that the challenge lay less in the conduct of monetary policy than in communication, since in Thailand an annual memorandum of understanding gives the government grounds to demand policy action on every target miss, particularly when inflation runs below target. He suggested that a core measure, which excludes food and energy where most of the supply shocks originate, or a ceiling target below 3%, similar to the older ECB formulation, would suit an economy repeatedly hit by supply shocks that tend to push inflation below target, while still anchoring long-run inflation low and stable. **Goolsbee** responded that beyond communication there was a reality problem, because a stagflationary shock cannot be resolved by raising, cutting, or holding rates, and that central banks should ask for some room to maneuver while accepting that the public would mostly be disappointed, recalling that as outlined in the US framework review, a stagflationary shock affects both sides of the

mandate negatively, placing a central bank in one of the most difficult circumstances. **Lombardelli** argued that scenarios helped separate what a central bank is certain about, namely the return of inflation to target over the medium term, from what it is uncertain about, such as the duration of a conflict, and that they also let policymakers test the robustness of policy against reasonable rather than extreme outcomes. **Nakamura** added that Japan had observed nonlinear reactions of domestic prices to external shocks, with consumer prices rising sharply in response to both import price and exchange rate shocks, and argued that such nonlinearities must be taken into account in the conduct of monetary policy. **Kose** pointed out that both the volatility and frequency of global supply shocks had increased, making it more difficult to look through global supply shocks, and thereby central banks now responded more strongly to them than in the past. **Kalemli-Özcan** commented that, rather than getting drawn into the duration and uncontrollable nature of global supply shocks, it might be better for central banks to deliver the simplest possible message, focusing on the demand-supply imbalance and on the demand-side tool the central bank actually controls.

Orphanides then asked whether scenario analysis along the lines the BOE had adopted could help address these difficulties. **Goolsbee** expressed skepticism about scenario analysis, noting that even internal Fed scenarios provoke debate over their assumptions, and that relying on scenarios to win public credit may not communicate what is intended. **Disyatat** added that scenarios would become particularly delicate when a contested fiscal program is under consideration, since publishing scenarios with and without it would reveal the central bank's judgment of the effects of fiscal policy, so that the Bank of Thailand presented only a baseline. **Nakamura** noted that the BOJ had already introduced scenario analysis in its most recent Outlook Report, drawing partly on the BOE's experience, but stressed that timing and circumstances were crucial, since, for example, publishing a worst-case scenario of financial system collapse could itself rattle markets. **Kose** saw the tool useful but agreed with Goolsbee that it does not necessarily ease communication from a dynamic perspective, illustrating with the sharp upward revision of the World Bank's oil price forecast through the year, which forced a reversal in the direction of the scenarios and created credibility challenges for forecasting. **Gourinchas** commented that communicating around scenarios without a baseline, as the IMF had effectively done in April by relabeling its baseline as a reference scenario, could be dangerous because the public ultimately wants a number and central banks need a number to anchor expectations. He argued that abandoning a baseline could be justified for shocks outside normal situations, such as major trade offensive or the closure of the Strait of Hormuz, but warned that once scenarios are published the central bank becomes locked into them, fielding constant questions about which scenario applies when the answer is none of them. **Goolsbee** expressed discomfort with the idea of using scenarios as forward guidance, since policymakers should not tie the hands of future committees, drawing an analogy to the way the dot plot is mistakenly read as a promise.

From the floor, **Hoshi** asked, as a follow-up to Nakamura, whether panelists had seen promising attempts to restore data quality and whether the growing body of alternative data offered a direction worth pursuing. **Nakamura** replied that with alternative data remaining partial, reliable public data designed to represent the whole econ-

omy was still essential, adding that more resources should be devoted to high quality official statistics. **Goolsbee** noted that budget cuts to US statistical agencies had increased noise, lengthened lags, and enlarged revisions in ways that had become politically charged, and he cautioned that private sector data, which is more timely, was still benchmarked to official statistics, so the public sector role could not be dispensed with. **Kose** added that beyond deterioration there was a problem of cross-country reliability and possible manipulation, worsened where countries are at war.

Lane returned to the earlier discussion of alternative target designs, cautioning that a ceiling or range inflation target creates a vagueness problem for large financial systems, since the rate required to deliver a 2% point target differs sharply from the rate consistent with a range. He defended a point target as effective for anchoring even when missed ex post, and stressed that inflation too low required a response as much as inflation too high. He noted that Thailand's much larger food share made its inflation more volatile, and urged to focus on medium- to long-term inflation expectations. **Kashkari** shared Goolsbee's skepticism and identified two purposes for scenarios, namely conveying the range of uncertainty and conveying the reaction function. He argued that scenarios could not capture the true range of outcomes, and that the reaction function was the hardest part to convey, since everything depends on whether long-run inflation expectations remain anchored. **Lombardelli** responded that the BOE was learning by doing the use of scenario analysis visibly. She reported that scenarios helped communication in the high-uncertainty period after the Iran conflict, that the reaction function was indeed where value could be added, and that simple messages worked best, such as showing that rates would be higher if the war lasted longer and oil prices were higher regardless of the policy rule applied. She noted that running multiple policy rules through a scenario had produced a more informative internal committee debate about how to calibrate the policy rules, including the degree of smoothing and the relative weighting of objectives, even if the material was for specialists rather than the general public, and she called for more research, observing that placing scenarios within a risk distribution, as the IMF had begun to explore, still required work to be usable for policy communication.

Junko Koeda (BOJ) asked, in light of frequent negative supply shocks, how to effectively communicate to the broader public the role of monetary policy and its trade-offs, noting that wider public outreach may surface more concerns about jobs and the cost of living, issues that might be better addressed by fiscal policy. **Masazumi Wakatabe** (Waseda University) posed two questions, first on how communication with the government could be improved, since a central bank with only one or two instruments against multiple shocks depends on cooperation with the government, and second on the lessons central bankers can offer academia, given that current macroeconomics handles poorly multiplicity, persistence, tipping points, and nonlinearities, including how staff should be trained to understand these features. **Goolsbee** underscored how difficult communication will be in a world of more supply shocks, since forecasting inflation and the slope of the Phillips curve is already hard, expertise on supply chain damage and persistence is limited, and being proven wrong carries a price for credibility. **Nakamura** noted the relationship between headline inflation and short-, medium-, and long-term inflation expectations, the changing behavior of households

and firms, and argued the need to combine statistical with anecdotal analysis given evidence of nonlinear price-setting and large cross-country differences such as the high food share in some CPI baskets. **Kose** returned to the tipping point question in the context of oil markets, noting that inventories were falling quickly toward operational levels, that financial and physical markets disagreed sharply on the appropriate oil price, and that the large uncertainty around the tipping point, whether reached in July or later in the autumn, made it very difficult to communicate within any well-defined confidence interval.

Orphanides concluded that central banking was considerably harder in an environment of pervasive supply shocks, and that the challenge lied in choosing between the nineteenth-century approach of saying nothing, which sacrifices transparency and credibility, and the harder path of building tools such as scenarios to explain what is not known.

References

Benhabib, Jess, Stephanie Schmitt-Grohé, and Martín Uribe. "The Perils of Taylor Rules." *Journal of Economic Theory* 96, no. 1–2 (2001): 40–69.

Brunnermeier, Markus K., and Jonathan Payne. "BigTech Lending, Banking, and Information Portability." Working paper. Princeton University, Princeton, NJ, 2026.

Forbes, Kristin, Jongrim Ha, and M. Ayhan Kose. "Heaven or Earth? The Evolving Role of Global Shocks for Domestic Monetary Policy." NBER Working Paper 34806. National Bureau of Economic Research, Cambridge, MA, February 2026.

Goodfriend, Marvin. "Interest Rate Policy and the Inflation Scare Problem: 1979–1992." *Federal Reserve Bank of Richmond Economic Quarterly* 79, no. 1 (1993): 1–23.

Guerrieri, Veronica, Guido Lorenzoni, and Iván Werning. "Global Price Shocks and International Monetary Coordination." NBER Working Paper 33840. National Bureau of Economic Research, Cambridge, MA, 2025.

Gust, Christopher, Edward Herbst, and David López-Salido. "Optimal Monetary Policy with Uncertain Private Sector Foresight." *Journal of Monetary Economics* 155 (2025): 103826.

Ikeda, Daisuke. "Monetary-Fiscal Nexus and Unintended Equilibria." IMES Discussion Paper, Institute for Monetary and Economic Studies, Bank of Japan, Tokyo, 2026 (forthcoming).

Kalemli-Özcan, Şebnem, Can Soylu, and Muhammed A. Yildirim. "Global Networks, Monetary Policy and Trade." NBER Working Paper 33686, National Bureau of Economic Research, Cambridge, MA, April 2025, revised May 2026. https://sebnemkalemliozcan.com/assets/workingpapers/GlobalNetwork_Monetary_Policy_and_Trade_latest.pdf.

Kohn, Donald. "The Mayekawa Lecture: Challenges to Independence: How Should Central Banks Respond—Lessons from History." *Monetary and Economic Studies*, 44 (2026): 35–46 (this issue).

Leeper, Eric M. "Equilibria under 'Active' and 'Passive' Monetary and Fiscal Policies." *Journal of Monetary Economics* 27 no. 1 (1991): 129–47.

Rogoff, Kenneth. "The Optimal Degree of Commitment to an Intermediate Monetary Target." *Quarterly Journal of Economics* 100, no. 4 (1985): 1169–89.

Ueda, Kazuo. "Opening Remarks." *Monetary and Economic Studies*, 44 (2026): 29–34 (this issue).

APPENDIX 1: PROGRAM

Wednesday, May 27, 2026

Opening Remarks
Speaker: **Kazuo Ueda**, Bank of Japan

Mayekawa Lecture: Challenges to Independence: How Should Central Banks Respond—Lessons from History
Chairperson: **Neel Kashkari**, Federal Reserve Bank of Minneapolis
Lecturer: **Donald Kohn**, The Brookings Institution

Session 1: Optimal Monetary Policy with Uncertain Private Sector Foresight
Chairperson: **Kartik Athreya**, Federal Reserve Bank of New York
Paper Presenter: **David López Salido**, Banco de España
Discussant: **Åsa Olli Segendorf**, Sveriges Riksbank

Keynote Speech:
Chairperson: **Peter Kažimír**, National Bank of Slovakia
Speaker: **Markus Brunnermeier**, Princeton University

Session 2: Global Networks, Monetary Policy and Trade
Chairperson: **Tao Zhang**, Bank for International Settlements
Paper Presenter: **Şebnem Kalemli-Özcan**, Brown University
Discussant: **Ippei Fujiwara**, Keio University/The University of Tokyo

Session 3: Global Price Shocks and International Monetary Coordination
Chairperson: **Josef Meichenitsch**, Austrian Central Bank
Paper Presenter: **Iván Werning**, Massachusetts Institute of Technology
Discussant: **Kosuke Aoki**, The University of Tokyo

Policy Panel Discussion 1: Monetary Policy and Imbalances
Moderator: **Takeo Hoshi**, The University of Tokyo
Panelists: **Pierre-Olivier Gourinchas**, International Monetary Fund
Andrew Hauser, Reserve Bank of Australia
Lorie Logan, Federal Reserve Bank of Dallas
Eli M. Remolona, Jr., Bangko Sentral ng Pilipinas

Thursday, May 28, 2026

Fireside Chat

Moderator:	**Ryozo Himino**, Bank of Japan
Guest Speaker:	**Philip Jefferson**, Federal Reserve Board
	Philip R. Lane, European Central Bank

Session 4: Monetary-Fiscal Nexus and Unintended Equilibria

Chairperson:	**Rosmarie Schlup**, Swiss National Bank
Paper Presenter:	**Daisuke Ikeda**, Bank of Japan
Discussant:	**Fernando Martin**, Federal Reserve Bank of St. Louis

Policy Panel Discussion 2: Monetary Policy in a Changing World Economy

Moderator:	**Athanasios Orphanides**, Massachusetts Institute of Technology
Panelists:	**Piti Disyatat**, Bank of Thailand
	Austan Goolsbee, Federal Reserve Bank of Chicago
	M. Ayhan Kose, The World Bank Group
	Clare Lombardelli, Bank of England
	Koji Nakamura, Bank of Japan

APPENDIX 2: LIST OF PARTICIPANTS

Harun Alp	Federal Reserve Board
Kosuke Aoki	The University of Tokyo
Preston Ash	Federal Reserve Bank of Dallas
Kartik Athreya	Federal Reserve Bank of New York
Markus Brunnermeier	Princeton University
Rudolf Christoph	Deutsche Bundesbank
Nerissa De Guzman	Bangko Sentral ng Pilipinas
Piti Disyatat	Bank of Thailand
Justin Ray Angelo Junio Fernandez	Bangko Sentral ng Pilipinas
Coletta Frenzel Baudisch	Deutsche Bundesbank
Takuji Fueki	Hitotsubashi University
Ippei Fujiwara	Keio University / The University of Tokyo
Andrea Gerali	Bank of Italy
Austan Goolsbee	Federal Reserve Bank of Chicago
Pierre-Olivier Gourinchas	International Monetary Fund (IMF)
Andrew Hauser	Reserve Bank of Australia
Johannes Hoffmann	Deutsche Bundesbank
Michal Horváth	National Bank of Slovakia
Takeo Hoshi	The University of Tokyo
Hibiki Ichiue	Keio University
Kazumasa Iwata	Japan Center for Economic Research
Philip Jefferson	Federal Reserve Board
Ryo Jinnai	Hitotsubashi University
Masaaki Kaizuka	NEC Corporation
Şebnem Kalemli-Özcan	Brown University
Hiroyuki Kasahara	University of British Columbia
Prudence Angelita Amposta Kasala	Bangko Sentral ng Pilipinas
Neel Kashkari	Federal Reserve Bank of Minneapolis
Mitsuru Katagiri	Waseda University
Peter Kažimír	National Bank of Slovakia
Keiichiro Kobayashi	Keio University
Donald Kohn	The Brookings Institution
M. Ayhan Kose	The World Bank Group
Haruhiko Kuroda	The National Graduate Institute for Policy Studies
Philip R. Lane	European Central Bank
Harry Lee	Monetary Authority of Singapore

Lorie Logan	Federal Reserve Bank of Dallas
Clare Lombardelli	Bank of England
David López Salido	Banco de España
Fernando Martin	Federal Reserve Bank of St. Louis
Peter McQuade	European Central Bank
Josef Meichenitsch	Austrian Central Bank
Kazuo Momma	Mizuho Research Institute
Seungho Nah	Bank of Korea
Makoto Nakajima	Federal Reserve Bank of Philadelphia
Hiroshi Nakaso	Daiwa Institute of Research Ltd.
Yoshiyuki Nakazono	Yokohama City University
Meri Obstbaum	Bank of Finland
Masayuki Okada	Hitotsubashi University
Åsa Olli Segendorf	Sveriges Riksbank
Athanasios Orphanides	Massachusetts Institute of Technology
Andrea Raffo	Federal Reserve Bank of Minneapolis
Eli Jr. Remolona	Bangko Sentral ng Pilipinas
Martin Šanta	National Bank of Slovakia
Rosmarie Schlup	Swiss National Bank
Toshitaka Sekine	Hitotsubashi University
Mototsugu Shintani	The University of Tokyo
Etsuro Shioji	Chuo University
Shigenori Shiratsuka	Keio University
Arthur Sogno Pèes	Banque de France
Masazumi Wakatabe	Waseda University
Toshiaki Watanabe	Hitotsubashi University
Tsutomu Watanabe	Nowcast Inc
Iván Werning	Massachusetts Institute of Technology
Beth Anne Wilson	Federal Reserve Board
Tao Zhang	Bank for International Settlements

Opening Remarks

by Kazuo Ueda, Governor of the Bank of Japan

We are pleased to welcome all of you, distinguished speakers and guests, to the 2026 BOJ-IMES Conference. Thank you very much for your participation.

The theme of this year's conference is "Monetary Policy from New Perspectives." I am sure that supply shocks loom large in everyone's mind. They are not a new phenomenon but at least have become more frequent. Whether a new perspective is truly needed, I leave it for debate—but revisiting past experience is, I think, an indispensable starting point.

I do not have a new perspective to offer at this point. Instead, let me go through Japan's experience with major energy shocks during the last five decades and offer some food for discussion.

Since the 1970s, the global economy has been hit by significant spikes in energy prices, especially oil prices, as shown in Chart 1. There are five notable incidents: the first oil shock of 1973, the second oil shock of 1979, the oil price surge of the mid-2000s leading to the 2008 Great Financial Crisis, Russia's invasion of Ukraine in 2022, and the recent conflict in the Middle East.

However, the response of Japan's consumer price index (CPI) to oil price increases was different from episode to episode, to which I now turn.

Let me begin with the first oil shock. The first oil shock came in late 1973. In Chart 2 we can detect a typical wage-price spiral in 1974, with both reaching about the 20–30% range. But Japan's inflation problem had started before that. Inflation was already close to 10% in early 1973, and wage growth was close to 20%. It was already an economy with significant inflationary momentum.

It is sometimes said that monetary policy was slow to react. There is some truth to this, especially for the period preceding the oil price increases. But after inflationary pressures became visible, the Bank of Japan (BOJ) did tighten policy. The key point is that the tightening came after high inflation dynamics had already developed. Also, the degree of tightening was clearly inadequate given the near 20% inflation.

The most important transmission channel was wages. The oil shock fed into domestic wages and prices. The 1974 spring wage negotiations produced very large wage increases, and firms passed higher labor and input costs into prices. Inflation expectations rose further. In this way, an external relative-price shock became a broader wage-price spiral.

The economy contracted sharply in early 1974: the deterioration in Japan's terms of trade, the squeeze on real income, weaker corporate profits, tighter monetary policy, and the correction of earlier overheating. Eventually, recession and policy tightening helped bring inflation down, but only at a large cost.

The second oil shock, shown in Chart 3, around 1979 and 1980, was also large. Yet the inflation outcome was far more moderate.

DO NOT REPRINT OR REPRODUCE WITHOUT PERMISSION

One reason was that monetary policy responded more promptly. But this is not the whole story. The initial conditions were very different. Inflation was lower. Wage behavior was more restrained. Firms and labor unions had learned from the painful experience of the first oil shock. There was a stronger recognition that trying to fully compensate for inflation associated with higher oil prices through nominal wage increases could produce another inflationary spiral.

The exchange rate also mattered. Before the second oil shock, Japan had experienced substantial yen appreciation. This helped reduce import prices more generally and created a more favorable starting point. In addition, Japanese firms had begun to improve energy efficiency and reduce oil dependence.

Thus, the second oil shock slowed the economy and raised inflation, but it did not produce the same wage-price spiral. Monetary policy was important, but it worked in an environment where wages, expectations, exchange rates, and structural adjustment were all more favorable.

Let me turn to the third episode: the mid- to late-2000s. During this period, oil and commodity prices rose substantially. Japan's inflation rate increased somewhat, and the BOJ ended quantitative easing in 2006 and raised the policy rate modestly in 2006 and 2007. Yet inflation remained low, especially the core, which remained in negative territory for almost the entire period, as shown in Chart 4.

Why was the outcome so different from the 1970s? The answer is that Japan had fallen into a deflationary equilibrium by this time. Given the experience of deflation since the late 1990s, firms were reluctant to raise prices. Households had become used to stable or falling prices. Wages were weak. Inflation expectations remained low. The economy was recovering, but not strongly enough to transform wage and price-setting behavior.

In this environment, higher oil prices mainly operated as a tax on real income. They raised costs for firms and prices for consumers, but they did not generate a sustained rise in wages or expectations. The result was a modest increase in headline inflation, but little change in underlying inflation.

Finally, let me turn to the most recent episode, beginning around 2021. At one level, this was again an external cost shock. Energy and food prices rose, global supply chains were disrupted, and Russia's invasion of Ukraine intensified pressures on commodities. For Japan, yen depreciation further amplified the rise in import prices.

But unlike in the mid-2000s, energy and food price inflation did not remain merely a temporary relative-price shock. Price increases became broader. Firms became more willing to pass on higher costs. Wage growth also began to rise, especially through the spring wage negotiations. Inflation expectations moved up from very low levels. These points are shown in Chart 5.

What made this episode different? First, the shock was broader. It was not just oil. It included energy, food, logistics, and imported materials. When many firms face rising costs at the same time, the barrier to raising prices becomes lower. Another way of saying this is it came during a global demand recovery from the shutdown related to the Covid-19 pandemic.

Second, yen depreciation amplified the shock. In the second oil shock, prior yen appreciation had cushioned import prices. In the recent episode, yen depreciation worked

in the opposite direction.

Third, the labor market was tighter. Japan's demographic structure meant that labor shortages were becoming more persistent. This changed the environment for wage bargaining.

Fourth, price and wage norms began to change. For decades, firms and households had behaved as if prices and wages would not rise much. But repeated and visible price increases weakened that norm. Firms became more willing to raise prices, and workers became more willing to demand wage increases.

For these reasons, the recent episode became more persistent than the oil price surge of the mid-2000s. Still, Japan has not experienced an early 1970s-style wage-price spiral. Medium- to long-term inflation expectations have shifted only modestly upward from a long-entrenched near-zero level to a range of 1.5–2+%, depending on the measure. This stands in contrast to the United States and Europe, where inflation expectations were already meaningfully positive when the shocks hit—leaving much less room between the starting point and high inflation significantly above 2%.

The policy implication of all this seems to be that central banks should not look at oil prices in isolation. The same oil price increase can have very different effects depending on wages, expectations, demand, and exchange rates. That is, initial conditions matter enormously. If inflation expectations are already high and wages are accelerating, the risk of second-round effects is large. If expectations are very low and wages are stagnant, even a large cost shock may not raise underlying inflation.

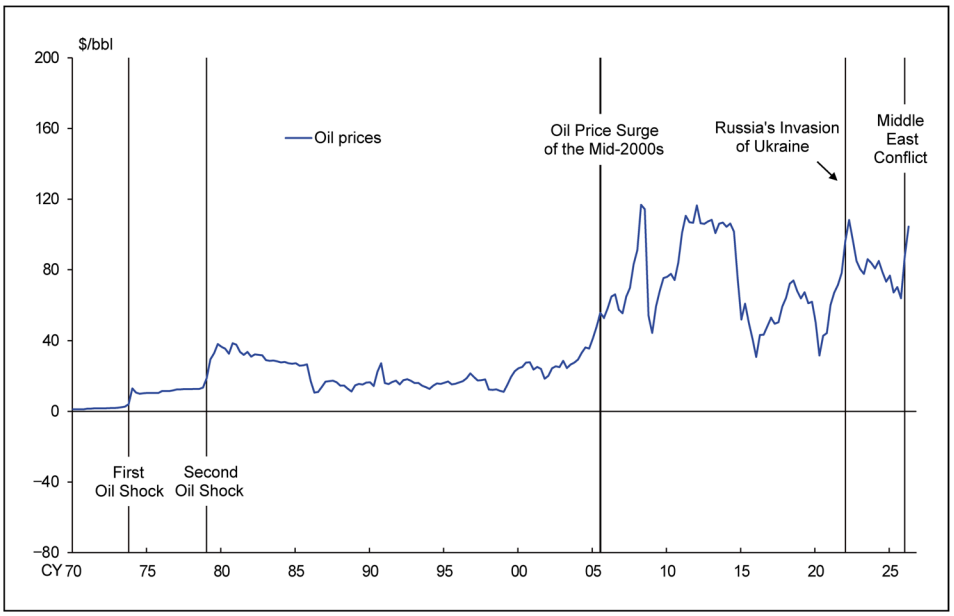
Thus, the boundary between temporary and persistent inflation is not mechanical. A temporary shock can become persistent if it changes wages, expectations, and price-setting behavior. Conversely, a large shock can remain temporary if those channels do not activate.

Let me conclude. Japan's experience shows that oil price shocks are never just oil price shocks. They are tests of the entire inflation regime.

In the first oil shock, the regime was already inflationary, and the shock intensified it. In the second, the economy had learned from the first, and the shock was contained. In the mid-2000s, the regime had shifted to a deflationary one, and the oil price surge could not change it. In the recent episode, the shock was broad and persistent enough to help move Japan away from the old deflationary norm, though not into an early 1970s-style inflation spiral.

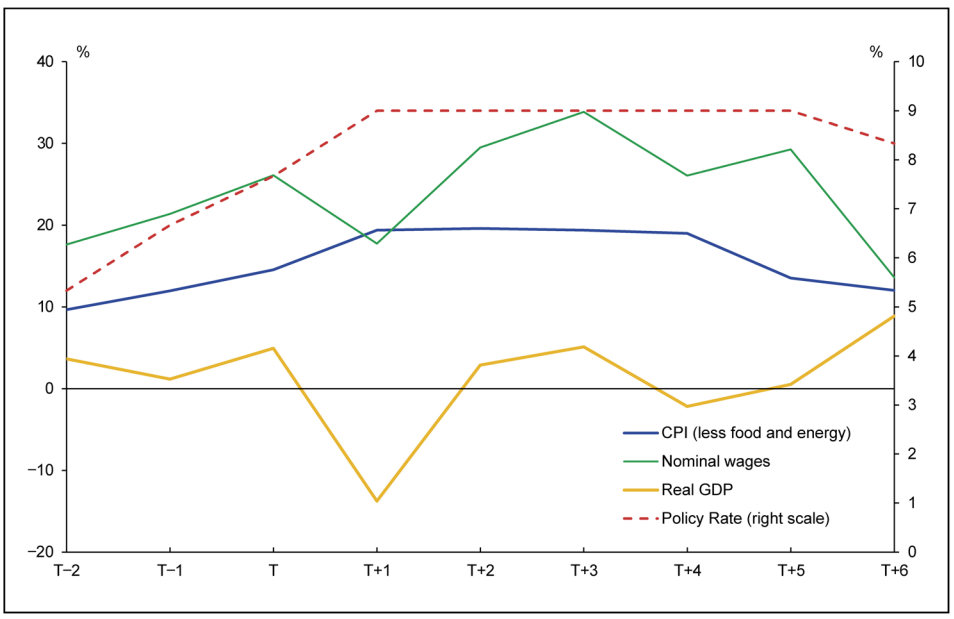
We are actually facing a fifth oil price shock. What are the important initial conditions that will matter for the evolution of the economy from here? What inflation regime are we in now? And, what is the best response from central banks around the world, including the BOJ? I look forward to hearing your views on these points during the conference.

Chart 1 Oil Prices and Notable Incidents



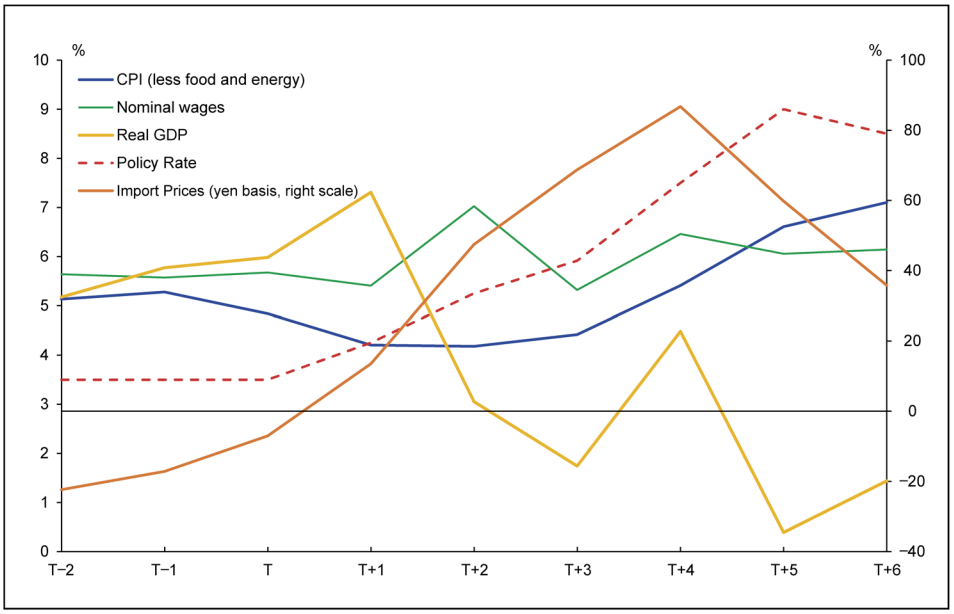
Note: Oil prices are Dubai crude oil prices.
Sources: Nikkei NEEDS; World Bank.

Chart 2 The First Oil Shock (T=Q4:1973)



Note: Policy rate is the Official Discount Rate. Real GDP is expressed as quarter-on-quarter annualized growth rate; CPI and nominal wages are year-on-year percent changes.
Sources: Bank of Japan; Cabinet Office; Ministry of Health, Labour and Welfare; Ministry of Internal Affairs and Communications.

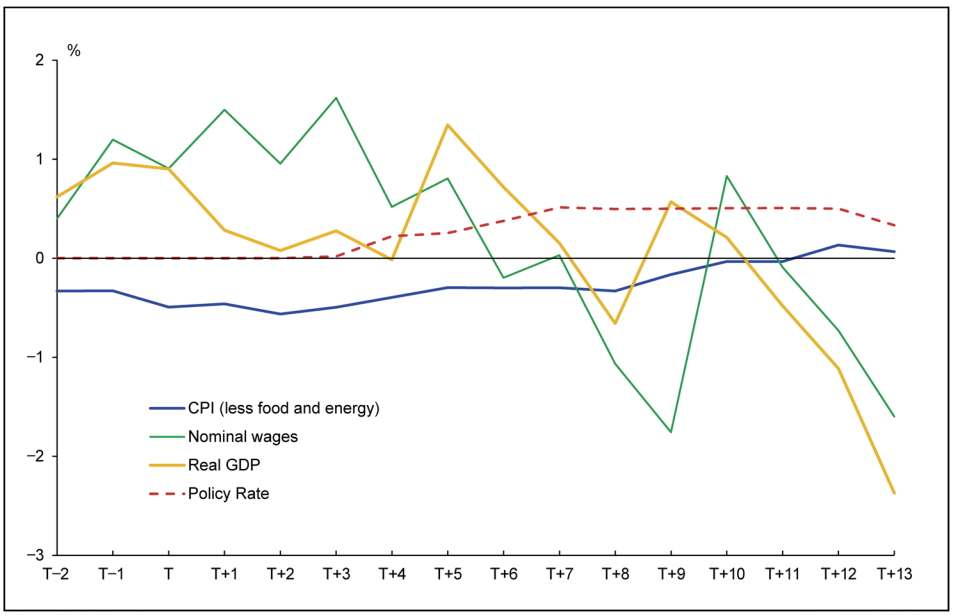
Chart 3 The Second Oil Shock (T=Q1:1979)



Note: Policy rate is the Official Discount Rate. Real GDP is expressed as quarter-on-quarter annualized growth rate; CPI, nominal wages, and import prices are year-on-year percent changes.

Sources: Bank of Japan; Cabinet Office; Ministry of Health, Labour and Welfare; Ministry of Internal Affairs and Communications.

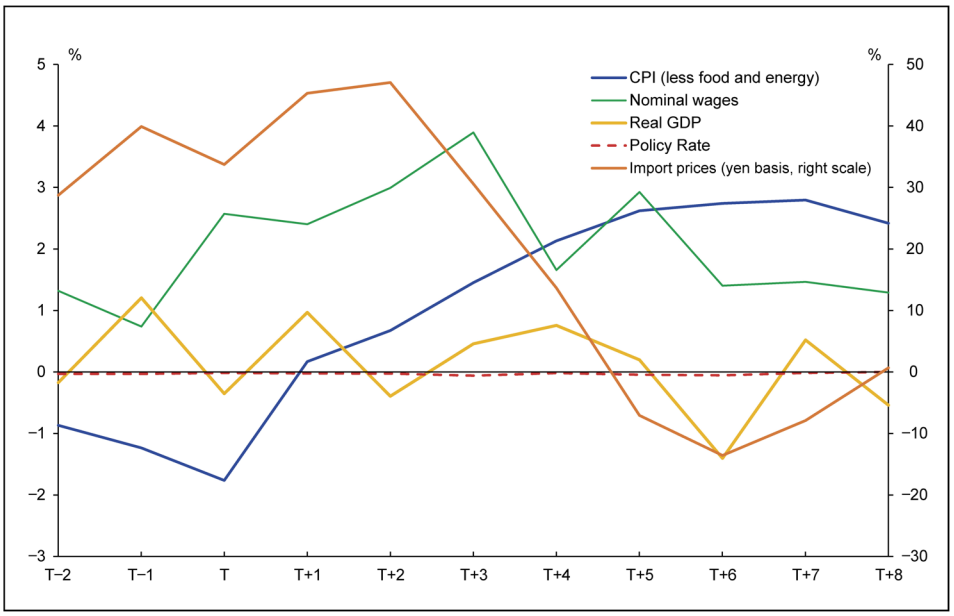
Chart 4 The Oil Price Surge of the Mid-2000s (T=Q3:2005)



Note: Policy rate is the uncollateralized overnight call rate. Real GDP is expressed as quarter-on-quarter percent change; CPI and nominal wages are year-on-year percent changes.

Sources: Bank of Japan; Cabinet Office; Ministry of Health, Labour and Welfare; Ministry of Internal Affairs and Communications.

Chart 5 Russia's Invasion of Ukraine (T=Q1:2022)



Note: Policy rate is the uncollateralized overnight call rate. Real GDP is expressed as quarter-on-quarter percent change; CPI, nominal wages, and import prices are year-on-year percent changes.

Sources: Bank of Japan; Cabinet Office; Ministry of Health, Labour and Welfare; Ministry of Internal Affairs and Communications.

The Mayekawa Lecture: Challenges to Independence: How should Central Banks Respond —Lessons from History

by Donald Kohn

I. Introduction

I am honored to deliver this conference's Mayekawa Lecture. Governor Ueda asked me to reflect on central bank independence, drawing on my experience and the lessons history offers for protecting it.

Threats to independence have risen sharply in the United States—to levels not seen since the Fed-Treasury accord of 1951. My remarks will draw primarily on the institutional and political circumstances of the U.S. But speeches by central bankers outside the U.S. suggest these concerns are broader, and preserving independence has become among the defining institutional challenges of the moment.[1]

I'll start by defining independence and documenting the growing pressures against it. I'll ask why these pressures have intensified and what central banks can do in response. In addition to my own experience, I will draw on conversations with a number of current and former central bankers as I prepared this lecture.

II. What Do We Mean by Independence

I suspect no one in this audience doubts the importance of insulating central banks, to some degree, from short-term political pressures. We have extensive evidence—across time and across countries—that when politicians control monetary policy, electoral incentives make it difficult to sustain a credible commitment to price stability. Recognizing the need for a longer horizon, elected representatives have delegated authority to independent central banks with clearly defined objectives—most often price stability, or in the case of the US, maximum employment and price stability.[2]

The author holds the Robert V. Roosa Chair in International Economics and is a senior fellow at the Brookings Institution.

This paper was prepared as the Mayekawa Lecture at the 2026 BOJ-IMES Conference, Tokyo, Japan, May 27–28, 2026. The views expressed in this text are those of the author and do not necessarily reflect the official views of the Bank of Japan.

1. Recent examples include: Bailey (2026), Hernández de Cos (2025), and Schnabel (2026).
2. The case for independent central banks is summarized well in the amicus brief filed by former Federal Reserve Chairs and Treasury Secretaries in the Lisa Cook case.

In a democracy, however, delegated authority has limits. In the United States it applies primarily to monetary policy in the pursuit of that "dual mandate". It does not extend to regulatory authority, which is more inherently political and is coordinated with other federal and state agencies. But it does encompass lender of last resort functions for banks to support financial stability. I will return later to the complicated intersection of central bank independence and financial stability.

Democratic accountability is maintained in the give and take between the central bank and elected representatives. And control is asserted over the medium and long-term through the appointments process. In the U.S. Federal Reserve governors are appointed by the president and confirmed by the Senate.

Independence rests on both laws and norms. Legally, the Federal Reserve controls its own budget; governors serve long staggered terms; chairs and vice chairs are designated for four-year terms; and governors can only be removed "for cause", generally understood to mean serious misconduct in office rather than policy disagreement. Reserve Bank presidents, who participate in monetary policy deliberations as effectively external members of the policy committee, are chosen by regional boards, subject to the approval of the Federal Reserve Board.

But legal protections alone are insufficient. Independence also depends on norms: appointing technically qualified officials willing to exercise independent judgment; respecting the diversity of views among reserve bank presidents; and the principle that policy disagreement is not grounds for dismissal. It is this final norm that President Trump, in effect, has been challenging.

III. Threats Have Increased and Could Intensify Further

President Trump's efforts to exert greater control over the Federal Reserve are unusual in scale and intensity, accompanied by sustained and often personal public criticism of Chair Powell and Federal Reserve policy.

To be sure, presidents have long preferred lower interest rates. Some have voiced that preference publicly; others exerted substantial pressure behind the scenes—notably Lyndon Johnson on William McChesney Martin and Richard Nixon on Arthur Burns. History suggests that when central banks yield to sustained political pressure for easier policy, inflation often follows.

The limited congressional response to recent threats has been troubling. Legislators in both parties generally understand and defend the principle of central bank independence. But many Republicans appear reluctant to challenge the president directly, while Democrats—though often supportive of independence—have historically placed greater emphasis on the employment side of the Federal Reserve's dual mandate and have not always been equally comfortable with an independent central bank prioritizing price stability.

The broader economic environment may intensify these political pressures. In many advanced economies, including the United States, rising public debt implies

https://business.cch.com/BFLD/Trump-v-Cook-US-Amici-Curiae-Former-Treasury-Secretaries-Fed-Chairs-09252025.pdf.

growing debt-service burdens that constrain governments' fiscal choices, especially if higher interest rates are needed to contain inflation.

At the same time, several structural disinflationary forces that supported price stability between roughly 1990 and 2019 are weakening or reversing. Trade liberalization and the integration of large economies into global markets lowered costs and supported disinflation. Today, tariffs, industrial policy, and efforts to build more resilient supply chains may work in the opposite direction.

Recent years have also been marked by adverse supply shocks: pandemic disruptions, energy price spikes following Russia's invasion of Ukraine and conflict in the Middle East, and tariff increases. These shocks raise prices while reducing real incomes—effects monetary policy cannot fully offset. Yet they also heighten public dissatisfaction with economic outcomes and increase the temptation for political leaders to assign blame to central banks.

Ironically, these circumstances strengthen rather than weaken the case for independence. When inflationary pressures arise from forces beyond monetary policy's control, political incentives to demand short-run relief become stronger, even as the need for disciplined policy becomes greater.[3]

IV. How Did We Get Here

President Trump's efforts to pressure the Federal Reserve may be extreme, but they emerge from broader political and economic developments. Across many democracies, populist movements have drawn strength from dissatisfaction with economic outcomes—especially rising inequality, stagnant mobility, and pessimism about the future.

These movements are often characterized by distrust of technocrats who are perceived as distant from the concerns of much of the population. Populist movements also tend to be skeptical of globalization—the freer movement of goods, capital, and people across borders—which many citizens see as benefiting elites while leaving others behind. Economists often emphasize aggregate gains in efficiency and lower costs from globalization; populist political movements focus more heavily on visible distributional consequences and the erosion of national autonomy. Rules-based systems and international commitments may therefore be viewed less as safeguards and more as constraints on corrective action, including trade restrictions or industrial policy.[4]

Distrust of technocratic institutions is often accompanied by a preference for more centralized political authority and by increasing polarization of political life. The rapid spread of unfiltered information through social media has amplified these tendencies, making it harder to distinguish fact from fiction and more difficult to sustain confidence in expert institutions.

Central banks are particularly vulnerable in this environment. By design, they are technocratic institutions. Their decisions depend on analysis, evidence, and long-term reasoning rather than immediate political responsiveness. They operate within an inter-

3. These forces and the need to strengthen independence are discussed in Afrouzi *et al*. (2024) and Kohn (2024) comment on this paper. https://www.brookings.edu/articles/changing-central-bank-pressures-and-inflation/.
4. For a more complete discussion see Goodhart and Lastra (2018).

national system of cooperation. Central banks are often perceived—fairly or not—as aligned with the interests of financial institutions rather than the broader public. Most importantly, central bank independence constrains elected leaders, which makes it a natural target for movements skeptical of institutional limits on political authority.

Economic events over the past two decades have reinforced these pressures on central banks. The Federal Reserve was criticized for failing to foresee or prevent vulnerabilities that contributed to the Global Financial Crisis and later for the inflation surge of 2021–23. Both episodes had multiple causes, many outside the control of central banks. But central banks are ultimately held responsible for financial and price stability, and failures—whether perceived or real—can erode public confidence.

Crisis responses also generated backlash. Near-zero interest rates and large-scale asset purchases were criticized for widening wealth inequality and blurring the boundary between fiscal and monetary policy. Emergency lending during the financial crisis was portrayed as "bail outs" favoring financial institutions over households harmed by the crisis.

In the United States, the post-pandemic inflation miss was partly self-inflicted. In 2020, the FOMC adopted a revised framework that emphasized the benefits of a strong labor market and placed less weight on preemptive responses to inflation risks. In my view, the framework and its implementation in forward guidance on rates and securities purchases contributed to a delayed response to emerging inflation pressures in 2021.[5]

The Federal Reserve also justified aspects of the framework in part by reference to employment opportunities for historically disadvantaged demographic groups.[6] However well intentioned, this risked stretching a narrow macroeconomic mandate toward objectives monetary policy is not well suited to achieve with a single instrument.

Some central banks also entered politically contested terrain—Brexit in the United Kingdom, climate policy in Europe and the United Kingdom. Ethical lapses by several Federal Reserve officials related to financial trading further damaged institutional credibility.

V. What Can Central Banks Do to Strengthen the Support for Independence?

In a democracy, the degree of central bank independence ultimately depends on political support, reinforced by legal protections that are respected by the courts. Central banks therefore need to ask what they themselves can do to sustain that support in a more difficult political environment.

At a high level, the answers are straightforward—though much harder to implement.

First, central banks should remain focused on the core objectives assigned by law

5. See Eggertsson and Kohn (2023): https://www.brookings.edu/articles/the-inflation-surge-of-the-2020s-the-role-of-monetary-policy/. To be fair, many members of the FOMC do not agree with our analysis; they point to very similar experiences in jurisdictions where there was no change in the historic focus on price stability. In this view, the main culprit was faulty inflation forecasts. Nonetheless, the 2020 alterations were largely reversed in 2025 (Powell 2025). https://www.federalreserve.gov/newsevents/speech/powell20250822a.htm.
6. Powell (2020a). https://www.federalreserve.gov/newsevents/speech/powell20200827a.htm.

and justified by experience: price stability and, where relevant, financial stability. They should avoid peripheral or politically contested objectives that risk distracting from those missions or diluting accountability.

This is not simply a question of institutional restraint. Monetary policy is already difficult. Supplemental goals can complicate decision-making and blur the connection between policy actions and legislated objectives. That connection matters—not only for accountability, but for policy effectiveness.

Second, central banks must be as successful as possible. Competence is the strongest defense of independence. If central banks repeatedly fail to achieve their mandates, the rationale for delegating authority weakens.

Of course, much lies outside their control: supply shocks, geopolitical events, fiscal choices, and structural change. But central banks must provide a credible explanation of how policy will navigate these developments and return the economy toward mandated objectives. And when policy falls short, candid analysis of mistakes can strengthen rather than weaken credibility.

Third, communication matters. Central banks have made enormous progress in communicating with markets and academics. Reaching legislators and the broader public—the ultimate arbiters of independence—has proven more difficult, but also increasingly necessary.

I will organize the remainder of these remarks around those three themes: focus, success, and communication. I begin with monetary policy, drawing on the experiences of the three chairs with whom I worked most closely—Paul Volcker, Alan Greenspan, and Ben Bernanke. I will then turn to two especially difficult challenges for independence: unsustainable fiscal trajectories and financial instability.[7]

VI. Monetary Policy

Focus: For most central banks, price stability is their primary legal objective. Even for a dual mandate central bank like the Federal Reserve, price stability is a necessary condition for meeting its other goal of maximum employment on a sustained basis. When households and businesses don't have to factor a guess about future inflation into their decision-making, uncertainty is reduced and resource allocation is more efficient. And by anchoring inflation expectations, credibility for achieving price stability gives scope for the central bank to lean against many disturbances to maximum employment. Paul Volcker, Alan Greenspan, and Ben Bernanke, all focused their monetary policy communication and actions around this proposition.[8]

Let me be clear that I am not suggesting a singular focus on price stability that ignores the effects of monetary policy on income and employment. There are often

7. Schnabel (2026) addresses these issues from the ECB's perspective. https://www.ecb.europa.eu/press/key/date/2026/html/ecb.sp260507_1~d5ae988ece.en.html.
8. For example, Greenspan: "a central bank's vigilance against inflation is more than a monetary policy cliche, it is, of course, the way we fulfill our ultimate mandate to promote maximum sustainable growth." For many similar examples from Volcker and Greenspan see López-Salido *et al.* (2024): https://www.federalreserve.gov/econres/feds/files/2024041pap.pdf?utm_source=chatgpt.com. Greenspan (2001): https://www.federalreserve.gov/boarddocs/speeches/2001/200105242/default.htm. Bernanke (2006) articulated the same idea in https://www.federalreserve.gov/newsevents/speech/bernanke20060224a.htm.

multiple paths to price stability; central banks should acknowledge in their communications and their policies that their choices will affect labor markets and opt for those that minimize adverse effects. Volcker, Greenspan and Bernanke were all flexible inflation targeters, even if the first two didn't call it that.

Success: Success begins with clarity about the mandate and with a coherent explanation of how policy actions support it. That explanation is a key to successful policy. Models help organize a complicated world and illuminate historical relationships, but they are simplifications. They depend on assumptions, incomplete knowledge, and imperfect representations of human behavior. In practice, policymaking requires something more: a narrative—a disciplined story about what is happening in the economy, what forces are driving outcomes, and how policy should respond. Models inform that story, but they cannot substitute for it. The narrative must be grounded in evidence, internally coherent, and open to revision when facts change. That last requirement points to two essential policymaking virtues: flexibility and humility.[9]

Recognizing when a story no longer fits the evidence is often harder than constructing it in the first place. Paul Volcker offers an example. In 1979 he embraced monetary targeting because he believed controlling money growth was necessary to reduce inflation and because it freed policymakers from pretending they knew precisely what interest-rate path would restore price stability. By 1982, however, circumstances had changed. Inflation had fallen but remained elevated, unemployment and interest rates were extraordinarily high, strains in the banking system were emerging, and financial deregulation had weakened the relationship between money growth and inflation. Volcker adapted. He moved back toward interest-rate targeting without abandoning the longer-run objective of restoring price stability.

Alan Greenspan greatly admired what Volcker had accomplished, and he was determined to finish the job. He was very clear that price stability remained the lodestar of monetary policy; he leaned hard against any early signs of a coming uptick, and he monitored inflation expectations carefully for hints of backsliding. But inflation was sufficiently low that he didn't see the need to put the economy through the ringer to achieve that last mile.

Greenspan always had a narrative to back his policy recommendations—albeit often unconventional and occasionally hard to understand, but one that could be and was often altered by new information and insights. His ability to shift the narrative and policy in a timely way was key to the soft landing of 1993–94, and to the accommodation of the productivity surge in the mid-1990s.

Bernanke confronted a different challenge. In 2007 he pivoted quickly from concerns about inflation toward stabilizing a deteriorating financial system and cushioning the macroeconomic fallout.

Volcker, Greenspan, and Bernanke differed in style and circumstance, but they shared a willingness to revise views when events challenged prior assumptions. They were flexible.

Flexibility in turn rests on a certain kind of humility. None of these chairs lacked confidence. But all understood the limits of knowledge. They were suspicious of dog-

9. Kay and King (2020) stresses the key role of narratives in policy making.

matic forecasts and policy positions. They reached out widely for new ideas or to test their own. Ben Bernanke faced a very different set of challenges after the financial markets began to freeze up. He provided very clear direction that we were going to supply the liquidity that stabilized institutions and markets, but he reached out to other policymakers and staff for ideas about how to accomplish this in unprecedented circumstances.

Strong staff are an often-underappreciated asset in conducting successful policy. Good staff, empowered to speak their minds, will be a resource for policymakers to test ideas in informal conversations. Staff will provide institutional memory while also being an avenue for bringing new ideas and the most recent research into policy analysis. Staff papers contribute to transparency and accountability by exposing the thinking and models informing policy to outside critical analysis. Staff forecasts are most often the starting place for the discussion of the economy and policy. All three of these chairs interacted extensively and in substantive ways with their staff.

Communication: Good communication is essential to preserving central bank independence.

Independence in a democracy requires accountability. Public understanding of the logic behind policy—why actions are taken and how they connect to legislated objectives—is part of that accountability. Communication also improves effectiveness: when markets understand the central bank's reaction function, policy works more efficiently through expectations and financial conditions.

Paul Volcker was skeptical of extensive transparency. He worried that policymakers would be held hostage to forecasts that reality might quickly invalidate and that excessive specificity could constrain flexibility. But even Volcker recognized that major policy shifts required explanation. He communicated extensively around the move to monetary targeting and again around the shift away from it, through speeches, testimony, and press conferences.

Equally important, Volcker engaged directly with constituencies most affected by tight policy. These were often uncomfortable encounters, but they demonstrated that the Federal Reserve was listening and provided an opportunity to explain why short-term pain was necessary to secure long-term gains.

Greenspan inherited some of Volcker's skepticism but gradually concluded that unnecessary uncertainty reduced policy effectiveness. Beginning in 1994, the Federal Reserve immediately announced policy decisions and increasingly explained the reasoning behind them.

Bernanke extended this evolution considerably, expanding forecasts and introducing regular press conferences in the service of both effectiveness and accountability.

Greater transparency, however, creates challenges. Communication must remain consistent with the flexibility and humility required for good policymaking.

Forecasts should communicate uncertainty, not false precision. Central banks know less than outsiders sometimes assume and should say so plainly. Scenario analysis can help explain risks and alternative outcomes without overstating confidence in any single path.

The same caution applies to forward guidance. Policy projections cannot become commitments that inhibit course correction when circumstances change. Forward guid-

ance is especially valuable near the effective lower bound, when policymakers need to shape expectations about future accommodation. Away from the lower bound, clear communication about the policy framework and economic narrative should reduce the need for explicit rate guidance.

Communication with legislators deserves particular emphasis. No constituency matters more for central bank independence. Better understanding can improve oversight, strengthen accountability, and reinforce institutional legitimacy. Jay Powell has devoted substantial effort to congressional outreach and, despite intense political pressure, broad support for monetary policy independence has largely held.

Powell has also provided a master class in communication when attacked by the president. He tuned out the noise for as long as possible, not responding and emphasizing that policy was made on the best analysis possible without regard to politics. But when the legal system was enlisted into the attack, he called it out, rallying support.

Communication with the broader public is more difficult. Most citizens rationally devote little attention to central banking when inflation is low, growth is steady, and institutions function well. But when inflation rises or independence is questioned, public attitudes matter.

Central banks therefore need to keep experimenting with ways to explain their role beyond specialist audiences. Success will be limited, especially in a media environment shaped by social platforms that reward speed, emotion, and oversimplification. Still, engagement matters. Institutions staffed by technocrats must show that they are listening as well as explaining.

VII. The Challenge of Unsustainable Fiscal Trajectories

Public finances are on unsustainable paths in many advanced economies. Debt relative to income has risen to historically high peacetime levels and, in many countries, is projected to continue increasing because of aging populations, geopolitical demands, and persistent structural deficits. That is going to put upward pressure on interest rates and along with strong investment demand—including for AI-related capital spending—may keep interest rates above growth rates for a time, limiting the ability of governments to stabilize debt burdens without major policy changes.

The extreme concern is fiscal dominance: a loss of confidence in government debt that pressures the central bank to finance public borrowing and subordinates monetary policy to fiscal needs, sacrificing price stability and independence.[10] That is not our current situation. But fiscal pressures can threaten independence well before outright fiscal dominance emerges.

Persistent deficits imply increasing debt servicing obligations, impinging on other government priorities. President Trump has justified his call for lower rates and his efforts to control the Federal Reserve in part on budgetary grounds.[11]

Governments facing constrained fiscal space may also expect monetary policy to

10. For a summary of the threat of fiscal dominance see Yellen (2026): https://www.brookings.edu/articles/remarks-by-janet-l-yellen-on-the-future-of-the-fed-central-bank-independence-and-fiscal-dominance/.
11. https://www.reuters.com/world/us/trump-again-calls-fed-board-act-says-powell-doesnt-get-it-2025-07-23/.

shoulder more responsibility during downturns or crises—even when monetary tools are poorly suited to the problem. Financial crises, for example, require close coordination: central banks address liquidity, while fiscal authorities address solvency. Severe downturns at the effective lower bound often require monetary and fiscal policy to work together.

Central banks do not make fiscal policy, but they can clarify its consequences.

In the United States, Federal Reserve officials have generally become more cautious about prescribing specific fiscal actions, appropriately recognizing the limits of technocratic authority. Volcker and especially Greenspan were more willing to comment directly on taxes and spending, sometimes too willing in my view. Subsequent chairs focused less on policy prescriptions and more on economic implications. Bernanke advocated less fiscal restraint during the weak post-crisis recovery; Powell supported fiscal support during the pandemic recovery when monetary policy alone was insufficient.[12]

Powell has repeatedly warned that current fiscal trajectories are unsustainable and may eventually limit governments' ability to respond to recessions while crowding out productive investment. This strikes me as the right balance: central banks should explain economic consequences clearly and forcefully while avoiding prescriptions about precisely how elected officials should close fiscal gaps.

Fiscal stress also raises difficult operational questions. Asset purchases have been used to address market dysfunction and to support macroeconomic stabilization at the effective lower bound. But central banks will protect themselves by clearly defining purchases undertaken for monetary policy or market-functioning purposes so they are not mistaken for actions to simply finance government borrowing or interfere with appropriate price adjustments. That will require setting out ahead of time criteria and circumstances that might trigger true market dysfunction or monetary policy purchases.

VIII. Financial Stability and Central Bank Independence

Financial stability is a core responsibility of most central banks, even where it is not always stated explicitly. In the United States, for example, the Federal Reserve was created in large part to mitigate the recurring financial panics of the late nineteenth and early twentieth centuries. It was given tools to do so: bank supervision, liquidity provision to individual banks at the discount window, and eventually broader open market operations and emergency lending powers to nonbanks.[13]

Yet financial stability presents special challenges for independence because responsibility is often shared. In the United States and elsewhere, central banks operate alongside other supervisory and regulatory agencies, many focused primarily on the safety and soundness of individual institutions rather than system-wide resilience. Central

12. For example, Bernanke testimony of 5/22/2013 (Bernanke 2013): https://www.federalreserve.gov/newsevents/testimony/bernanke20130522a.htm. Powell speech of 10/06/2020 (Powell 2020b): https://www.federalreserve.gov/newsevents/speech/powell20201006a.htm.
13. The preamble to the Federal Reserve Act: "An Act To provide for the establishment of Federal reserve banks, to furnish an elastic currency, to afford means of rediscounting commercial paper, to establish a more effective supervision of banking in the United States, and for other purposes."

banks also frequently lack authority over nonbank intermediaries, where risks may accumulate.

Central banks nevertheless bring a distinctive perspective. Because monetary policy works through financial conditions, central banks operate at the intersection of macroeconomics and financial markets. They monitor vulnerabilities across institutions and markets and are uniquely positioned to assess how shocks may propagate through the broader economy. Independence matters here as well. Short-term political incentives may favor deregulation that stimulates credit and activity in the near term while increasing systemic fragility over time. A degree of insulation allows policymakers to take the longer view.

When instability strikes, the central bank's capacity to provide liquidity becomes indispensable. One early episode in my career illustrates the point. Following the 1987 stock market crash, when equity prices fell more than 20 percent in a single day, the Federal Reserve responded with a brief but powerful statement affirming its readiness to supply liquidity to support the functioning of the financial system. That statement, reinforced by extra open market operations, easing policy, and work behind the scenes to keep payments flowing, helped stabilize markets and prevent broader disruption.[14] Similar principles guided responses in the much more severe crises of 2008 and 2020.

Price stability and financial stability are closely connected.[15] Stable financial institutions improve the transmission of monetary policy, while a resilient financial system gives central banks greater confidence to tighten policy when needed without fear of widespread instability. And crises can weaken support for independence. Central banks are often blamed for failures of supervision or financial excesses, even when responsibility is widely shared.[16] And crisis responses themselves can generate backlash, as we discussed earlier.

What, then, can central banks do?

Most importantly, they should continue to articulate clearly their independent assessment of systemic risk, its macroeconomic implications, and the policies necessary to address it.

In the United States, regulatory authority is becoming more closely aligned with the priorities of elected administrations. Among other causes, the tenure of the vice chair for supervision has become tied to the change in administrations, strengthening their influence inside the Federal Reserve. That is appropriate to a degree: regulation is more political than monetary policy because it often has disproportionate effects across firms and sectors.

But responsibility under the Federal Reserve Act ultimately rests with the Board as a whole. The public interest is best served when the Federal Reserve brings an independent, system-wide perspective to regulatory discussions and remains willing to speak candidly about systemic vulnerabilities—even when that view differs from the administration's.

14. See Carlson (2007): https://www.federalreserve.gov/pubs/feds/2007/200713/index.html.
15. The recent Bailey and Schnabel speeches referenced earlier both make this point in different ways.
16. See for example the conclusions of the Financial Crisis Inquiry Commission (2011), which leaned heavily on Alan Greenspan's deregulatory bent and supervisory failures at the Federal Reserve Bank of New York. https://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_conclusions.pdf. Others blame what they characterize as too-loose monetary policy in the years just before the crisis.

Such judgments are necessarily imperfect. Stress tests are useful but they are model and scenario dependent and don't cover all risks. Central banks should therefore use their macroeconomic perspective to resist procyclical tendencies in regulation and private risk-taking and to identify vulnerabilities that may otherwise be overlooked.

Where responsibilities are shared across agencies, central banks should first seek persuasion and coordination. But when concerns are ignored, public communication—through financial stability reports, speeches, and testimony—may become necessary. Over time, credibility and independence depend on exercising judgment well.

IX. Conclusion

These are difficult times for central banks.

The economic environment is challenging. Supply shocks have complicated the return to low and stable inflation after the inflation surge of 2021–23. Tariffs, geopolitical fragmentation, and concerns about supply-chain resilience may continue to place upward pressure on prices while weighing on real incomes.

At the same time, central banks operate in a political environment that is increasingly polarized, impatient, and skeptical of technocratic institutions. Rising public debt has heightened the fiscal consequences of monetary policy decisions. Reactions against post-crisis regulation may increase financial vulnerabilities even as central banks attempt to preserve resilience.

In such an environment, pressures on independence are likely to grow rather than recede. History nevertheless offers an encouraging lesson. Central bank independence has endured not because it is theoretically elegant, but because experience repeatedly demonstrates its value. We know from difficult experience that neither price stability nor financial stability is likely to be sustained without some insulation from short-term political pressure.

That insulation, however, cannot be taken for granted. It must be earned and re-earned. The strongest protections are not legal alone. They rest on disciplined focus, institutional competence, humility about uncertainty, and a willingness to explain difficult choices clearly and candidly. I have tried, drawing on my own experience and on the central bankers with whom I worked most closely, to suggest how institutions might preserve support for their independence in a more difficult era.

I conclude with a reminder from Paul Volcker: "In the last analysis independence rests on perceptions of high confidence, of unquestioned integrity, of broad experience, of nonconflicted judgment and the will to act. Clear lines of accountability to the Congress and the public will need to be honored."[17]

17. Volcker (2013). https://www.senseoncents.com/wp-content/uploads/2013/05/Volcker-Transcript-May2013.pdf.

References

Afrouzi, Hassan, Marina Holac, Kenneth Rogoff, and Pierre Yared. "Changing Central Bank Pressures and Inflation." *Brooking Papers on Economic Activity* Spring 2024 (2024): 205–41.

Bailey, Andrew. "Central Bank Independence—in need of further thinking—." speech at the Columbia University in New York, on April 14, 2026.

Bernanke, Ben S. "The Benefits of Price Stability." speech at The Center for Economic Policy Studies and on the occasion of the Seventy-Fifth Anniversary of the Woodrow Wilson School of Public and International Affairs, Princeton University, in Princeton, New Jersey, on February 24, 2006.

———. "The Economic Outlook." speech before the Joint Economic Committee, U.S. Congress, Washington, D.C., on May 22, 2013.

Carlson, Mark. "A Brief History of the 1987 Stock Market Crash with a Discussion of the Federal Reserve Response." Finance and Economics Discussion Series 2007–13, 2007.

Eggertsson, Gauti B., and Donald Kohn. "The Inflation Surge of the 2020s: The Role of Monetary Policy." Hutchins Center Working Paper 87, 2023.

Financial Crisis Inquiry Commission. *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*. Wasington: U.S. Government Printing Office, 2011.

Goodhart, Charles, and Rosa Lastra. "Populism and Central Bank Independence." *Open Economies Review* 29 (2018): 49–68.

Greenspan, Alan. "Economic Developments." speech before the Economic Club of New York in New York, on May 24, 2001.

Hernández de Cos, Pablo. "Delivering on central bank mandates in a changing world," speech at the Bank of Mexico 100th Anniversary Conference in Mexico City, on August 26, 2025.

Kay, John, and Mervyn King. *Radical Uncertainty: Decision-Making Beyond the Numbers.* New York: W. W. Norton & Company, 2020.

Kohn, Donald. "Comment on 'Changing Central Bank Pressures and Inflation.'" *Brooking Papers on Economic Activity* Spring 2024 (2024): 242–49.

López-Salido, David, Emily J. Markowitz, and Edward Nelson. "Continuity and Change in the Federal Reserve's Perspective on Price Stability." Finance and Economics Discussion Series 2024-041, 2024.

Powell, Jerome H. "New Economic Challenges and the Fed's Monetary Policy Review," speech at the "Navigating the Decade Ahead: Implications for Monetary Policy," an economic policy symposium sponsored by the Federal Reserve Bank of Kansas City, Jackson Hole, Wyoming (via webcast), on August 27, 2020a.

———. "Recent Economic Developments and the Challenges Ahead," speech at the National Association for Business Economics Virtual Annual Meeting, on October 6, 2020b.

———. "Monetary Policy and the Fed's Framework Review," speech at the "Labor Markets in Transition: Demographics, Productivity, and Macroeconomic Policy," an economic symposium sponsored by the Federal Reserve Bank of Kansas City, in Jackson Hole, Wyoming, on August 22, 2025.

Schnabel, Isabel. "The quiet erosion of central bank independence." speech at the Fifth Annual Charles Goodhart Lecture in London, on May 7, 2026.

Volcker, Paul. "Central Banking at a Crossroad." speech at the Economic Club of New York, on May 29, 2013.

Yellen, Janet L. "Remarks." speech at "The Future of the Fed," the annual meetings of the American Economic Association, on January 4, 2026.

The Presence of Foreign Open-End Funds in Japan's Financial Markets

by Kenta Yamamoto, Tomohiro Okubo, Nobuhiro Abe and Yukio Minoura

In recent years, the rising share of Non-Bank Financial Intermediaries (NBFIs) in the global financial system has been accompanied by an increase in the presence of foreign open-end funds in Japan's financial markets. This paper first documents the fund flows into equity, bond, and real estate open-end funds investing in Japanese financial assets, as well as their buying and selling behavior, using granular data sets. Similar to findings in existing studies, we find that significant outflows from foreign open-end funds investing in Japanese financial assets occurred during events such as the global financial crisis and the COVID-19 pandemic, as well as during episodes of rising policy interest rates abroad. These funds sold their assets, including their Japanese assets, in response to redemption requests. Next, we estimate the sensitivity of asset prices in Japan's stock and REIT markets to asset sales by market participants to understand the impact of trading by foreign open-end funds on Japan's financial markets. The estimated sensitivity is statistically significant and positive, and its magnitude is found to be close to estimates for the United States reported in the literature. These findings together imply that outflows from foreign open-end funds could affect asset prices in Japan's financial markets through asset sales during periods of stress originating abroad or when uncertainty in domestic financial markets rises.

Keywords: global investment funds; NBFIs; fund flows; price impact

JEL Classification: G01, G11, G12, G15, G23

Kenta Yamamoto: Financial System and Bank Examination Department (currently Personnel and Corporate Affairs Department), Bank of Japan (E-mail: kenta.yamamoto@boj.or.jp)

Tomohiro Okubo: Financial System and Bank Examination Department, Bank of Japan (E-mail: tomohiro.ookubo@boj.or.jp)

Nobuhiro Abe: Financial System and Bank Examination Department (currently Monetary Affairs Department), Bank of Japan (E-mail: nobuhiro.abe@boj.or.jp)

Yukio Minoura: Financial System and Bank Examination Department (currently Secretariat of the Policy Board), Bank of Japan (E-mail: yukio.minoura@boj.or.jp)

The authors thank Kosuke Aoki, Takeo Hoshi, and the staff of the Bank of Japan for their valuable comments and discussions. The views expressed in this paper are those of the authors and do not necessarily reflect the official view of the Bank of Japan or of the Financial System and Bank Examination Department.

DO NOT REPRINT OR REPRODUCE WITHOUT PERMISSION

I. Introduction

In recent years, the presence of Non-Bank Financial Intermediaries (NBFIs) in the global financial system has expanded significantly. This growth has been primarily driven by investment funds, particularly open-end funds, such as U.S. mutual funds, which account for a substantial proportion of the investment funds.[1] In Japan as well, foreign open-end funds have come to hold a significant share of assets in financial markets, with their asset holdings exceeding 10% of the market in the stock and REIT markets.[2]

While these open-end funds must always be able to accommodate investors' redemption requests and thus face risks on the liability side, the assets they hold include investments in less liquid assets, which could result in liquidity mismatches.[3] These funds typically hold liquid assets to prepare for redemptions. However, in times of market stress, if large-scale redemption requests are concentrated within a short period due to heightened investor liquidity demands, the funds may be forced to respond not only by using cash on hand but also by selling less liquid assets. Furthermore, if the sale of these less liquid assets leads to further price declines, the losses on the fund's holdings would result in losses for investors who continue to hold their investments without redeeming. In times of stress, this dynamic creates an incentive for investors, anticipating losses, to redeem more quickly. When this mechanism is at work, redemption pressures may be amplified, leading to fire sales of assets and sharp declines in asset prices.[4]

This paper examines the impact of stress events abroad on asset prices in Japan's financial markets by conducting an analysis in two ways: 1) an analysis of fund flows into foreign open-end funds and their investment behavior, and 2) an analysis of the impact of fund flows on price determination in the stock and REIT markets. In the first analysis, we conduct a detailed fact-finding and factor analysis of fund flows into equity, bond, and real estate funds that invest in Japan, as well as the trading behavior related to Japanese financial assets using high-granularity data on foreign open-end funds. The key takeaways are as follows: First, regarding fund flows, during shocks such as the global financial crisis in September 2008 and the initial phase of the COVID-19 pandemic in March 2020, there were outflows from funds in a number of asset classes. In particular, bond funds saw relatively large outflows. A panel analysis using fund flows as the dependent variable showed that stress originating abroad and deteriorating investor sentiment led to outflows from open-end funds investing in

1. FSB (2024b) and Oishi, Kobayashi, and Sugihara (2025) indicate that investment funds, particularly open-end funds, have accounted for a significant portion of the expansion of NBFIs in the global financial system in recent years.
2. In this paper, open-end funds established overseas are defined as "foreign open-end funds," and open-end funds established in Japan are excluded from the analysis. For information on the presence of foreign open-end funds in Japan's financial markets, refer to BOJ (2025) and Eguchi, Okubo, Yamamoto, and Washimi (2025).
3. The structural vulnerabilities inherent in open-end funds had been widely pointed out even before the COVID-19 pandemic by the Financial Stability Board (FSB) (FSB 2022, FSB 2023).
4. Based on a model that takes into account the impact of fire sales, Hogen, Kasai, and Shinozaki (2025) estimate the spillover effects (interconnectedness) between jurisdictions and asset classes. They also point out that, since the global financial crisis, the interconnectedness effects have been amplified significantly, both domestically and internationally.

Japan. On the other hand, during the market turmoil in August 2024, no significant outflows were observed, which supports the view of the IMF (2024) that the turmoil was largely driven by position adjustments of hedge funds.[5]

Second, regarding the sale of Japanese assets by foreign open-end funds, particularly in the initial phase of the COVID-19 pandemic, we document that asset sales were observed across various financial markets in Japan as a result of fund outflows. In particular, bond funds, such as government bond funds that shifted to U.S. government money market funds and mixed bond funds that invest in various bonds, exhibited significant sales of Japanese assets.[6] A detailed look at the sales of Japanese assets by mixed bond funds reveals that primarily government bonds were sold. This implies that foreign open-end funds respond to redemption requests by selling highly liquid assets.

In the second analysis, to examine the impact of asset sales by foreign open-end funds on Japan's financial markets, we estimate the price sensitivity in the stock and REIT markets to the buying and selling behavior of market participants, following the methodologies of previous studies, such as Gabaix and Koijen (2023) and Amihud (2002). While conventional asset pricing theory suggests that price sensitivity should be low, we argue that the price sensitivity of Japan's stock and REIT markets is relatively large. This result is consistent with recent empirical studies, including Gabaix and Koijen (2023).

A. Related Literature

In the initial phase of the COVID-19 pandemic in March 2020, asset sales by open-end funds were considered to have amplified asset price fluctuations. In this regard, various recommendations and proposals pertaining to the activities of open-end funds have been proposed by the FSB and the International Organization of Securities Commissions (IOSCO).[7] Against this backdrop, discussions and policy responses in each country have progressed.

For example, FSB (2020) conducts a holistic review of the market turmoil in the aftermath of the COVID-19 pandemic and emphasizes that substantial fund redemptions occurred, especially from bond funds and funds investing in emerging markets. Claessens and Lewrick (2021) analyze fund inflows and outflows by fund characteristics and show that, in March 2020, funds with a high proportion of less liquid or relatively high-risk assets, funds with higher institutional investor ownership compared to

5. In early August 2024, weaker-than-expected economic indicators in the U.S. triggered concerns about an economic slowdown, leading to a rapid decline in the dollar and global stock prices. A global depreciation of the dollar and policy changes by the Bank of Japan also led to a reversal of the previously one-sided depreciation of the yen, while domestic financial markets temporarily saw a sharp drop in stock prices. According to IMF (2024) and BOJ (2024), the unwinding of positions by hedge funds, including an increase in short sales of stocks in the futures market, likely had a significant impact on Japan's financial markets and asset prices during this period.
6. Kawasumi and Kataoka (2020) and FSB (2020) note that, with the onset of risk-off sentiment among investors, there was a shift from bond funds and prime MMFs to government MMFs.
7. IOSCO (2023) argues that if open-end funds do not use liquidity management tools (LMTs) to address liquidity mismatches, investors redeeming their shares may benefit at the expense of remaining investors. Consequently, IOSCO published guidance on the use of anti-dilution LMTs. FSB (2024a), in its comprehensive review of market disruptions during the COVID-19 pandemic, highlighted the vulnerabilities of NBFIs. In light of this, the FSB and IOSCO have provided reports on the progress of their work, along with policy recommendations and work plans aimed at enhancing the resilience of NBFIs.

household investors, and funds primarily investing in emerging markets experienced larger outflows.[8] Similarly, IMF (2022) discusses the unprecedented outflows that occurred during the COVID-19 pandemic, particularly in emerging market funds. Dekker, Vivar, Wedow, and Weistroffer (2024) analyze fund flows in open-end funds in Europe during the COVID-19 pandemic, highlighting that funds investing in relatively illiquid high-yield bonds experienced larger outflows, and that the reduction in cash buffers prior to the COVID-19 pandemic amplified the crisis.

On the other hand, there is limited prior research on the trends in open-end funds investing in Japanese financial assets and their impact on the financial markets. Hogen and Koide (2022) use high-granularity data on fund location and the asset allocation of investment funds to capture cross-border flows into real estate funds. They estimate the impacts of global financial and economic changes on investment flows and real estate prices in regions that serve as investment destinations, including Japan. Okamoto (2020) and Kankawa (2020) analyze the impact of the trading behavior of foreign investors on Japan's government bond market during the initial phase of the COVID-19 pandemic. In particular, Okamoto (2020) examines the effects of the rapid position adjustment by foreign investors on the government bond market and Kankawa (2020) empirically analyzes the factors determining the investment behavior of foreign investors engaging in arbitrage between Japan's government bonds with currency hedging and U.S. Treasury bonds, using data broken down by investor type. Koide, Hogen, and Sudo (2022) show that the degree of overlap between Japanese regional financial institutions and investment funds, measured by the correlation of returns on securities held, has been trending upwards. Moreover, they point out that the market value of the securities portfolios of financial institutions that have greater overlap with funds tend to respond more strongly during periods of stress in global financial markets, such as when large-scale redemptions occur in foreign funds. In addition, Japan's FSA has recently begun to conduct a monitoring survey of domestic investment funds, organizing data on exposures, liquidity, and leverage (FSA 2025). However, to the best of the authors' knowledge, there is no comprehensive research that uses high-granularity data to specifically examine fund flows into foreign open-end funds investing in Japan and the impact of subsequent asset sales on Japan's financial markets.

The structure of this paper is as follows: Section II outlines the composition of foreign open-end funds investing in Japan and the trends in their fund flows. In Section III, we analyze the trading activity of these funds in Japanese assets. Section IV provides estimation results of the price sensitivity in Japan's stock and REIT markets. Section V concludes the paper.

8. The data used in this study does not include information about fund investors, so the impact of differences in investor composition is not analyzed. In a prior study analyzing the impact of investor composition on fund flows, Allaire *et al*. (2023) point out that bond and equity funds with high ownership ratios by other funds experienced larger outflows in March 2020 compared to funds with higher household ownership ratios.

II. Fund Flows into Foreign Open-End Funds Investing in Japan

A. Composition of Open-End Funds

1. Overview of the data

This paper uses high-granularity data from LSEG Lipper on foreign open-end funds. This database includes information on approximately 900,000 share classes of domestic and international open-end funds (including merged or redeemed funds), along with attribute information such as asset types and fund domicile. It also contains financial data such as total net assets (TNA) and the cash holding ratio, as well as details on country-level investment allocations and asset holdings. The analysis covers the period from January 2007 to September 2024, using monthly frequency.

2. Composition of open-end funds

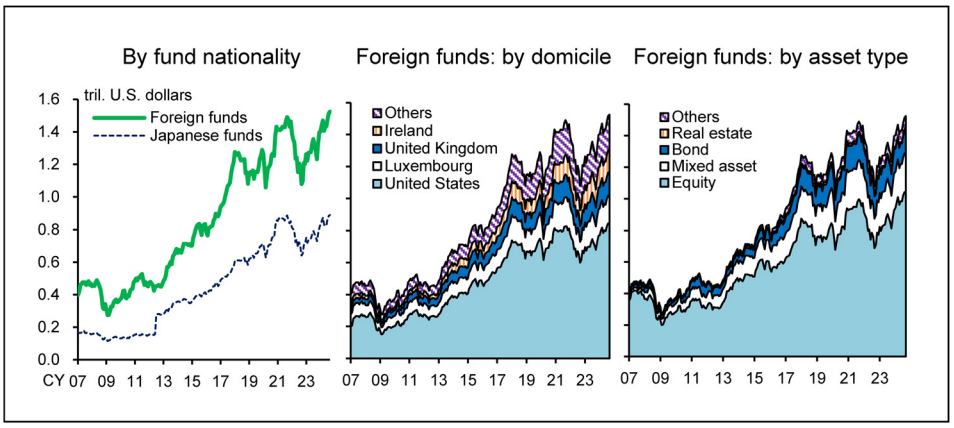
Using the above data, we observe that the amount of Japanese assets held by open-end funds has been trending upwards since the global financial crisis, particularly among foreign-domiciled funds (Figure 1). In terms of fund domicile, U.S.-domiciled funds account for more than half of total assets, with funds domiciled in Luxembourg, the U.K., and Ireland also holding notable shares. Regarding asset types, equity funds account for approximately 70% of the total, while mixed-asset and bond funds also have relatively large shares.

B. Fund Flows into Foreign Open-End Funds

1. Estimation of fund flows

Next, we analyze the fund flows into foreign open-end funds. The changes in fund assets noted in the previous section can be broken down into two components: 1) changes due to fluctuations in the market value of the assets held, and 2) increases or

Figure 1 Holdings of Japanese assets by open-end funds



Note: 1. Showsthe sum of Japanese asset holdings of individual funds (estimated as total net assets multipliedby the percentage of Japanese asset holdings). Latest data as of September 2024.
2. In the middle chart, domicile refers to the fund's country of establishment. In the right chart, "mixed asset" refers to funds that invest in both stocksand bonds. "Real estate" refers to funds that invest mainly in REITs.

Source: LSEG Lipper.

decreases due to investor fund flows (inflows and outflows).

$$TNA_t - TNA_{t-1} = TNA_{t-1} * \left(\frac{P_t}{P_{t-1}} - 1 \right) + flow_t. \quad (1)$$

Here, TNA_t represents the total net assets of the fund at time t, P_t represents the fund's price (net asset value per share) at time t, and $flow_t$ denotes the inflow of funds from investors from time $t-1$ to t.

By using the relationship above, we can estimate the fund flows by removing the effects of price fluctuations from the changes in asset values. The following analysis is based on fund flows calculated using the formula below.

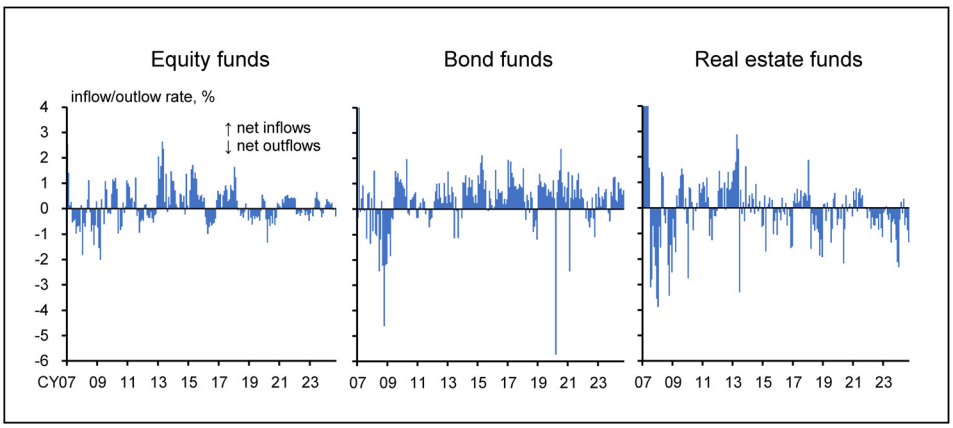
$$flow_t = TNA_t - TNA_{t-1} * \frac{P_t}{P_{t-1}}. \quad (2)$$

2. Fund flows into foreign open-end funds by asset type

We now examine the fund flows into foreign open-end funds investing in Japan, broken down by asset type. We show that, for equity, bond, and real estate funds, fund sizes have been on an upward trend driven by inflows, as calculated using the method above. However, during times of market turmoil, such as the global financial crisis in September 2008, the initial phase of the COVID-19 pandemic in March 2020, and the start of the U.S. interest rate hike cycle in March 2022, there were significant outflows across various asset types (Figures 2 and 3). In particular, bond funds experienced large outflows during the global financial crisis and the initial phase of the COVID-19 pandemic.

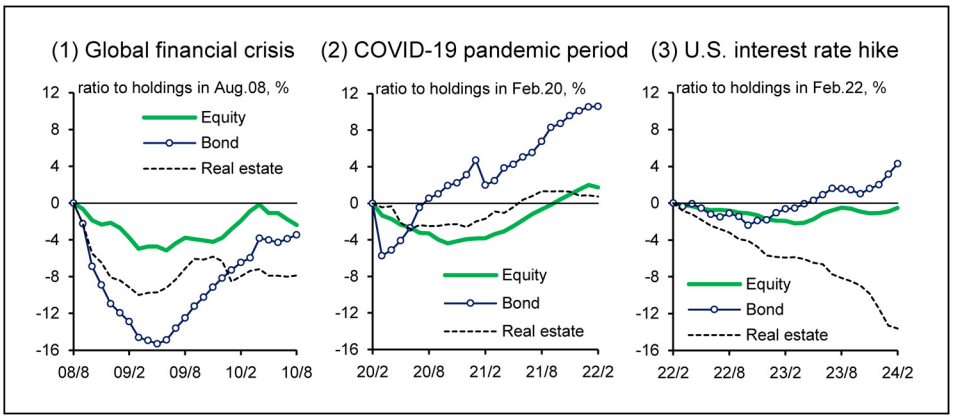
On the other hand, during the market turmoil of August 2024, no significant outflows were observed in any asset type. To better understand the movements during early August, we examine the fund flows of the 30 largest funds in the equity, bond, and real estate categories using daily data. While a slight outflow was observed in eq-

Figure 2 Asset type-based fund flow (1)



Note: 1. Covers foreign funds investing in Japan. Weighted average based on the value of Japanese asset holdings.
2. Latest data as of September 2024.
Source: LSEG Lipper.

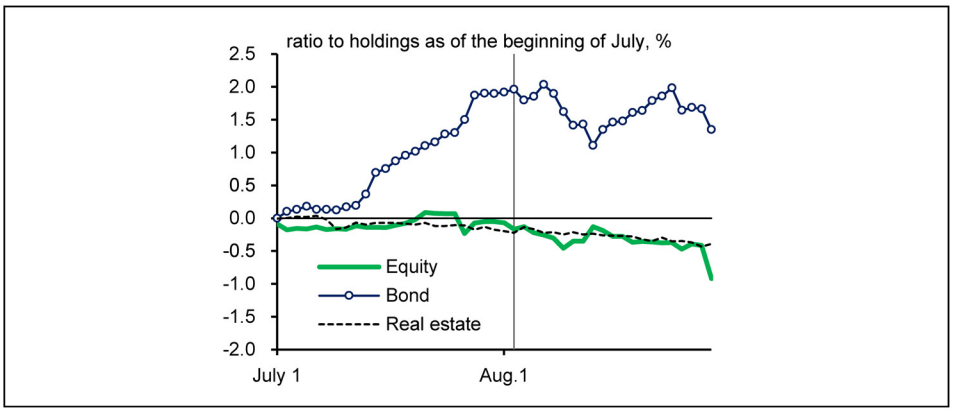
Figure 3 Asset type-based fund flow (2)



Note: 1. Covers foreign funds investing in Japan. Weighted average based on the value of Japanese asset holdings.
2. Cumulative change over a 24-month period following the shock, with the month before the shock as the starting point.

Source: LSEG Lipper.

Figure 4 Foreign fund flows during the market turmoil in August 2024



Note: 1. For foreign funds investing in Japan, the aggregated values are based on the top 30 holdings of Japanese assets, with data available on a daily basis (weighted average by Japanese asset holdings).
2. The cumulative fund flows since July (on a daily basis) are divided by Japanese asset holdings at the beginning of July.
3. The vertical line in the figure represents August 2, 2024 (the day the U.S. employment report for July was released).
4. Latest data as of end-August 2024.

Source: LSEG Lipper.

uity funds during the initial stage of the turmoil, it quickly reversed into inflows. Bond funds consistently showed net inflows during this period (Figure 4).[9] This suggests that the shock in August 2024 was primarily driven by position adjustments by hedge

9. The daily data used in this study are from the LSEG Global Fund Flows database, which contains high-frequency data (weekly and daily) on fund flows for each fund.

funds in the futures market, and it appears to be a different type of shock compared to the rapid surge in liquidity demand and the heightened stress in the real economy that occurred during the initial phase of the COVID-19 pandemic in March 2020.

3. Fund flows into foreign open-end funds by fund characteristics

In addition to asset types, it has been pointed out that the characteristics of the assets held by funds, such as liquidity, also influence fund flows. Falato, Goldstein, and Hortacsu (2021) and Jiang *et al*. (2022) conclude that funds with a higher weight of investments in less liquid assets experienced larger outflows during the initial phase of the COVID-19 pandemic.

Building on these prior studies, in this section we analyze the factors influencing fund inflows and outflows for foreign open-end funds investing in Japan by including the characteristics of each fund as explanatory variables in a panel regression model.[10] Specifically, the ratio of fund flows to total net assets (TNA) at time $t-1$ is defined as follows, and this ratio is used as the dependent variable in the model below. The regression is estimated for March 2020, when large fund outflows were observed, as well as for other periods.

$$flow\ \ rate_{i,t} \equiv \frac{flow_{i,t}}{TNA_{i,t-1}}. \tag{3}$$

$$\begin{aligned} flow\ \ rate_{i,t} =& TimeDummy_t + \alpha + \beta * TNA_{i,t-1} + \gamma * fund\ \ age_{i,t-1} \\ &+ \delta * fund\ return_{i,t-1} + \varepsilon * controls_{i,t-1} + \epsilon_{i,t}. \end{aligned} \tag{4}$$

Following the methodology used by Claessens and Lewrick (2021) and other studies on foreign funds, we include explanatory variables such as the fund's size (log value), years in operation (fund age), and fund return. For equity funds, we also include a "small and mid-cap dummy" for funds primarily investing in small and mid-cap stocks, as well as industry dummies. For bond funds, we include the "Non-IG ratio," which represents the proportion of assets with ratings below BBB. For real estate funds, we include a dummy variable for the fund's domicile (U.S. domicile dummy), among other characteristics. These variables have all been identified in prior research as factors related to fund outflows during times of crisis.[11]

The results of the panel regression are shown in Table 1. Looking at the results for equity funds, we observe that small and mid-cap focused funds, which tend to hold less liquid assets, experienced larger outflows during the initial phase of the COVID-19 pandemic. Additionally, while the fund size typically has a significantly negative effect under normal conditions, this pattern was not observed during the COVID-19 pandemic. It suggests that relatively small funds experienced greater capital outflows compared to normal periods.

10. The characteristics used as explanatory variables are lagged one-period relative to the dependent variable, which is the fund flow. In other words, the analysis observes how the characteristics of the fund from the previous month affect the fund flows of the current month.
11. The impact of the COVID-19 pandemic on business performance and stock prices is expected to vary significantly by industry. Therefore, for funds where investments predominantly focus on industries that appear to have benefited from the COVID-19 pandemic, such as Health Care, Consumer Staples, and Communication Services, industry dummy variables are included.

Table 1 Panel estimation results

Equity funds

		Dependent variable: flow rate		
		Mar. 20	Excluding Mar. 20	Mar. 20 ~ May 20
Explanatory variables	Cash holding ratio	0.011	0.044***	0.033***
	Total Net Assets	0.031	-0.013***	0.092***
	Total return	0.025***	0.045***	0.034***
	Fund age	-0.092***	-0.114***	-0.104***
	Small and mid -cap dummy	-0.340*	-0.188***	-0.564***
	Industry dummy	0.649	0.163***	2.117***
	Constant	0.062	1.986***	-0.043
Time fixed effects		No	Yes	Yes
Adj. R^2		0.008	0.034	0.019
Sample size		17,268	2,803,034	52,542

Bond funds

		Dependent variable: flow rate	
		Mar. 20	Other periods
Explanatory variables	Cash holding ratio	-0.059**	0.007***
	Non-IG ratio	-0.040***	-0.002***
	Total Net Assets	-0.421***	-0.049***
	Distribution yield	-0.187***	0.038***
	Fund age	0.024	-0.133***
	Constant	-1.086***	2.950***
Time fixed effects		No	Yes
Adj. R^2		0.023	0.034
Sample size		8,877	1,341,880

Real estate funds

		Dependent variable: flow rate		
		Mar. 20	Excluding Mar. 20	Mar. 20 ~ May 20
Explanatory variables	Cash holding ratio	-0.325***	-0.016***	-0.127***
	Total Net Assets	0.090	-0.065***	0.084*
	Total return	-0.008	0.031***	-0.016
	Fund age	-0.157***	-0.141***	-0.128***
	U.S. domicile dummy	-0.832*	0.031	-0.850***
	Constant	1.723***	23.738***	0.743*
Time fixed effects		No	Yes	Yes
Adj. R^2		0.054	0.044	0.020
Sample size		817	130,719	2,453

Note: The estimation period is from January 2007 to September 2024. ***, **, and * indicate statistical significance at the 1 percent, 5 percent, and 10 percent levels, respectively.
Source: LSEG Lipper.

Similarly for bond funds, the coefficient of the Non-IG ratio expanded significantly in absolute terms in March 2020, suggesting that funds with higher ratios of lower-rated assets (i.e., less liquid assets) experienced larger redemptions compared to normal times.

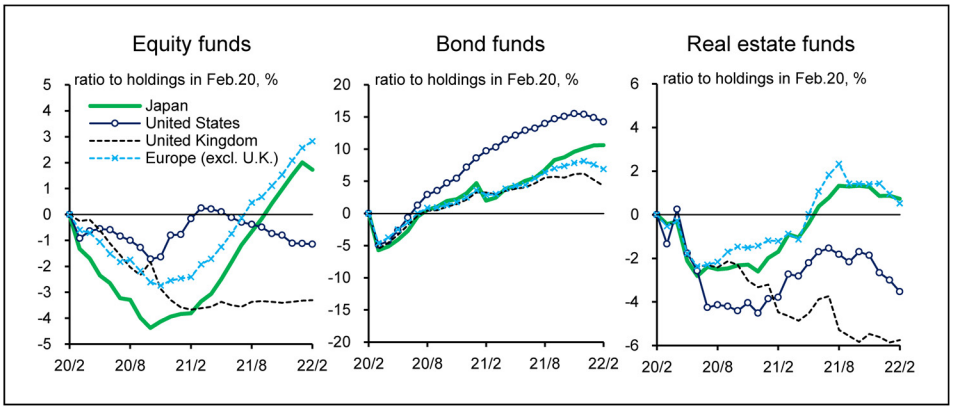
Furthermore, regarding real estate funds, the U.S. domicile dummy coefficient suggests that U.S.-domiciled funds had larger outflows immediately following the COVID-19 pandemic compared to funds domiciled in Europe or other regions. In this regard, ESMA (2020) shows that the outflows from real estate funds located in Europe were relatively limited. Hogen and Koide (2022) point to institutional factors such as lock-up periods following purchase and advance notice requirements for redemptions as potential reasons for this. Additionally, Grill, Vivar, and Wedow (2022) suggest that real estate funds in Europe implemented redemption suspensions to a significant extent, which may have helped to mitigate the outflows.

C. Impact of Global Financial and Economic Environment on Fund Flows

1. Impact of the global financial and economic environment

As previously mentioned, we documented that foreign open-end funds investing in Japan faced significant outflows during events such as the global financial crisis and the initial phase of the COVID-19 pandemic. This suggests that global investor sentiment influences the flows of open-end funds investing in Japan. Comparing fund flows into funds investing in Japan with those into funds investing in other jurisdictions, we find that the flows of both follow a generally similar trend, particularly for bond funds, where an outflow occurs immediately after the stress event, followed by a gradual shift towards inflows (Figure 5). Moreover, when comparing the flows into funds investing in Japan and those investing in the U.S., we observe a positive correlation for all asset

Figure 5 Comparison with fund flows investing in overseas jurisdictions



Note: Fund flows into funds investing in "Japan," "United States," "United Kingdom," and "Europe (excl. UK). " Cumulative change from March 2020. Weighted average based on asset holdings in each jurisdiction.

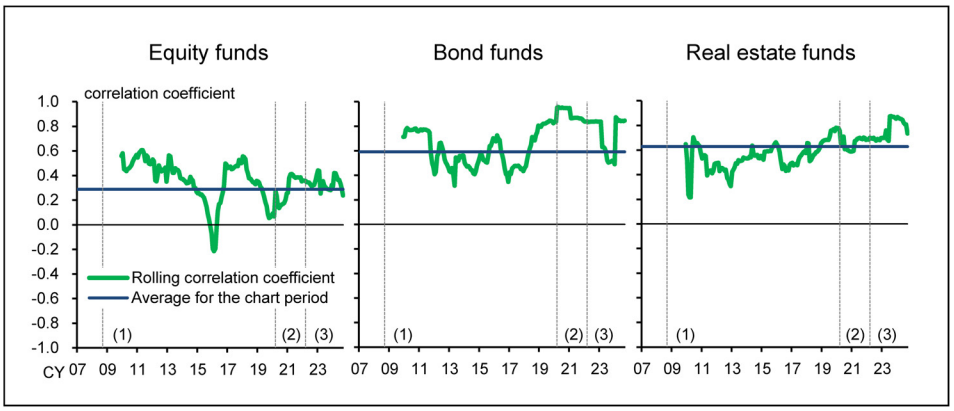
Source: LSEG Lipper.

types, with a particularly high correlation for bond and real estate funds (Figure 6).[12] Additionally, we find that a principal component analysis of the fund flows into foreign open-end funds investing in Japan, the U.S., the U.K., and Europe shows that, especially during shock events like the initial phase of the COVID-19 pandemic, a common global factor explains most of the fund flows into funds investing in Japan (Figure 7).[13]

This reflects the fact that foreign open-end funds investing in Japan are highly influenced by global investor sentiment. When examining the breakdown of funds investing in Japan by investment region, we find that very few funds focus exclusively on Japan. Instead, global funds that invest across multiple regions, including Japan, hold the largest share (Figure 8). This suggests that when global investor sentiment worsens, fund outflows may occur even in cases where the shock is not directly related to Japan, as global investors adjust their portfolios.

12. The strength of these correlations is influenced by global funds that invest in both the U.S. and Japan and account for a large share of the market. The flows from these funds are counted in both the funds investing in Japan and those investing in the U.S.
13. The number of common factors extracted was determined using the panel criteria of Bai and Ng (2002).

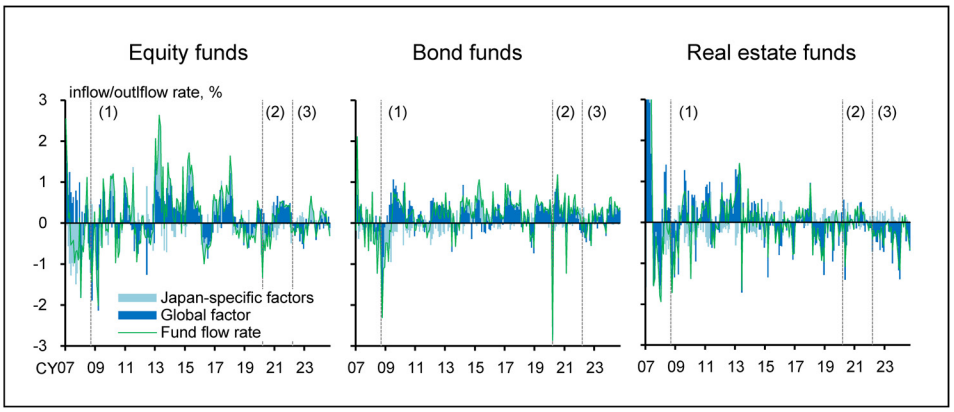
Figure 6 Correlation with fund flows into funds investing in the U.S.



Note: 1. The correlation between the fund flow rates of foreign funds investing in Japan and those investing in the US.
2. The estimation period is from January 2007 to September 2024. "Rolling correlation coefficient" represents the sequentially calculated monthly correlation coefficient, rolling over a 36-month window.
3. Points (1), (2), and (3) in the graph indicate the global financial crisis (September 2008), the COVID-19 Shock (March 2020), and the start of the US interest rate hike cycle (March 2022), respectively.

Source: LSEG Lipper.

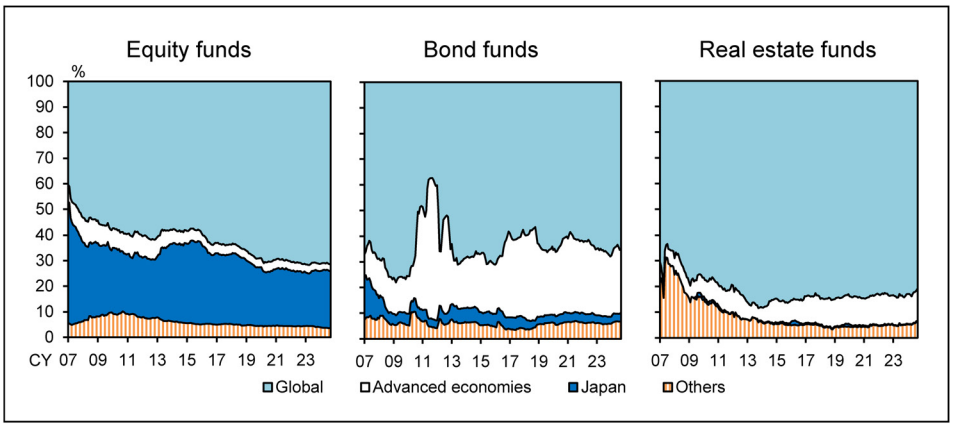
Figure 7 Contribution of global factor extracted through principal component analysis



Note: 1. Principal component analysis was performed on the fund flows of foreign funds investing in Japan, US, UK, and Europe (excluding UK). The first principal component is considered the global factor.
2. The vertical axis represents the flow rate of funds investing in Japan. Points (1), (2), and (3) in the graph indicate the global financial crisis (September 2008), the COVID-19 Shock (March 2020), and the start of the US interest rate hike cycle (March 2022), respectively.

Source: LSEG Lipper.

Figure 8 Investment regions of foreign open-end funds



Note: 1. Shows the composition of foreign open-end funds by main investment region (share in the total value of Japanese asset holdings).
2. "Global" and "Advanced economies" are on a reported basis. "Japan" refers to funds that invest 50% or more of their total net assets in Japan.

Source: LSEG Lipper.

2. Impact of the global financial and economic environment on fund flows

Next, building on the panel estimation from the previous section, we conduct a panel analysis incorporating macro-financial variables to estimate how the global financial and economic environment impacts the fund flows into open-end funds investing in Japan. Specifically, we incorporate U.S. interest rates, the National Financial Conditions Index (NFCI) provided by the Federal Reserve Bank of Chicago, and the U.S. dollar index (Advanced Foreign Economies (AFE) Dollar Index) as variables that are considered to have a significant impact on global investor behavior.

$$flow\ \ rate_{i,t} = \alpha + \beta * US\ \ interest\ \ rate_t + \gamma\ * NFCI_t + \delta * AFE\ \ dollar\ \ index_t + \varepsilon\ * controls_{i,t-1} + \epsilon_{i,t}. \quad (5)$$

The estimation results show that changes in external factors such as rising U.S. interest rates, a worsening NFCI, and a stronger U.S. dollar lead to outflows from foreign open-end funds investing in Japan (Table 2).[14] By decomposing the factors contributing to past fund flows, we find that the deterioration of the NFCI in March 2020 and the rise in U.S. interest rates since March 2022 were major contributors to outflows (Figure 9). This suggests that even in the absence of stress originating in the Japanese market, global shocks triggered by external factors can lead to portfolio adjustments by global investors, resulting in fund outflows from open-end funds investing in Japan.

14. In model 3 for bond funds, the interaction term between the Non-IG ratio and the NFCI is included in the estimation. This variable is significantly negative, suggesting that when the global financial environment deteriorates, funds investing in relatively illiquid assets experience non-linear increases in outflows.

Table 2　Panel estimation results with macroeconomic financial variables

Equity funds

		Dependent variable: flow rate		
		Model 1	Model 2	Model 3
Explanatory variables	Cash holding ratio	0.049***	0.052***	0.049***
	Total Net Assets	-0.001	0.003*	-0.001
	Total return	0.023***	0.024***	0.023***
	Fund age	-0.116***	-0.118***	-0.116***
	Small and mid-cap dummy	-0.167***	-0.159***	-0.167***
	U.S. federal funds rate (deviation from average)	-0.087***	—	—
	U.S. federal funds rate (deviation from the trend)	—	-0.077***	—
	U.S. federal funds rate (level)	—	—	-0.087***
	AFE dollar index	-0.028***	-0.018***	-0.028***
	NFCI	-0.449***	-0.531***	-0.449***
	Constant	1.155***	1.139***	1.275***
Adj. R^2		0.023	0.022	0.023
Sample size		2,820,302	2,820,302	2,820,302

Bond funds

		Dependent variable: flow rate		
		Model 1	Model 2	Model 3
Explanatory variables	Cash holding ratio	0.012***	0.010***	0.012***
	Non-IG ratio	-0.004***	-0.005***	-0.004***
	Total Net Assets	-0.021***	-0.033***	-0.021***
	Distribution yield	0.047***	0.064***	0.045***
	Fund age	-0.140***	-0.136***	-0.140***
	U.S. federal funds rate (month-to-month diff.)	-0.977***	—	-1.000***
	U.S. federal funds rate (deviation from average)	—	-0.140***	—
	AFE dollar index	-0.061***	-0.107***	-0.059***
	NFCI	-4.355***	-3.688***	-3.028***
	Non-IG ratio × NFCI	—	—	-0.065***
	Constant	1.930***	1.934***	1.936***
Adj. R^2		0.022	0.022	0.023
Sample size		1,350,757	1,350,757	1,350,757

Real estate funds

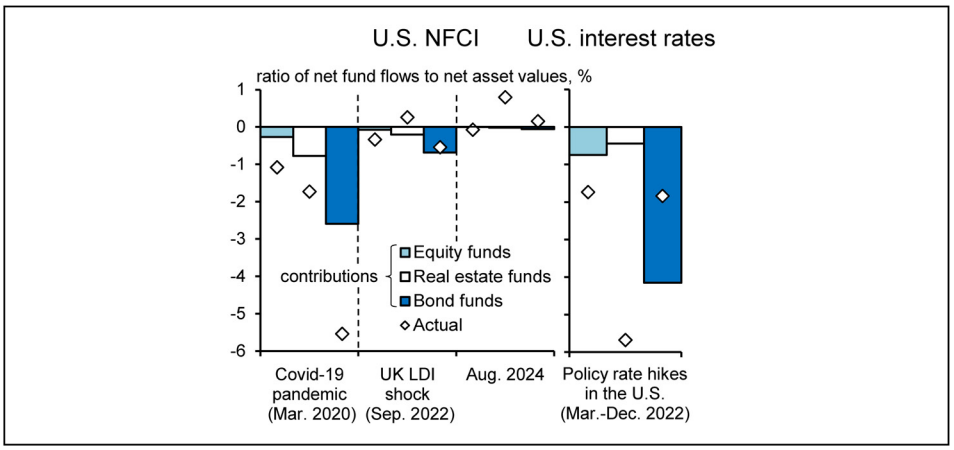
		Dependent variable: flow rate		
		Model 1	Model 2	model 3
Explanatory variables	Cash holding ratio	-0.004	-0.003	-0.004
	Total Net Assets	-0.039***	-0.034***	-0.039***
	Total return	0.031***	0.032***	0.031***
	Fund age	-0.156***	-0.159***	-0.155***
	U.S. domicile dummy	0.125***	0.140***	0.124***
	U.S. federal funds rate (deviation from average)	-0.051***	—	-0.053***
	U.S. federal funds rate (deviation from the trend)	—	-0.008	—
	AFE dollar index	0.039**	0.045***	0.036**
	VIX	—	—	-0.005***
	NFCI	-1.301***	-1.359***	-0.743***
	Constant	1.268***	1.263***	1.280***
Adj. R^2		0.020	0.020	0.020
Sample size		131,536	131,536	131,536

Note: 1. Covers foreign funds investing in Japan. Total net assets (TNA) is logarithmic value. The Dollar Index is measured as the monthly change (nominal value), and both NFCI and VIX are measured as month-to-month changes. The explanatory variables, excluding macroeconomic variables, are lagged by one period.

2. The estimation period is from January 2007 to September 2024. ***, **, and * indicate statistical significance at the 1 percent, 5 percent, and 10 percent levels, respectively.

Source: Federal Reserve Bank of Chicago; Haver Analytics; LSEG Lipper.

Figure 9 Impact of deterioration in foreign financial conditions on net fund flows to open-end funds investing in Japan



Note: 1. The contribution of each variable to the change in net fund flows from the month preceding each event is calculated based on a panel regression using net fund flows as the dependent variable and fund attributes (return, size, and liquidity ratio) and macroeconomic indicators (U.S. short-term interest rates, U.S. NFCI, and U.S. dollar index) as the independent variables. The estimation period is from January 2007 to September 2024.

2. The left chart shows the flow rates (equity, real estate, and bond funds) and the estimated contributions of NFCI during each crisis period (March 2020, September 2022, and August 2024). Flow rates are measured as the difference from the value in the month prior to each crisis.
3. The right chart shows the fund flow rates (equity, real estate, and bond funds) from March to December 2022 and the contributions of U.S. interest rates (cumulative over the period) derived from the panel estimation.
4. Figures for net asset values are for the month preceding each event. The right-hand chart shows the cumulative values during the period.

Source: Federal Reserve Bank of Chicago; Haver Analytics; LSEG Lipper.

III. Trading Activity of Foreign Open-End Funds in Japanese Assets

A. Estimation of Asset Sales and Purchases by Foreign Open-End Funds

When funds flow into and out of foreign open-end funds, the funds buy and sell assets. However, the extent to which funds sell assets in proportion to their holdings, or prioritize certain assets, does not necessarily correspond directly to the inflows or outflows from investors. Therefore, this section analyzes the trading activities of foreign open-end funds in Japanese assets.

In the analysis, we first estimate the trading volumes of Japanese assets by each fund. As mentioned in the previous section, the changes in each fund's asset holdings include both the effect of price changes in the assets and the impact from buying and selling. By decomposing the fund's total net assets (TNA_t) into price (P_t) and quantity (Q_t), and considering the investment ratio in Japanese assets (denoted $JP\ \ ratio_t$), the change in holdings of Japanese assets ($\Delta JP\ \ asset\ \ holdings_t$) from period $t-1$ to period

t can be expressed as follows:

$$\begin{aligned}\Delta JP\ \ asset\ \ holdings_t &= TNA_t * JP\ \ ratio_t - TNA_{t-1} * JP\ \ ratio_{t-1} \\ &= P_t * Q_t * JP\ \ ratio_t - P_{t-1} * Q_{t-1} * JP\ \ ratio_{t-1} \\ &= P_{t-1} * (Q_t * JP\ \ ratio_t - Q_{t-1} * JP\ \ ratio_{t-1}) \\ &\quad + (P_t - P_{t-1}) * Q_t * JP\ \ ratio_t,\end{aligned} \tag{6}$$

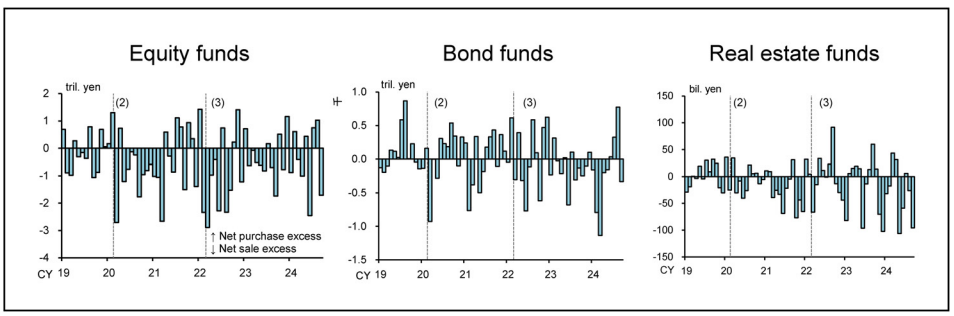
where the first term on the right-hand side represents the change in holdings of Japanese assets excluding the impact of price changes, and the second term reflects the effect of price fluctuations. We extract the first term on the right-hand side as the amount of trading in Japanese assets ($JP\ \ asset\ \ trading_t$), as shown below:

$$\begin{aligned}JP\ \ asset\ \ trading_t &= P_{t-1} * Q_t * JP\ \ ratio_t - P_{t-1} * Q_{t-1} * JP\ \ ratio_{t-1} \\ &= \frac{TNA_t}{\Delta P_t} * JP\ \ ratio_t - TNA_{t-1} * JP\ \ ratio_{t-1},\end{aligned} \tag{7}$$

where $\Delta P_t = P_t / P_{t-1}$ is the price change from period t–1 to period t, and the values used for this calculation are taken from the previous section, which calculated the fund flows. For equity funds, where the price fluctuations can vary significantly across countries, we use the price change of funds with a Japan investment ratio exceeding 80% as a proxy variable.

When we examine the trading activity of foreign funds investing in Japanese financial assets by asset type using the equation above, we find that during times of large fund outflows globally, the funds also sold assets in Japan (Figure 10). Sales of Japanese assets were also large in the initial phase of the COVID-19 pandemic. This was especially true especially for bond funds, which saw the largest fund outflows. When comparing this trading behavior with the spot trading behavior of foreign investors in each market, we find that they generally move in the same direction during times of market shock, suggesting that asset sales by foreign open-end funds influence these movements (Figure 11).

Figure 10 Foreign fund transactions in Japanese assets

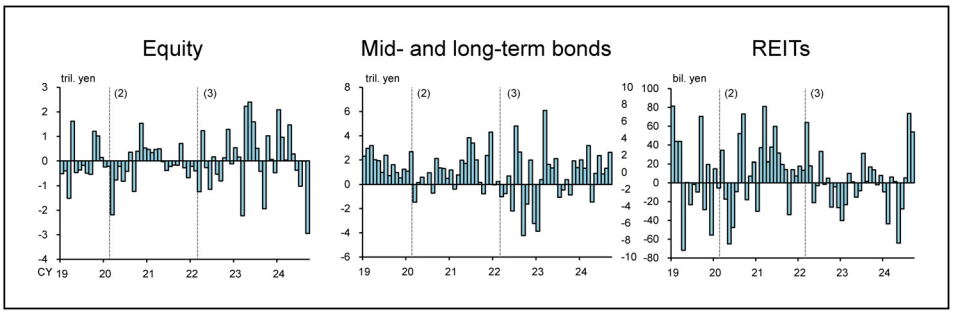


Note: Covers foreign funds investing in Japan. Points (2) and (3) in the graph indicate the COVID-19 Shock (March 2020), and the start of the US interest rate hike cycle (March 2022), respectively. Latest data as of September 2024.

Source: LSEG Lipper.

When examining the investment ratio by country, categorized by asset type, we observe that for equity and real estate funds, the investment ratio in the U.S. has increased, while the investment ratios in Europe and Japan have declined. These trends did not change before and after the COVID-19 pandemic (Figure 12). In the case of real estate

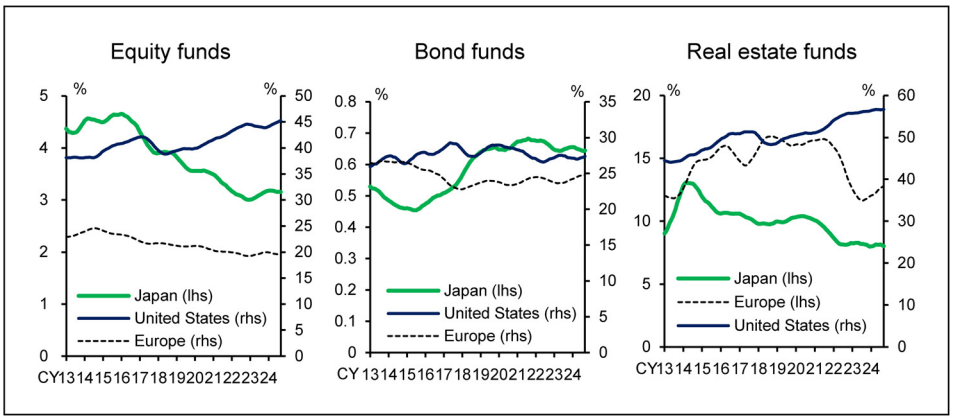
Figure 11 Foreign investor spot market transactions by market



Note: 1. The left chart shows the net trading volume in the Tokyo Stock Exchange Prime Market (the Tokyo Stock Exchange First Section before March 2022).
2. The middle chart shows the net trading volume of coupon-bearing medium- and long-term government bonds.
3. The right chart shows the net trading volume of Real Estate Investment Trusts (REITs) listed on the Tokyo Stock Exchange.
4. Points (2) and (3) correspond to the COVID-19 shock (March 2020) and the beginning of the US interest rate hike cycle (March 2022), respectively. Latest data as of September 2024.

Source: Japan Securities Dealers Association; Tokyo Stock Exchange.

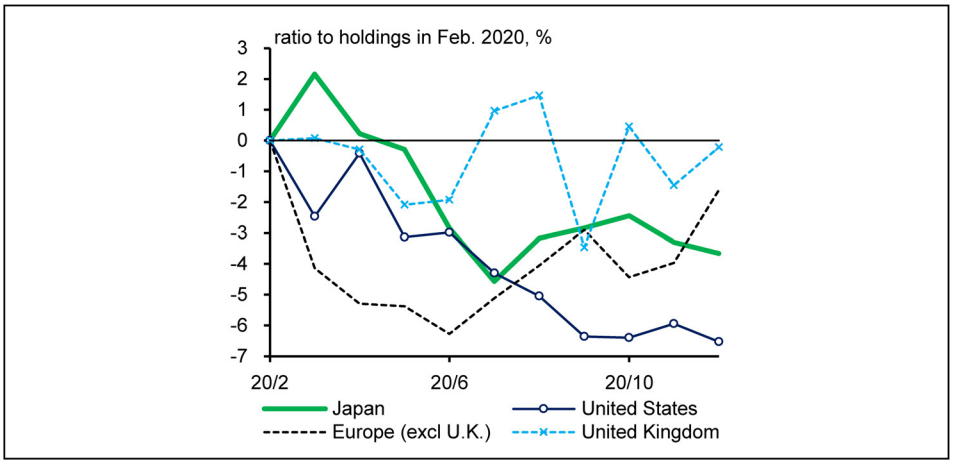
Figure 12 Country-specific investment ratios by asset type



Note: 1. Shows median values. Europe is the combined value of the United Kingdom and Europe (excluding UK).
2. For funds where country-specific investment ratios are unavailable, it is assumed that the entire net asset value is invested in the "focus region" of each fund (the region they primarily invest in). For example, if the investment ratio for Japan is unavailable for funds A and B, and their focus regions are Japan and the US, it is assumed that Fund A invests 100% in Japan (i.e., Japan investment ratio = 100%) and Fund B invests 0% in Japan (i.e., Japan investment ratio = 0%). Covers foreign funds investing in Japan.

Source: LSEG Lipper.

Figure 13 Real estate funds' asset trading by jurisdiction



Note: The cumulative value of asset trading in each country since March 2020, divided by the asset holdings in each country as of February 2020. Latest data as of December 2020.
Source: LSEG Lipper.

funds, particularly during the initial phase of the COVID-19 pandemic, while the sales of European assets were significant, the sales of Japanese assets were limited. This may reflect differences in the REIT market conditions across countries (Figure 13).

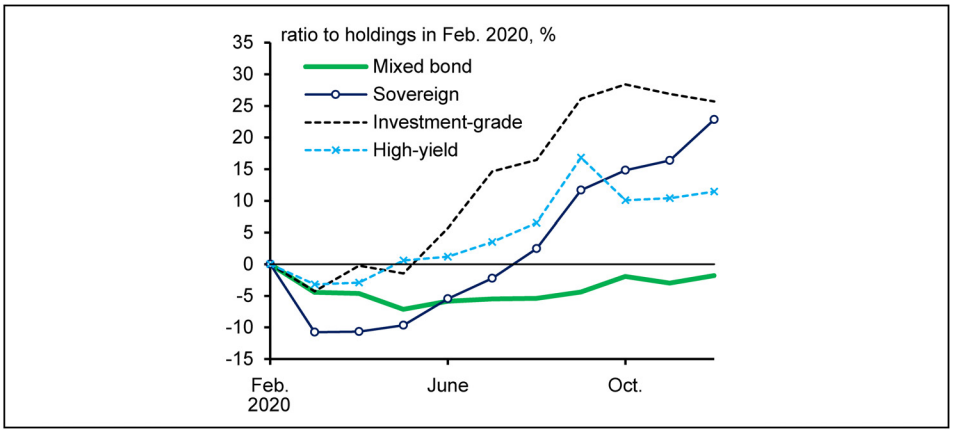
B. Breakdown of Asset Sales in Bond Funds

In this section, we analyze the asset trading behavior of bond funds, which saw significant Japanese asset sales during the initial phase of the COVID-19 pandemic. First, by examining the asset sales by type of bond fund, we find that particularly funds investing in government bonds and various other bonds, such as mixed bond funds, sold Japanese assets (Figure 14).[15]

For mixed bond funds, an examination of asset sales among the top holders of Japanese assets reveals that, during this period, government bonds accounted for the majority of the asset sales (Figure 15). This suggests that these funds may have sold highly liquid assets to secure liquidity in response to redemption requests from investors. This finding is consistent with prior research on similar trends in other regions. Ma, Xiao, and Zeng (2022) analyze the trading behavior of U.S. bond funds during the COVID-19 pandemic and conclude that highly liquid assets were sold. Claessens and Lewrick (2021) similarly point out that bond funds, including those outside of the U.S., may have engaged in horizontal slicing, selling highly liquid assets during the COVID-19 pandemic.[16]

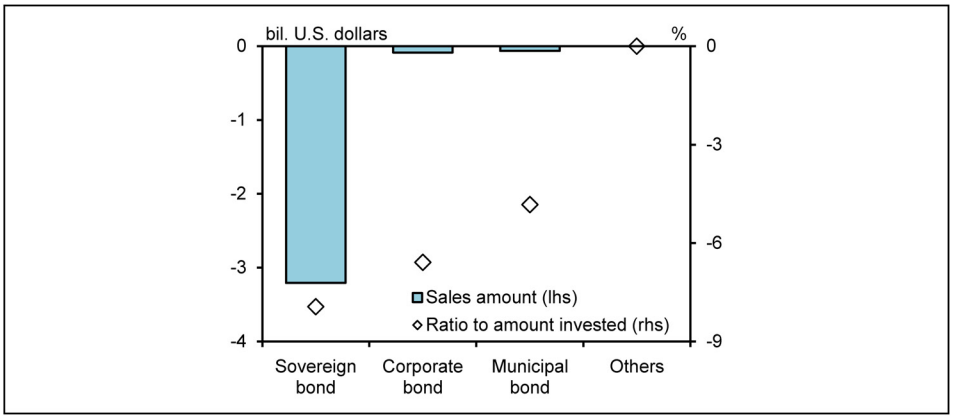
15. Here, bond funds are categorized by the type of bonds they invest in. "Government bond funds" focus on government bonds, "IG bond funds" invest in investment-grade corporate bonds, "HY bond funds" target high-yield bonds, and "mixed bond funds" invest in a combination of these bonds.
16. There are two liquidity management methods for open-end funds in response to redemption requests: horizontal slicing and vertical slicing. The former involves selling the most liquid assets first, while the latter involves selling assets in a way that does not alter the asset composition. Dekker, Vivar, and Weistroffer (2024) note that open-end funds located in Europe held a significant amount of ETFs, which, due to their intraday liquidity, were sold to meet redemption requests during the COVID-19 pandemic.

Figure 14 Foreign bond funds' Japanese asset trading



Note: The cumulative value of asset trading in Japan since March 2020, divided by Japanese asset holdings in February 2020. Latest data as of December 2020.
Source: LSEG Lipper.

Figure 15 Foreign mixed bond funds' Japanese asset trading

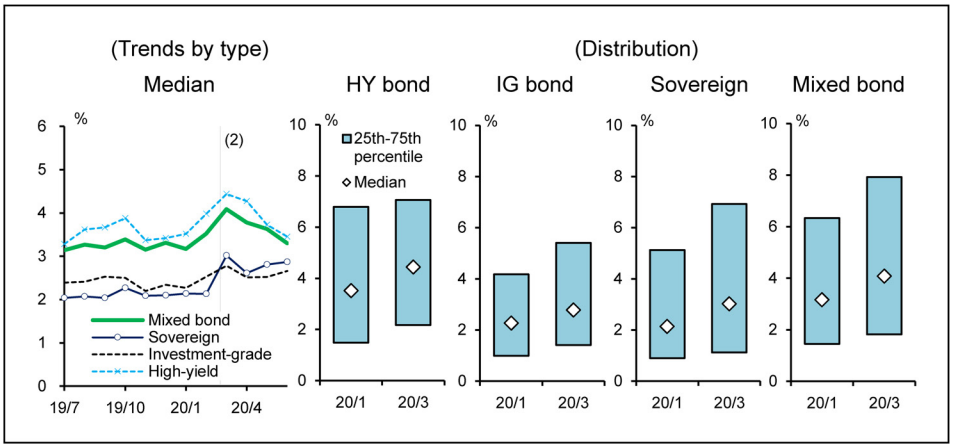


Note: Aggregate figures for the top 10 foreign mixed bond funds investing in Japan (covering approximately 50% of total Japanese asset holdings). For holdings as of the end of February 2020, the asset value as of the end of March 2020 with fixed prices was calculated, and the difference was treated as the amount of trading.
Source: LSEG Lipper.

Additionally, when comparing the cash holding ratio of bond funds before and after the COVID-19 pandemic, we find that, particularly among high-yield bond funds, cash holdings increased significantly from January to March 2020 across all types of bond funds (Figure 16).[17] Similar trends have been suggested in analyses focused on Europe. ECB (2022) indicates that bond funds investing in low-liquidity assets, in particular, increased their cash holdings during the COVID-19 pandemic, resulting in asset sales that exceeded the redemption requests. This suggests that in response to redemption

17. A t-test based on the change in the cash holding ratio from January to March for each fund verifies that the increase in the cash holding ratio from January to March 2020 was significant.

Figure 16 Cash holding ratio of bond funds before and after the COVID-19 pandemic



Note: Covers foreign bond funds investing in Japan. In the left chart, point (2) represents the COVID-19 shock (March 2020). All values are month-end figures. Latest data for the left chart is the end of June 2020.

Source: LSEG Lipper.

requests, assets sales, including those with precautionary motives, may have amplified the impact on financial markets.

IV. The Impact of Foreign Open-End Funds on Japan's Financial Markets

In this section, we estimate the "macro multipliers" in Japan's stock and REIT markets. These multipliers help quantify the impact of asset trading by foreign open-end funds. The term "macro multipliers" refers to the price change resulting from a one-unit increase in asset demand (i.e., the slope of the demand curve).[18,19] In other words, it is the reciprocal of the change in demand for the asset when its price changes by one unit.

A. Estimation of "Macro Multipliers" for Stock and REIT Markets

1. Overview of estimation method

We employ the estimation method proposed by Gabaix and Koijen (2023) (hereafter, GK2023) to estimate macro multipliers. GK2023 argue that the stock market multiplier suggested by traditional financial theory (the Modigliani–Miller theorem), which assumes frictionless financial markets, is smaller than those found in existing empirical studies, such as Hartzmark and Solomon (2021) and Li and Lin (2022). They

18. We discuss the demand and supply curves with quantity on the horizontal axis and price on the vertical axis in the analyses of this section. An inelastic market (i.e., one in which the quantity change is small relative to the price change) corresponds to a steep demand curve and implies a larger macro multiplier. GK2023 show that the stock market's macro multiplier is approximately between 0.05 and 0.1 according to traditional financial theory. In contrast, several empirical studies typically find the range to be between 1 and 5.
19. When measuring price sensitivity in transactions, liquidity measures, such as the one in Amihud (2002), are often used (we use this measure in Appendix 2). These indicators reflect concepts such as market depth and elasticity.

also present estimation results using the Granular Instrumental Variable (GIV) method developed by Gabaix and Koijen (2024) and propose a theoretical model that is consistent with those results. GIV uses idiosyncratic shocks to micro-level agents (such as individual sectors or companies), which are less correlated with macro variables, as instrumental variables. It helps address endogeneity issues in the price-quantity relationship that standard regression analysis might encounter.[20] We estimate the macro multipliers for Japan's stock and REIT markets using the method outlined in GK2023.

In the main text, we mainly show the key idea of GIV, a brief description of the construction of GIV, and estimation results. We leave a more detailed steps to obtain GIV from the datasets in Appendix 1.

2. Empirical environment

Consider an economy with investor sectors $i = 1, \ldots, N$. Let Δq_{it} denote the growth rate of equity holdings of sector i, and Δp_t the aggregate market return. Sectoral demand satisfies:

$$-\Delta q_{it} = -\zeta \Delta p_t + \xi_{it}, \tag{8}$$

where ζ is the aggregate demand elasticity and ξ_{it} is an idiosyncratic demand shifter. Under the market-clearing condition $\sum_i \Delta q_{it} = 0$, aggregate price movements satisfy:

$$\Delta p_t = M \xi_t^S, \ \ and \ \ M \equiv \frac{1}{\zeta}, \tag{9}$$

where ξ_t^S denotes the size-weighted aggregate demand shock. The object of interest is the aggregate market multiplier M, which measures the price response to a unit aggregate demand shock. A direct regression of prices on quantities is biased due to simultaneity: both are jointly determined in equilibrium and driven by common macroeconomic factors. Therefore, an instrument is required to obtain an unbiased estimator of M.

3. Intuition behind the GIV estimator

Decompose the demand shifter as:

$$\xi_{it} = \beta_i' \eta_t + u_{it}, \tag{10}$$

where η_t are common factors and u_{it} are idiosyncratic shocks satisfying:

$$\mathbb{E}\left[u_{it}\eta_t\right] = 0, \quad \mathbb{E}\left[u_{it}u_{jt}\right] = 0, \quad \forall i \neq j. \tag{11}$$

20. Generally, the price of a good is expected to decrease as its quantity increases in order to clear the market, depending on the shape of the demand curve. However, when prices fall, suppliers observing the price decrease may reduce the supply of the good, indicating a causal relationship from price to quantity. Therefore, simply regressing price on quantity introduces endogeneity, which biases the estimation of the macro multiplier. In this context, if we can extract quantity fluctuations that are independent of price changes, the price fluctuations corresponding to these quantity changes can help address the endogeneity issue. GK2023 assume that sector-specific demand shocks are uncorrelated with macroeconomic or supply-side shocks, weights them by sector size, and then constructs the GIV.

Under market clearing,

$$\Delta p_t = M\beta_S^{'}\eta_t + Mu_t^S, \quad where \;\; u_t^S = \sum_i S_{it-1}u_{it}. \tag{12}$$

If sectors were infinitesimal, u_t^S would vanish by the law of large numbers. However, because sector sizes ($S_{i,t-1}$) are concentrated, large-sector shocks do not diversify away. These granular shocks generate exogenous aggregate demand shifts and therefore move prices.

After removing observable and latent common factors from sectoral quantity changes, the residuals u_{it} capture idiosyncratic demand shocks that are orthogonal to aggregate macroeconomic news. The granular instrument is constructed as their size-weighted aggregation,

$$z_t = \sum_i S_{it-1}u_{it}. \tag{13}$$

Because sector sizes are concentrated, this weighted sum does not average out and therefore represents the aggregate impact of large investors' idiosyncratic portfolio shocks.

Substituting this object into the equilibrium pricing equation implies:

$$\Delta p_t = Mz_t + e_t, \, \mathbb{E}\left[e_t z_t\right] = 0. \tag{14}$$

This orthogonality condition constitutes the key identifying moment. Although the true aggregate idiosyncratic demand shock is unobservable, the constructed instrument z_t consistently recovers it under the maintained assumptions. Identification of the aggregate multiplier follows from the fact that granular shocks shift aggregate demand while remaining orthogonal to macroeconomic fundamentals that directly affect prices.[21]

4. Economic intuition

Identification rests on three distinct economic mechanisms. The first mechanism concerns finite market depth. When aggregate demand is inelastic, that is, when ζ is small, equilibrium requires a comparatively large price adjustment to clear the market. In such an environment, the aggregate multiplier $M = 1/\zeta$ is necessarily large, reflecting a strong price response to demand disturbances. The second mechanism is granularity. The cross-sectional distribution of sector sizes is highly concentrated, so that shocks to large investors do not average out in the aggregate. Idiosyncratic portfolio reallocations of sufficiently large sectors therefore generate economically meaningful shifts in aggregate demand and induce equilibrium price movements. The third mechanism is orthogonality. After removing observable and latent common factors, the remaining sector-level residuals are orthogonal to macroeconomic news that directly affects prices. These residual shocks thus provide exogenous variation in aggregate demand. Taken together, these mechanisms imply that identification arises from the interaction

21. While GK2023 use the cross-sectionally demeaned value of a vector u_{it}, we skip these steps for the sake of simplicity.

Table 3 Data used for estimation

	Stock Market	REIT Market
Price	TOPIX (Tokyo Stock Price Index)	Tokyo Stock Exchange REIT Index
Trade flows	Bank of Japan "Flow of Funds"	Tokyo Stock Exchange "Trading by Type of Investors"
Transaction volume (stock)	Bank of Japan "Flow of Funds"	Tokyo Stock Exchange "REIT Investor Survey"
Period	Apr.-Jun. 1998 to Jul.-Sep. 2024	Sep. 2014 to Aug. 2024
Frequency	Quarterly	Monthly[22]
Investment sectors	Depository corporations Securities investment trusts Insurance and pension funds Other financial intermediaries Financial auxiliaries Public captive financial institutions Nonfinancial corporations General government Households Private nonprofit institutions serving households Overseas Central bank	Individuals Foreigners Securities corporations Investment trusts Business corporations Life and non-life insurance cos. Banks Other financial institutions

between cross-sectional heterogeneity in demand shocks and dispersion in sector size. Granular shocks from large sectors propagate to the aggregate level and, under orthogonality, isolate the structural price elasticity.

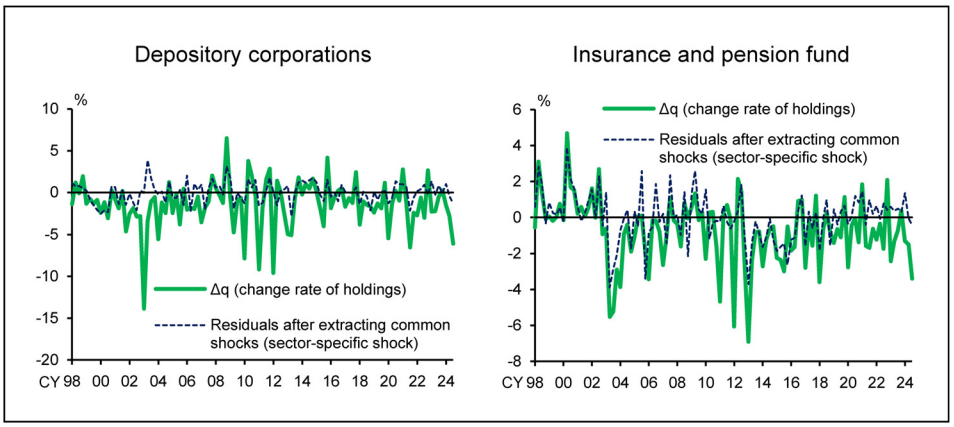
5. Data used for estimation

We summarize the data used for estimation in Table 3. We source data on trade flows and transaction volume (stock) for the stock market from the Bank of Japan's "Flow of Funds" following GK2023. For the REIT market, we source trade flow data from the Tokyo Stock Exchange's "Trading by Type of Investors" and transaction volume (stock) from the "REIT Investor Survey." The data frequency is quarterly for the stock market and monthly for the REIT market.

6. Constructing the GIV

We extract idiosyncratic shocks by dividing each market into approximately 10 sectors. The number of sectors is almost the same as that in GK2023. In addition, we assume that investment behavior varies across sub-sectors within the financial sector. Therefore, we further divide the financial sector into more detailed sub-sectors, such as depository corporations, insurance and pension funds, and other financial interme-

Figure 17 Sector-specific shocks (in equity market)



Note: We include an observable macroeconomic variable as a common factor to extract the sector-specific shocks in Step 2.
Source: BOJ.

diaries.

When extracting macro factors from the net trading flows, we use the exchange rate (USD/JPY) for the stock market and the VIX for the REIT market as the common macroeconomic variables, which are observable to all investors (Step 2 in Appendix 1). This is in contrast to GK2023, who use the GDP growth rate as the observable common factor for the U.S. stock market multiplier. We choose to use the change in the USD/JPY exchange rate instead because it has greater explanatory power for Δq_{it}.[22]

Figure 17 shows the idiosyncratic sector-specific shocks ($\breve{u}_{it}$ in Step 3 in Appendix 1). We exclude common shocks by omitting variation from the macro component and principal component analysis. We show sector-specific shocks, along with the original series (Δq_{it}) for depository corporations and insurance and pension funds. In both cases, we observe that the range of fluctuations is generally smaller. Lastly, we regress GIV, which represents the weighted sector-specific shocks, on price fluctuations (Step 4 in Appendix 1).

B. Estimation Results

This section reports estimates of the aggregate market multiplier M obtained using the GIV estimator. We summarize the estimation results in Table 4. The baseline specification includes observable macro controls and two latent principal components extracted from sectoral quantity data. Across specifications, the estimated multiplier is approximately $M \approx 3$ for the stock market and $M \approx 5$ for the REIT market. Again, $M \approx 3$ implies that purchasing 1% of the market results in a 3% increase in the aggregate price level. Furthermore, this implies that the aggregate demand elasticity, $1/M$, is around 0.3 for the stock market and 0.2 for the REIT market, indicating substantial price sensitivity to aggregate demand shocks and therefore limited market depth. This suggests

22. It should be noted that these results may vary depending on the choice of investment sectors, observable common macroeconomic variables, the number of factors in the principal component analysis (non-observable common macroeconomic variables), and other factors.

Table 4 Estimation results

	Stock market			REIT market		
	incl. macroeconomic variable		excl. macro val.	incl. macroeconomic variable		excl. macro val.
M	3.46 **	3.43 *	2.87	5.20 ***	4.26 **	4.79 ***
	(1.63)	(2.05)	(1.75)	(1.79)	(1.75)	(1.81)
Macroeconomic variables	0.78 ***	0.83 ***		-0.22 ***	-0.17 *	
	(0.15)	(0.18)		(0.05)	(0.09)	
Principal component 1	2.71 ***	3.21 ***	2.55 ***	0.46	0.42	0.26
	(0.75)	(0.89)	(0.81)	(0.53)	(0.56)	(0.53)
Principal component 2	-4.17 ***	-2.10 ***	-2.11 ***	-2.81 ***	-2.67 ***	-3.20 ***
	(0.61)	(0.70)	(0.66)	(0.55)	(0.63)	(0.53)
# of data	106	87	106	120	64	120
Frequency	Quarterly	Quarterly	Quarterly	Monthly	Monthly	Monthly
Period	1998Q2-2024Q3	1998Q2-2019Q4	1998Q2-2024Q3	2014M9-2024M8	2014M9-2019M12	2014M9-2024M8

Note: 1. We use the month-on-month rate of change in USD/JPY for the stock market and the month-on-month differential in VIX for the REIT market as observable macroeconomic variables, respectively.

2. The values in parentheses are standard errors. ***, **, and * indicate statistical significance at the 1 percent, 5 percent, and 10 percent levels, respectively.

Source: Bloomberg; FRED; Tokyo Stock Exchange; BOJ.

that prices are sensitive to the volume of assets supplied to the market. The multipliers for the stock market are similar to those reported in GK2023, indicating that the demand curve for Japan's stock market is as steep as that of the U.S.[23]

The estimated multiplier remains stable across alternative specifications. We estimate the multipliers for the period excluding the COVID-19 pandemic, as in GK2023, as well as for the entire sample period, and find that the two sets of estimates are similar.[24]

Additionally, we compare the estimated macro multipliers with liquidity indicators based on the measure proposed by Amihud (2002) in Appendix 2. We find that the estimates obtained using GIV are similar to the liquidity indicators during periods of heightened uncertainty, such as the volatility episode in the Chinese stock market in 2015 and the COVID-19 pandemic. These results suggest that, particularly during episodes of increased uncertainty—for example, when redemption requests for open-end funds trigger asset sales—financial market prices may fluctuate substantially.

Overall, the empirical evidence indicates that aggregate stock and REIT demand is inelastic and that granular sectoral shocks constitute a quantitatively important source of price fluctuations.

23. GK2023 estimates the macro multiplier for the U.S. stock market to generally range from 4 to 6. Furthermore, Aliyev *et al*. (2025) show that liquidity levels in the U.S. and Japanese markets have been roughly similar since the global financial crisis.

24. In the literature, methods such as Bai and Ng (2002) are often used to determine the number of principal components. However, GK2023 determines the number based on the cumulative contribution of the principal components to explaining the observed variables and on how the estimation results change as the number of principal components increases. We employ the same approach and set the number of principal components to two. We also verify that the cumulative contribution of principal components for Japan's stock market is higher than that for the U.S. stock market, and we reproduce the U.S. results using the method in GK2023. For more details, see Gabaix and Koijen (2024).

V. Conclusion

This paper has examined the presence of foreign open-end funds in Japan's financial markets and assessed their potential impact through two complementary lenses: (i) the dynamics of fund flows and trading behavior, and (ii) the price sensitivity of Japanese asset markets to net trading pressure.

We use high-granularity data of foreign open-end funds to analyze trends in fund flows from investors and the buying and selling behavior of equity, bond, and real estate funds investing in Japan. Additionally, we examine the impact of these transactions on asset prices in Japan's financial markets. First, when examining the flows into and out of foreign open-end funds investing in Japan, we find that capital outflows tend to occur when financial conditions abroad deteriorate and U.S. interest rates rise. In response to these outflows, foreign open-end funds sell their holdings of securities, including Japanese assets. Notably, during the volatile initial phase of the COVID-19 pandemic in March 2020, there were sales of Japanese assets across asset classes. We find that government bonds accounted for the majority of the securities sold by bond funds, which experienced significant outflows during this period. This implies that bond funds sell highly liquid assets in response to redemption requests from investors.

Next, we examine the impact of asset sales on asset prices by estimating price sensitivity (or "macro multipliers") for the domestic equity and REIT markets. The estimated sensitivity values obtained are similar to those from GK2023, who estimated the macro multiplier for the U.S. stock market. This suggests that, like the U.S., the Japanese equity market is inelastic. Based on our results, we conclude that the trading behavior of foreign open-end funds, which have expanded their presence in Japan's financial markets, could lead to significant price fluctuations in the Japanese market when risk events originating abroad occur.

Several important questions remain open and warrant further investigation. For example, a more granular identification of causal price impact would strengthen the interpretation of our estimates. While our approach follows established methodologies, distinguishing exogenous demand shocks from endogenous responses to price changes remains challenging. Future research could exploit high-frequency data, or instrument-based strategies to better isolate exogenous flow-driven variation. Second, heterogeneity across funds within each sector could be explored. Given the restriction of data availability, we estimate "macro multipliers," these sensitivities could differ across funds. While our dataset does not contain investor composition, incorporating such information could refine our understanding of redemption dynamics.

References

Aliyev, N., M. Aquilina, K. Rzayev, and S. Zhu. "Through Stormy Seas: How Fragile Is Liquidity across Asset Classes?" BIS Working Papers No 1229. November 2024 (revised May 2025).

Allaire, N., J. Breckenfelder, and M. Hoerova. "Fund Fragility: the Role of Investor Base." ECB Working Paper Series No.2874. 2023.

Amihud, Y. "Illiquidity and Stock Returns: Cross-Section and Time-Series Effects." *Journal of Financial Markets* 5, no. 1 (2002): 31–56.

Bai, J., and S. Ng. "Determining the Number of Factors in Approximate Factor Models." *Econometrica* 70, no. 1 (2002): 191–221.

Bank of Japan. "Financial System Report (October 2024)." October 2024.

———. "Financial System Report (April 2025)." April 2025.

Claessens, S., and U. Lewrick. "Open-Ended Bond Funds: Systemic Risks and Policy Implications." *BIS Quarterly Review*, December 2021.

Coval, J., and E. Stafford. "Asset Fire Sales (and Purchases) in Equity Markets." *Journal of Financial Economics* 86, no. 2 (2007): 479–512.

Dekker, L., L. M. Vivar, M. Wedow, and C. Weistroffer. "Liquidity Buffers and Open-End Investment Funds: Containing Outflows or Reducing Fire Sales?" *Journal of International Financial Markets, Institutions and Money* 91 (2024): 101909.

———, ———, and C. Weistroffer. "Passing on the Hot Potato: The Use of ETFs by Open-Ended Funds to Manage Redemption Requests." ECB Working Paper Series No. 2963. 2024.

Eguchi, M., T. Okubo, K. Yamamoto, and K. Washimi. "Changing Landscape of NBFIs in Financial Systems —A Comparative Analysis of Japan, the U.S., and Germany—," Bank of Japan Review Series 2025-E-7. 2025.

European Central Bank. "Financial Stability Review." November 2022.

European Securities and Markets Authority. "Recommendation of the European Systemic Risk Board (ESRB) on Liquidity Risk in Investment Funds." November 2020, ESMA34-39-1119.

Falato, A., I. Goldstein, and A. Hortacsu. "Financial Fragility in the COVID-19 Crisis: The Case of Investment Funds in Corporate Bond Markets." *Journal of Monetary Economics* 123 (2021): 35–52.

Financial Services Agency. "Fund Monitoring Survey (1st) Summary of Results." 2025.

Financial Stability Board. "Holistic Review of the March Market Turmoil." November 2020.

———. "Assessment of the Effectiveness of the FSB's 2017 Recommendations on Liquidity Mismatch in Open-Ended Funds." December 2022.

———. "Revised Policy Recommendations to Address Structural Vulnerabilities from Liquidity Mismatch in Open-Ended Funds." December 2023.

———. "Enhancing the Resilience of Non-Bank Financial Intermediation: Progress Report." July 2024a.

———. "Global Monitoring Report on Non-Bank Financial Intermediation 2024." December 2024b.

Gabaix, X., and R. S. J. Koijen. "In Search of the Origins of Financial Fluctuations: The Inelastic Markets Hypothesis (December 23, 2023)." 2023. Available at SSRN: https://ssrn.com/abstract=3686935.

———, and ———. "Granular Instrumental Variables." *Journal of Political Economy* 132, no. 7 (2024): 2274–2303.

Grill, M., L. M. Vivar, and M. Wedow. "Mutual Fund Suspensions during the Covid-19 Market Turmoil-Asset Liquidity, Liquidity Management Tools and Spillover Effects." *Finance Research Letters* 50 (2022): 103249.

Hartzmark, S. M., and D. H. Solomon. "Marketwide Predictable Price Pressure." 2021. Available at SSRN: https://ssrn.com/abstract=3853096.

Hogen, Y., Y. Kasai, and Y. Shinozaki. "Rise of NBFIs and the Global Structural Change in the Transmission of Market Shocks." *Journal of Financial Stability* 79, (2025): 101419.

———, and Y. Koide. "Flows of Overseas Funds in the Real Estate Market." Bank of Japan Review Series 2022-E-7. 2022.

International Monetary Fund. "Global Financial Stability Report." October 2022.

———. "Global Financial Stability Report." October 2024.

International Organization of Securities Commissions. "Anti-dilution Liquidity Management Tools-Guidance for Effective Implementation of the Recommendations for Liquidity Risk Management for Collective Investment Schemes." FR15/2023, 2023.

Jiang, H., Y. Li, Z. Sun, and A. Wang. "Does Mutual Fund Illiquidity Introduce Fragility into Asset Prices? Evidence from the Corporate Bond Market," *Journal of Financial Economics* 143, no. 1 (2022): 277–302.

Kankawa, S. "Genbutsu shijō ni okeru kaigai tōshika no tōshikōdō (Investment Behavior of Foreign Investors in the Cash Government Bond Market)." Bank of Japan Working Paper Series No.20-J-4. 2020 (in Japanese).

Kawasumi, Y. and M. Kataoka. "Beikoku tanki kinyū shijō no fuanteika to gulōbalu na hakyū-Shingata corona uirusu kansensyō no kakudai to kinyū shijō (2) (Instability in the U.S. Short-Term Financial Market and Its Global Spillover: The Spread of COVID-19 and the Financial Market (2))." Bank of Japan Review Series 2020-J-10. 2020 (in Japanese).

Koide, Y., Y. Hogen, and N. Sudo. "Increasing Portfolio Overlap of Japanese Regional Banks with Global Investment Funds and Its Financial Stability Implications." Bank of Japan Working Paper Series No.22-E-15. 2022.

Li, J., and Z. Lin. "Price Multipliers are Larger at More Aggregate Levels." 2022. Available at SSRN: https://ssrn.com/abstract=4038664.

Ma, Y., K. Xiao, and Y. Zeng. "Mutual Fund Liquidity Transformation and Reverse Flight to Liquidity." *The Review of Financial Studies* 35, no.10 (2022): 4674–4711.

Oishi, H., E. Kobayashi, and Y. Sugihara. "Recent Developments in Non-Bank Financial Intermediation and Initiatives to Enhance Its Resilience." Bank of Japan Review Series 2025-E-6. 2025.

Okamoto, T. "Beikoku tanki kokusai shijō no fuanteika to wagakuni kokusai shijō heno eikyō-Shingata corona uirusu kansensyō no kakudai to kinyū shijō (1) (Instability in the U.S. Treasury Market and Its Impact on the Japanese Government Bond Market: The Spread of COVID-19 and the Financial Market (1))." Bank of Japan Review Series 2020-J-9. 2020 (in Japanese).

APPENDIX 1: ESTIMATION PROCEDURE WITH GIV

We follow the estimation procedure outlined in Section IV.A of GK2023. The procedure is as follows: Δq_{it} represents the rate of change in investor i 's holdings (Q_{it}) from time $t-1$ to time t, Δp_t represents the rate of change in the asset price from time $t-1$ to time t, and S_{it} denotes the share of the market held by investor i at time t. η_t represents the macroeconomic factor common to all investors, where η_t^o is observable and η_t^l is unobservable. We assume that Δq_{it} is the sum of the part driven by common factors and the idiosyncratic fluctuations specific to investor i.

Step 1: Calculate the precision weights E_i for Step 2.

$$E_i = \frac{\overline{\sigma}_{\Delta q,i}^{-2}}{\sum_j \overline{\sigma}_{\Delta q,j}^{-2}}. \tag{A-1}$$

where $\sigma_{\Delta q,i}$ refers to the standard deviation of Δq_{it} and

$$\overline{\sigma}_{\Delta q,i} = \max\left\{\sigma_{\Delta q,i}, \text{median}\left(\sigma_{\Delta q,i}\right)\right\}, \text{respectively.} \tag{A-2}$$

Step 2: Estimate the following panel regression and obtain the residuals $\Delta\breve{q}_{it}$ using E_i calculated in Step 1 as regression weights.

$$\Delta q_{it} = \alpha_i + \beta_t + \gamma_i^{'}\eta_t^o + \Delta\breve{q}_{it}. \tag{A-3}$$

Step 3: Extract the principal components η_t^l of $E_i^{0.5}\Delta\breve{q}_{it}$, and estimate the residuals $\breve{u}_{it}$ by regressing $\Delta\breve{q}_{it}$, calculated in Step 2, on η_t^l.

$$\Delta\breve{q}_{it} = \breve{\lambda}_i^{'}\eta_t^l + \breve{u}_{it}. \tag{A-4}$$

Step 4: Estimate the multiplier M using the GIV z_t,[25] which is $\breve{u}_{it}$ weighted by the market share $S_{i,t-1}$.

$$z_t = \sum_{i=1}^{N} S_{i,t-1}\breve{u}_{it}, \Delta p_t = Mz_t + \lambda'\eta_t + e_t. \tag{A-5}$$

We estimate the macro multiplier M following this procedure. [26]

25. We use robust linear regression to account for outliers when estimating the multipliers.
26. We omit Step 5 (recalculating the precision weights E_i using $\overline{\sigma}_{\breve{u},i}$ based on the residuals $\breve{u}_{it}$ obtained in Step 3, and then repeating Step 2 to Step 4) in the estimation procedures outlined in GK2023 for simplicity. However, including Step 5 when estimating the multiplier for the stock market does not significantly affect the results.

APPENDIX 2: COMPARISON OF MACRO MULTIPLIERS AND LIQUIDITY INDICATORS

In the main text, we estimate the macro multipliers using GIV (hereinafter referred to as "Estimation 1"). In this appendix, we estimate liquidity indicators using the method of Amihud (2002) (hereinafter referred to as "Estimation 2") and compare the results of the two estimations. [27,28]

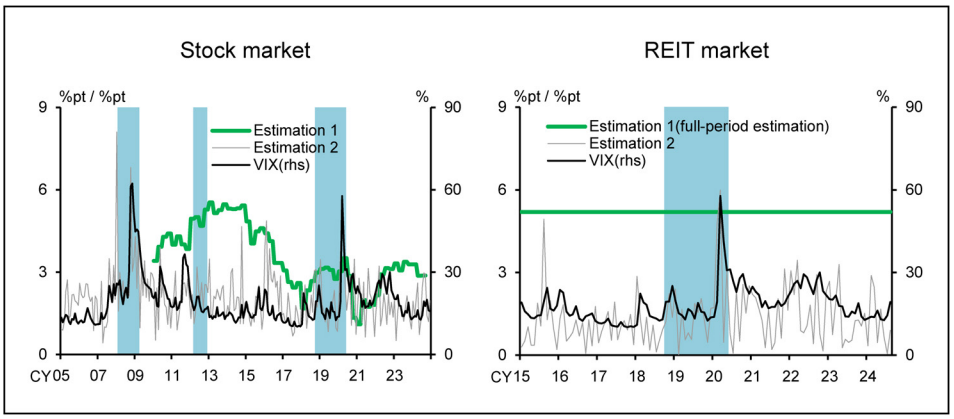
Figure A-1 shows the time-series results of Estimation 2 alongside those of Estimation 1. For Estimation 1, we perform rolling estimations when regressing the price (Δp_t) on GIV (z_t), as outlined in Step 4, to capture the time-series changes in the equity market.[29] First, we find that the macro multiplier is positive, even when examining the time-series fluctuations from the rolling estimation of Estimation 1. In other words, a decrease in the volume of assets pushes prices down.

Additionally, in Estimation 2, we find that the estimated multipliers increase during periods of turmoil, such as the volatility in the Chinese stock market in 2015 and the COVID-19 pandemic. We can also observe this characteristic in Estimation 1 using rolling estimations, though it is less prominent. This may reflect the fact that, during periods of heightened uncertainty, market liquidity decreases, which leads to an increase in the rate of price change in response to trade flows. In such situations where liquidity is reduced, several factors may explain the observed dynamics, including increased selling pressure in the market by open-end funds, which are susceptible to liquidity constraints, as they respond to redemption requests from investors. Additionally, investors and brokers may also become risk-averse and reduce trading. (Coval and Stafford 2007).

For both estimation methods caution is required in interpreting the results due to differences in data frequency and model specification. However, the estimation results suggest that, when open-end funds sell securities in response to redemption requests, prices may fluctuate significantly, particularly during periods of heightened uncertainty.

27. Amihud (2002) calculated an illiquidity indicator for U.S. stock prices based on daily returns and trading volume. It is common to increase the data frequency (i.e., shorten the trading window) to address potential endogeneity in similar analyses. However, we calculate the liquidity indicator using price changes rather than returns. Due to data limitations, we may not have fully addressed the endogeneity concerns.
28. We generally use the same dataset for estimating the liquidity indicator in "Estimation 2," based on the method outlined in Amihud (2002), as we use in "Estimation 1." However, while "Estimation 1" uses the net trading volume for each investment sector, "Estimation 2" uses the gross trading volume instead.
29. We set the rolling period so that the estimates are generally significant at the 10 percent level. Additionally, for the REIT market, we use the entire period's data for estimation due to insufficient sample size.

Figure A-1 Comparison of the two estimation results



Note: 1. We include observable macroeconomic variables as common factors to extract the sector-specific shocks in Estimation 1.
2. Figures in Estimation 1 for the stock market are estimated using a 48-period window.
3. The shadow periods correspond to the periods from February 2008 to March 2009, from March 2012 to November 2012, and from October 2018 to May 2020, respectively.

Source: Bloomberg; FRED; Tokyo Stock Exchange; Cabinet Office; BOJ.

A Technical Examination of Non-Ledger-Based Payment Systems

by Yuko Tamura, Masayuki Abe, Tetsuya Okuda, Hiromasa Tsugawa, Toshiyuki Miyazawa, Kazuki Yamamura, Yoshiharu Akahane, Tomoki Taguchi, Yuto Hirakuri, Hiroto Masuda and Kento Yamada

This paper explores a payment system that enables transactions without relying on a ledger or intermediary service providers, examining it from a technical perspective. The system facilitates payments through the transmission and receipt of electronic data, analogous to physical cash. In the field of cryptography, this concept has been studied under the name "electronic cash." While several demonstration experiments were conducted in the 1990s, it is presumed that the technology at the time could not ensure sufficient usability. In this paper, we revisit the concept of electronic cash in light of technological advancements and evolving societal needs. Additionally, we conduct practical verification using smartphones to demonstrate that current technological standards can offer electronic cash systems with high usability. From a technical standpoint, we propose methods to further enhance usability and privacy for electronic cash schemes. These include mechanisms for splitting and aggregating electronic cash into arbitrary amounts, as well as schemes that make it difficult to link electronic cash transactions made by the same user. It should be noted that this paper focuses solely on the technical aspects of electronic cash and does not examine the feasibility of its legal, institutional, or practical implementation in society.

Keywords: digital payments; electronic cash; electronic money; privacy protection; smartphone payments
JEL Classification: L86, L96

Yuko Tamura: Institute for Monetary and Economic Studies, Bank of Japan
(E-mail: yuuko.tamura@boj.or.jp)
Masayuki Abe, Tetsuya Okuda, Hiromasa Tsugawa, Toshiyuki Miyazawa, Kazuki Yamamura: NTT Social Informatics Laboratories (E-mail: msyk.abe@ntt.com)
(Miyazawa is currently in NTT Service Innovation Laboratory Group)
Yoshiharu Akahane, Tomoki Taguchi, Yuto Hirakuri, Hiroto Masuda, Kento Yamada: Third Financial Sector, NTT DATA Corporation
(E-mail: yoshiharu.akahane@nttdata.com)

The authors would like to thank Professor Atsushi Fujioka (Kanagawa University) and Professor Noboru Kunihiro (University of Tsukuba). The views expressed in this paper are those of the authors and do not necessarily reflect the official views of the Bank of Japan, NTT Corporation, and NTT DATA Corporation.

DO NOT REPRINT OR REPRODUCE WITHOUT PERMISSION

I. Introduction

Most of the cashless payment systems currently in widespread use adopt a "ledger-based" approach. Here, a ledger refers to a database that records transaction details based on instructions from users, consolidating and managing all transactions and balances for all users. A typical example is deposit transactions, and it appears that recently popularized QR code-based payments also use this approach. Cryptographic assets,[1] although differing in the entity and method of ledger management, can also be cited as an example of a ledger-based system. In these ledger-based systems, users issue payment instructions to service providers (or blockchain nodes in the case of cryptographic assets) via the Internet, and the service providers execute the payment by updating the ledger.

In contrast, "electronic cash"[2] (Okamoto and Ohta 1993, Nakayama *et al*. 1997) enables payments without relying on a ledger, representing a significant departure from existing cashless payment systems. Electronic cash facilitates payments through the transmission of electronic data that functions as physical cash. Payments can be made via data communication between the sender and recipient, resembling the exchange of physical cash. This approach, therefore, potentially offers advantages over ledger-based systems in terms of server fault tolerance, network failure resilience, transaction processing performance, and interoperability with external systems. Furthermore, as the payment process is confined to the two parties involved, transaction details can be kept confidential from service providers. Additionally, when using short-range communication between devices, payments can be made in environments disconnected from the Internet.

The feasibility of electronic cash has been examined in several pilot experiments.[3] For instance, the "Internet Cash" experiment conducted in 1998 tested a system where Internet Cash (electronic cash) issued online was stored on IC cards and could be sent to online stores or friends. However, ensuring sufficient usability[4] with the technology available at the time proved difficult, and electronic cash did not gain traction. Subsequently, the spread of contactless IC-card-based electronic money led to a temporary halt in the study of electronic cash.

Recently, the promotion of cashless payments by the government has led to a year-on-year increase in the use of various cashless payment services, including electronic money. In 2023, the cashless payment ratio in Japan rose to approximately 40% (Ministry of Economy, Trade and Industry 2024). The government has set a final target

1. Before the amendment of the Payment Services Act that came into effect in May 2020, this was called "virtual currency."
2. Nakayama *et al*. (1997) referred to the proposed payment method as "electronic money." In recent years, contactless IC cards are often referred to as "electronic money." Therefore, this paper uses the term "electronic cash," which Okamoto and Ohta (1993) used. The "electronic cash" discussed in this paper is different from the Central Bank Digital Currency (CBDC) being studied by the government and the Bank of Japan.
3. Demonstration experiments based on the electronic cash system include experiments conducted in December 1995 (NTT Corporation 1995), September 1996 (NTT Corporation 1996), September 1998 to February 2000 (Cyber Business Council 2000), and April 1999 to May 2000 (NTT Communications Corporation 2000).
4. Usability refers to the ease of use for users. It is similar to "convenience," and in this paper, it refers to one of the properties required of electronic cash system (safety, convenience, inheritance of benefits of physical cash, and transparency) defined in Section II.B.

of 80% for the cashless payment ratio (Consumption and Distribution Policy Division, Commerce and Service Industry Policy Group, Ministry of Economy, Trade and Industry (METI) 2018), suggesting that the use of cashless payment services will continue to grow. This anticipated growth underscores the importance of considering the potential impact of server failures and network disruptions on domestic payment services. In this context, exploring non-ledger-based payment systems could contribute to achieving a stable cashless society.

Against this backdrop, this paper first revisits the concept of electronic cash in light of recent technological advancements and societal needs. It then reports on practical verification using commonly available smartphones to evaluate usability under current technological standards. Furthermore, the paper explores methods to enhance the usability of electronic cash schemes and proposes approaches to strengthen user privacy. It is important to note that this study focuses solely on the technical aspects of electronic cash and does not address legal, institutional, or operational feasibility for societal implementation.

The structure of this paper is as follows: Section II organizes the basic framework of electronic cash systems and the properties required of electronic cash, while discussing the balance between privacy protection and transparency. Section III reviews the results of practical tests on the transmission and receipt of electronic cash items and evaluates its usability under current technological standards. Section IV explores efficiency improvements in electronic cash systems, including methods to optimize transmission, receipt, and redemption, as well as approaches to enable the splitting and aggregation of electronic cash items and enhance privacy. Finally, Section V concludes with future prospects and closes the paper.

II. Basic Framework of the Electronic Cash System

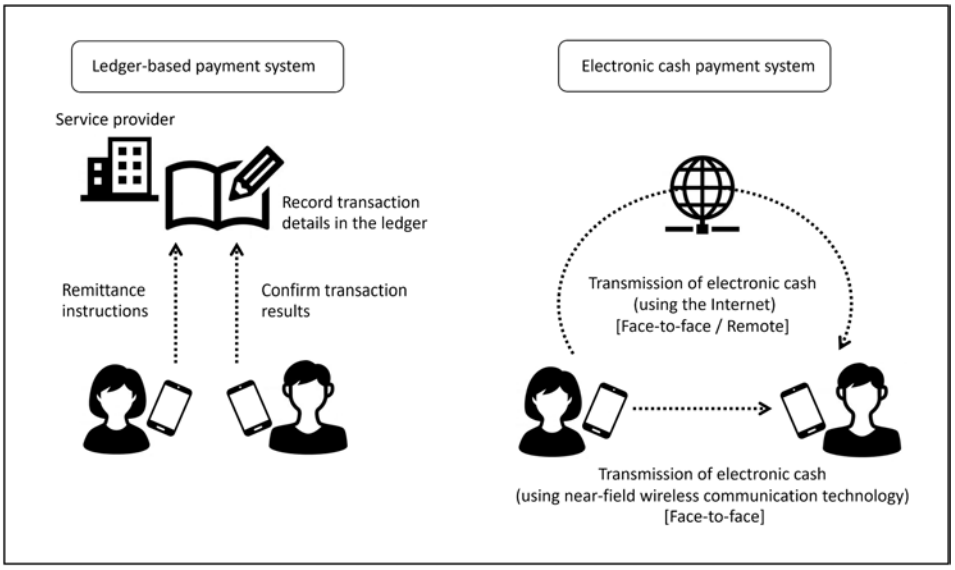
A. Differences between the Ledger-Based System and the Electronic Cash System

Most payment services currently available use a ledger-based system, where a service provider intermediates the transactions. The service provider records the transaction details in the ledger after receiving a remittance instruction from the user. For example, in the case of deposit transactions, financial institutions execute the transfer by deducting from the sender's account balance and adding to the receiving user's account balance as recorded in the ledger (refer to Figure 1).

On the other hand, methods allowing payment without a ledger have also been considered in the past (Okamoto and Ohta 1993, Nakayama *et al.* 1997). These aim to enable payment by transmitting electronic data directly from the sender to the recipient, similar to physical cash, and are referred to as "electronic cash." Electronic cash items are stored on user devices such as smartphones,[5] and the transfer can occur via the

5. Although this paper assumes a smartphone as the device used by the user, the electronic cash system can be implemented on a computer equipped with a tamper-resistant device similar to embedded Secure Element (eSE). SE is a module that is highly secure against external attacks and is implemented by combining hardware and software. The type built into the smartphone is called eSE. Tamper resistance refers to resistance to unauthorized reading and alteration of internal information. The necessity of tamper resistance is summarized in Subsection D.

Figure 1 Comparison of ledger-based payment system and electronic cash payment system



Internet or through proximity-based wireless communication technologies in face-to-face scenarios (refer to Figure 1).

Electronic cash system, therefore, enables payments without involving a service provider. While the provider's involvement is necessary for user registration and issuance of electronic cash items, the transmission process can be confined to data communication between the sender and the recipient. Consequently, electronic cash system offers the following advantages: resilience to server disruptions (less affected by server outages); resilience to network disruptions (possibility of making payments without Internet access); high processing efficiency (dependent on the device's processing power rather than the provider's servers or network bandwidth); and privacy of transaction details from the provider (the provider does not have real-time visibility into transactions).

Additionally, the electronic cash system can easily integrate multiple services. For instance, combining electronic cash items issued by different providers or exchanging different electronic cash types requires the providers to connect their ledgers via Application Programming Interfaces (APIs) in a ledger-based system. However, in an electronic cash system, the absence of ledgers eliminates the need for such inter-provider API connections. Users can simply install the necessary applications on their devices to facilitate service integration.

In addition, taking advantage of the feature that allows the modification of service formats through applications on the user side without requiring system updates on the service provider's side, it is possible to introduce programmability[6] to electronic cash. Here, "programmability" refers to the ability for entities other than the service provider

6. Programmability in payment systems means that various entities, not only operators of payment systems, can program settlement functions according to their individual needs (Hojo and Hatogai 2022).

to apply unique rules for using electronic cash. Users within the applicable scope can program these unique rules into their devices to execute them individually. Furthermore, by embedding usage rules for electronic cash items at the time of issuance, the service provider may provide programmable money.[7] For example, rules such as imposing expiration dates on electronic cash items or restricting the scope of its usage could be implemented.

On the other hand, one concern regarding the electronic cash system is the implications of storing electronic cash items solely on the user's device. In ledger-based systems, all asset data are managed by the service provider. Therefore, even if a user loses their device, as long as their identity can be verified, access to their data could theoretically be restored. In contrast, with the electronic cash system, since the electronic cash items are stored within the user's device, losing the device means losing the electronic cash items as well.[8] This characteristic is similar to physical cash. Additionally, attention must be paid to the requirement that user devices possess a certain level of tamper resistance[9] (see Subsection D).

This paper assumes that the medium for storing electronic cash items is a user-owned device, such as a smartphone. However, in the future, it may become possible to store electronic cash items in secure areas outside of the device. For example, in discussions surrounding the advancement of networks for the sixth-generation mobile communication system (6G),[10] there is consideration of equipping mobile networks with advanced encryption and secure computation functions to robustly protect user information. The Trusted Execution Environment (TEE)[11] is also included in this scope (as reported by NTT Network Service Systems Laboratories 2023). When such advancements in network security are realized, it may be possible to address the risk of device loss by storing the device owner's electronic cash items within the TEE environment at the edge of the network (e.g., base stations that serve as mobile network entry points) linked to the user's device.

7. Programmable money is a concept that focuses on controlling individual behavior by storing attribute information and programs specific to "objects" called fund data (Hojo and Hatogai 2022). Since electronic cash is issued as a digital signature of the service provider to the serial number (refer to BOX 1 of Subsection C), it is possible to write rules on the use of electronic cash in the message part of the signature.
8. The service provider may back up all electronic cash items in preparation for the loss of the device, but in that case, it will be necessary to send and maintain backup data, so it will have the same risk of failure as the ledger-based systems.
9. Specifically, this is achieved by protecting data by leaving traces of intrusion or erasing data against unauthorized access. Specific functions include tamper evidence, which provides evidence of unauthorized access; tamper resistance, which protects data from unauthorized access; and tamper response, which erases data against unauthorized access (Tamura and Une 2007).
10. With the advancement of mobile communication systems that support mobile devices, discussions are underway to deploy not only data transfer but also various information processing functions at the edge (base stations, etc.), which is the entry point to mobile networks. Devices will distribute functionality to the edge and access services over the Internet via mobile networks.
11. TEE is a function that provides an execution environment for processing that requires high security. This execution environment (TEE space) is separated from the space where normal applications run (Rich Execution Environment (REE)), and communication between the two spaces is designed to be executed under strict access control.

B. Properties Required of the Electronic Cash System

Nakayama *et al*. (1997) outlined the desired properties of electronic cash: safety, convenience, and the preservation of the inherent advantages of physical cash. From the need to consider measures for anti-money laundering and countering the financing of terrorism (AML/CFT) in providing payment systems, this paper adds transaction transparency as another essential property of electronic cash.

Safety

(1) Electronic cash should be resistant to forgery, tampering, duplication, and double spending.
Like physical cash, electronic cash must be secure against forgery and tampering. Additionally, due to the replicable nature of electronic data, it must be difficult to duplicate or use twice. From the viewpoint of safety, possible fraudulent actions for electronic cash are as follows.
- Forgery and tampering: Unauthorized creation or modification of electronic cash items
- Duplication usage: Unauthorized copying and usage of another person's electronic cash items
- Double spending: Duplicating and reusing one's electronic cash items

The electronic cash system prevents forgery and tampering through cryptographic techniques like digital signatures. Adding owner-specific information to electronic cash items can prevent unauthorized duplication by a third party. To address double spending, which is harder for payment service providers to detect in real time without a ledger, tamper-resistant devices are employed (see Subsection D). Additionally, even in cases where the tamper resistance is compromised, the service provider manages the situation by tracking serial numbers, enabling retrospective detection.[12]

Convenience

(2) Electronic cash items should allow usage in arbitrary denominations.
(3) It should support both face-to-face and remote payments.
(4) The issuance and management costs of electronic cash items should be low.

Convenience refers to the degree by which electronic cash is easier to use than physical cash for both users and service providers. Users particularly value the ability to divide electronic cash items into arbitrary denominations and the flexibility to use them in both face-to-face and remote payment scenarios (properties (2) and (3)). For providers, lower issuance and management costs than physical cash (property (4)) are a key benefit.

In the basic scheme introduced in Subsection C and the verification experiments in Section III, the unit of electronic cash items is fixed, leaving property (2) for future exploration. A method enabling the division and aggregation of electronic cash items is discussed in Section IV.C.

12. In the electronic cash system, a database (DB) of serial numbers is required for the retrospective detection of duplication and double spending, but it is different from a ledger for recording settlements.

Preservation of advantages of physical cash[13]

(5) Difficult to identify past users of electronic cash items (anonymity).[14]
(6) Difficult to link different transactions of the same user (unlinkability).
(7) Capable of offline payments in network-disconnected environments.
(8) Electronic cash items received can be reused for other payments.
(9) Devices required for electronic payments should be portable.

Anonymity, a key feature of physical cash, ensures that recipients cannot deduce past transaction information, even if collusion occurs between merchants and/or financial institutions (Furuichi 1995). Similarly, electronic cash scheme should protect user privacy, making it difficult to identify past users (property (5)). Additionally, unlinkability is crucial in situations where large amounts of data can be collected and analyzed, ensuring that even with access to multiple electronic cash items' records, it is impossible to correlate them to deduce user activity (property (6)).

Most existing cashless payment methods rely on Internet connectivity. However, offline functionality is essential for scenarios like natural disasters (property (7)), Nakata 2021). Other usability requirements include the ability to reuse received electronic cash items without returning it to service providers (transferability)[15] and the portability of the payment device to enable settlement anytime and anywhere (properties (8) and (9)).

Transparency

(10) Service providers must be able to trace electronic cash items when necessary.

For AML/CFT purposes, payment transparency is essential, enabling the tracing of funds as necessary. This requires service providers to verify users' identity information (name, address, etc.) and ensure its accuracy.

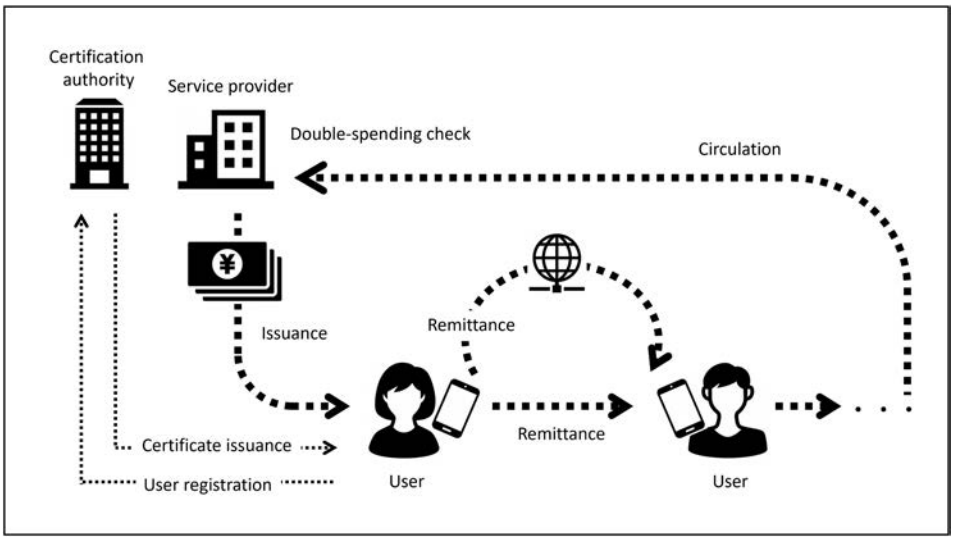
However, excessive user data management could allow providers to identify users based on usage history of redeemed electronic cash items. To balance privacy and transparency, an independent certification authority should handle user authentication.[16] Privacy protection and transparency are further addressed in Subsection E.

C. Basic Scheme

This section introduces the electronic cash system designed to have the aforementioned properties (Nakayama *et al*. 1997). The primary entities that make up the electronic

13. Nakayama *et al*. (1997) also identified the property of supporting multiple financial institutions in addition to properties (5) and (6). Nakayama *et al*. (1997) assumed that electronic cash would be issued against deposits and could be converted back into deposits, suggesting that the ability to deposit it with financial institutions other than the issuing institution would be a desirable feature. However, this paper assumes that electronic cash is issued by payment service providers and does not make the involvement of financial institutions a requirement; therefore, the property of supporting multiple financial institutions is not included.
14. Nakayama *et al*. (1997) described this as "untraceability" of the user.
15. A method with this property is called an open-loop type, while a method that does not is called a closed-loop type.
16. From the viewpoint of protecting the privacy of users, as in Nakayama *et al* (1997), it was determined to establish an independent organization to manage user information. However, since this paper does not consider the current legal system, it is necessary to examine the relationship with the legal system separately.

Figure 2 Basic framework of the electronic cash scheme



cash system are the service provider, the certification authority,[17] users (including both senders and receivers of electronic cash items, such as stores), and the users' devices (devices used for sending, receiving, and storing electronic cash items). From here, we describe electronic cash items as electronic cash for brevity. The basic scheme of the electronic cash system consists of the following phases: user registration and certificate issuance,[18] electronic cash issuance, electronic cash transmission, electronic cash redemption, and double-spending verification[19] (refer to Figure 2). The specific flow is described below. For details on cryptographic processing methods, refer to BOX 1.

1. User registration and certificate issuance

When using electronic cash, users generate the key pair necessary for cryptographic processing[20] and obtain a certificate from the certification authority.

(1) The user submits their personal information (e.g., name, address) required for certificate issuance to the certification authority.
(2) The certification authority verifies the user's identity and registers the user's information.

.....

17. A certification authority verifies the user's identity and issues a certificate for the user's public key. It is possible that multiple service providers may work with a single certification authority.
18. A certificate issued by a certification authority is used by a third party to verify that the key pair used for cryptographic processing is the correct one registered with the certification authority.
19. For crypto assets that do not have a specific administrator, there are generally no procedures such as user registration or certificate issuance. Therefore, the user of the crypto asset is not identified, and the key cannot be invalidated even if the key is stolen. However, when using a crypto asset exchange service provider for crypto asset transactions, identity verification by a crypto asset exchange service provider, etc. is required, and since all crypto assets are managed in a ledger, there is no redemption process.
20. A key pair called a private key and a public key is used for cryptographic processing. The private key must be managed as information known only to the user, while the public key is information that can be disclosed to other users. In the digital signature method, processing using a public key enables confirming that the message to be signed was created by the owner of the private key and that it has not been subsequently tampered.

(3) The user generates a key pair consisting of a private key and a public key and sends the public key to the certification authority.
(4) The certification authority associates the public key with the user's information and issues a certificate for the public key to the user.

2. Issuance of electronic cash

The service provider issues electronic cash to the user upon request. To prevent forgery and tampering, the electronic cash is digitally signed by the service provider. Additionally, measures are taken against duplication and double spending by designating the owner at the time of issuance. Therefore, the electronic cash is processed along with the data that includes information about the owners. For details, refer to BOX 2.

(1) The service provider requests the user's certificate and verifies its validity. The certificate's validity is checked against the Certificate Revocation List (CRL) maintained by the certification authority.
(2) The service provider issues electronic cash corresponding to the amount requested by the user.[21] A serial number is assigned to the electronic cash, and the serial number of the issued electronic cash is added to the Issued Electronic Cash Database(DB). Furthermore, a transfer record is attached to each electronic cash instance to indicate that it has been issued (transferred) by the service provider to the user.
(3) The user verifies the service provider's certificate and confirms that the electronic cash and transfer record have been correctly generated (i.e., that the electronic cash has not been forged or tampered with, that the electronic cash and transfer record correspond to the same serial number, and that the user has been specified as the recipient). The electronic cash is then stored on the user's device.

3. Transmission of electronic cash

Users can send electronic cash to other users or to stores. During transmission, the recipient's information is added to the transfer record to prevent duplication and double spending (refer to BOX 2 for details).

(1) The user requests the recipient's certificate and verifies its validity.[22]
(2) The user adds the recipient's information to the transfer record of the electronic cash, then sends the electronic cash, the updated transfer record, and their own certificate to the recipient.
(3) The recipient verifies the sender's certificate and confirms that the received electronic cash and transfer record have been properly transmitted (i.e., that the electronic cash has not been forged or tampered with, that the electronic cash and transfer record correspond to the same serial number, that the electronic cash is

21. In this electronic cash system, the face value of the issued electronic cash is fixed. If it is the same as physical cash, there are 10 kinds of denominations (10,000 yen, 5,000 yen, 2,000 yen, 1,000 yen, 500 yen, 100 yen, 50 yen, 10 yen, 5 yen, and 1 yen).
22. Certificate validation verifies that the counterpart user is the correct user enrolled with the certification authority and that the certificate is valid. To verify the latter, the certification authority must check the Certificate Revocation List (CRL). If it is possible to connect to the Internet, the latest CRL can be checked. Otherwise, it is necessary to set the specification so that the CRL is automatically downloaded to the device as soon as it is connected to the Internet.

not a duplicate of someone else's, and that the recipient has been specified as the intended recipient). The recipient also checks the accuracy of all transfer records generated since issuance by the service provider.[23] The electronic cash and transfer records are then stored on the recipient's device.

4. Redemption of electronic cash

To enable retrospective verification of double spending and reissuance of electronic cash, electronic cash must periodically be returned to the service provider.[24] Redemption by the service provider may occur during user refund (cashing out) or be enforced when the number of transfers exceeds a specified limit.[25]

(1) The user sends the electronic cash and its transfer record to the service provider.
(2) The service provider verifies that the electronic cash and its transfer record have been correctly transmitted. During this verification, the provider ensures that all transfer records since issuance have been accurately generated and checks the validity of the public keys in the transfer record by referring to the CRL.
(3) The service provider performs a double-spending check (described below).
(4) If the user requests reissuance of the electronic cash, the service provider issues new electronic cash equivalent to the same amount.

5. Double-spending check for electronic cash

The service provider verifies whether double spending has occurred by checking the serial numbers of redeemed electronic cash.

(1) The service provider references the Issued Electronic Cash DB to check whether the serial number of the redeemed electronic cash exists in the database.
(2) If the serial number is found in the DB, it is removed from the database, and the returned electronic cash and its transfer record are stored in the Redeemed Electronic Cash DB.
(3) If the serial number is not found in the DB, the electronic cash is deemed to have been double spent. The transfer record of electronic cash with the same serial number is retrieved from the Redeemed Electronic Cash DB, and the public key of the user who double spent the electronic cash is identified from the two transfer

.....

23. This is done to confirm that there is no falsification or inconsistency in the data. If there is falsification or inconsistency, the recipient shall refuse to receive the electronic cash. Since the certificates of other users in the transfer record are not confirmed, even if a user who has not registered with the service provider (without a certificate) or a user who has used a private key stolen from others (the private key corresponding to the public key posted in the CRL) is included in the transfer record, this cannot be detected. Even if such an unauthorized user has engaged in double spending, the service provider cannot identify the user because it does not have the information of the user. However, a user who uses the correct application should not be able to transact with a user who does not have a certificate (the application will reject the transaction). Therefore, it is highly likely that the user who sent electronic cash to the unauthorized user or the user who received electronic cash from the unauthorized person is an accomplice. As a result, service providers may be able to track double spenders by identifying the users involved in the fraud.
24. Since the size of the transfer record attached to the electronic cash increases in proportion to the number of transfers, it is desirable to recover and reissue electronic cash that has been transferred more frequently.
25. In Nakayama *et al*. (1997), since the institution issuing the electronic cash is a financial institution, it is possible to check the double spending of electronic cash returned in the form of deposits in an account. In this method, it is also possible for service providers to cooperate with financial institutions to return electronic cash deposited at financial institutions to the service providers for double-spending checks.

records.

(4) The service provider sends the public key of the double-spending user to the certification authority, which identifies the user corresponding to the public key.[26]

BOX 1 Six phases of the electronic cash system

- **Initial setup**
  (1) Service provider I generates a pair of private and public keys for each denomination and publishes the public key along with a certificate issued by a certification authority. Here, the key pair for a denomination of Y yen is represented as $(\mathrm{sk}_{I(Y)}, \mathrm{pk}_{I(Y)})$.
  (2) Certification authority C generates a private and public key pair and publishes the public key together with its own certificate. The certification authority's key pair is represented as $(\mathrm{sk}_C, \mathrm{pk}_C)$.
- **User registration and certificate issuance**
  (1) User U submits their personal information required for certificate issuance to certification authority C.
  (2) Certification authority C verifies the identity of user U and registers the user information.
  (3) User U generates a pair of private and public keys $(\mathrm{sk}_U, \mathrm{pk}_U)$ and sends the public key pk_U to certification authority C.
  (4) Certification authority C associates public key pk_U with the user information and issues a certificate $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{pk}_U)$ to user U. Sign is a signature generation function, and $\mathrm{Sign}_{\mathrm{sk}}(m)$ represents the digital signature of the message m with the private key sk. Since the certificate is digitally signed by the certification authority, its validity is verified by the digital signature verification process $1/0 \leftarrow \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$. $\mathrm{Verify}_{\mathrm{pk}}(m, \sigma)$ represents the verification formula of the digital signature σ for the message m, and by using the public key pk, it is possible to confirm that the digital signature σ was generated using the private key corresponding to pk and that the message m has not been tampered with. Verify outputs 1 if σ is the correct signature, and 0 if otherwise.
- **Issuance of electronic cash**
  Service provider I issues electronic cash equivalent to Y yen to user U.
  (1) Service provider I requests public key pk_U and its certificate Cer_U from user U who wishes to issue electronic cash and verifies the correctness of Cer_U using $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$. The validity of pk_U is also checked by referring to the CRL by the certification authority.
  (2) Service provider I issues electronic cash for the amount requested by user U. When SN_i is used as serial number,[27] the electronic cash equivalent to Y yen is represented with service provider I's digital signature for $\mathrm{SN}_i{:}T_i \leftarrow$

26. This requires a separate agreement between the service provider and the certification authority and the prior permission of the user.
27. The index *i is* the serial number when dealing with multiple electronic cash.

$\mathrm{Sign}_{\mathrm{sk}_{I(Y)}}(\mathrm{SN}_i)$. Also, $\sigma_{i(0)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_{I(Y)}}(\mathrm{SN}_i \,\|\, \mathrm{pk}_U)$ is generated as the transfer record of T_i, and T_i and $\sigma_{i(0)}$ are sent to user U. The serial number SN_i required for verification of $(T_i, \sigma_{i(0)})$ is also sent. Here, $\|$ represents the concatenation and $\sigma_{i(n)}$ represents the *n-th* transfer record of T_i (counting the issuance as 0). After that, the service provider adds the serial number SN_i to the Issued Electronic Cash DB.

(3) In addition to verifying the certificate of the service provider, user U confirms that the electronic cash and transfer record $(T_i, \sigma_{i(0)})$ are issued correctly using $\mathrm{Verify}_{\mathrm{pk}_{I(Y)}}(\mathrm{SN}_i, T_i)$ and $\mathrm{Verify}_{\mathrm{pk}_{I(Y)}}((\mathrm{SN}_i \,\|\, \mathrm{pk}_U), \sigma_{i(0)})$, and if outputs for both are 1, they are stored in the device.

- **Transmission of electronic cash**

  User U sends m items of electronic cash $\{T_i\}_{1 \le i \le m}$ to user V.[28]

  (1) User U requests the recipient's (user V) public key pk_V and its certificate Cer_V, verifying Cer_V using $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_V, \mathrm{Cer}_V)$.

  (2) When updating the transfer record $\sigma_{i(n)}$, for electronic cash T_i, user U generates the digital signature $\sigma_{i(n+1)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(\sigma_{i(n)} \,\|\, \mathrm{pk}_V)$. The message part of $\sigma_{i(n+1)}$ includes $\sigma_{i(n)}$ and user V's public key pk_V. User U sends the electronic cash and its transfer record $(T_i, \{\sigma_{i(\ell)}\}_{0 \le \ell \le n+1})$ to user V, along with serial number SN_i required for these verifications, public keys of users in the transfer record, and their own public key and certificate. m items of electronic cash $\{T_i\}_{1 \le i \le m}$ are sent as m sets.

  (3) User V verifies user U's certificate Cer_U using $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$, confirms that the received electronic cash and the transfer record are correct, and saves them in their device. Validity of electronic cash T_i and transfer record $\{\sigma_{i(\ell)}\}_{0 \le \ell \le n+1}$ entails: (1) both T_i and $\sigma_{i(0)}$ are signed by the service provider for SN_i; (2) for $0 \le \ell \le n-1$, $\sigma_{i(\ell+1)}$ is the signature for $\sigma_{i(\ell)}$ and the user's public key, whose signer is the user corresponding to the public key in the message portion of $\sigma_{i(\ell)}$; and (3) $\sigma_{i(n+1)}$ is the sending user U's signature for $\sigma_{i(n)}$ and their own public key.

  Further, in (1), for a user's public key pk, it holds that $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}_{I(Y)}}(\mathrm{SN}_i, T_i)$ and $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}_{I(Y)}}((\mathrm{SN}_i \,\|\, \mathrm{pk}), \sigma_{i(0)})$, and in (2), for $0 \le \ell \le n-1$, it holds that $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}}((\sigma_{i(\ell+1)} \,\|\, \mathrm{pk}'), \sigma_{i(\ell+2)})$ and $1 \leftarrow \mathrm{Verify}_{\widetilde{\mathrm{pk}}}((\sigma_{i(\ell)} \,\|\, \mathrm{pk}), \sigma_{i(\ell+1)})$, for a user's public key pk. Here, pk' is the public key of the user to whom the user with public key pk sent T_i, and $\widetilde{\mathrm{pk}}$ is the public key of the user who sent T_i to the user with public key pk. Also, in (3), it holds that $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}_U}((\sigma_{i(n)} \,\|\, \mathrm{pk}_V), \sigma_{i(n+1)})$.

- **Redemption of electronic cash**

  (1) User V sends the electronic cash, its transfer record $(T_i, \{\sigma_{i(\ell)}\}_{0 \le \ell \le n+1})$, serial number SN_i, user public keys in the transfer record, and their own public key and certificate to the service provider.

28. Since electronic cash is issued in face value unit (footnote 21), it should be counted by the number of items when transmitting.

(2) The service provider I confirms that the received $(T_i, \{\sigma_{i(\ell)}\}_{0\leq\ell\leq n+1})$ is correct. The validity of public keys in the transfer record is confirmed via the certification authority's CRL.

- **Double-spending check for electronic cash**
  (1) Service provider I refers to the Issued Electronic Cash DB to check whether the serial number SN_i for the redeemed electronic cash T_i is in the DB.
  (2) If SN_i exists, it is removed from the Issued Electronic Cash DB and the returned electronic cash, along with its transfer record, is added to the Redeemed Electronic Cash DB.
  (3) If SN_i does not exist, double spending is suspected. The service provider retrieves the electronic cash and transfer records with the same SN_i from the Redeemed Electronic Cash DB and identifies the double-spending user from the two transfer records. For instance, for two transfer records with the same serial number, if one transfer shows recipient pk_{U_2} the other pk_{U_3}, the user associated with public key pk_{U_1} is identified as the offender.
  (4) The service provider reports the offending user's public key to the certification authority, which identifies the corresponding user.

BOX 2 Measures against forgery, tampering, duplication, and double spending of electronic cash

- **Measures against forgery and tampering of electronic cash**
  (To prevent the forgery of electronic cash by entities other than the issuing authority, as well as the tampering of amounts or ownership information by entities other than the issuing authority): Electronic cash T is represented as digital signature $T \leftarrow \mathrm{Sign}_{\mathrm{sk}_I}(\mathrm{SN})$ created by the issuing authority I for the serial number SN. Digital signature technology prevents forgery and tampering of electronic cash by third parties.

- **Measures against duplication of electronic cash by third parties**
  (To prevent fraud involving the duplication and use of electronic cash owned by others): The correspondence between electronic cash and its owner prevents third parties from duplicating and using electronic cash fraudulently. Specifically, by adding the public key of the user to the transfer record of electronic cash in a tamper-resistant format, only the corresponding user is able to use the electronic cash.[29]

- **Measures against double spending of electronic cash across multiple users**
  (To prevent fraud where the legitimate owner duplicates received electronic cash and uses it by sending the duplicated cash to multiple users): Since the generation of a signature using a private key is required when sending electronic cash, fraud

29. An attacker can duplicate electronic cash by eavesdropping the communication channel between users or by illegally reading it from the device.

can be prevented through the tamper resistance of the device. However, as technological advancements may reduce the tamper resistance of devices, it is essential to prepare for such situations (see Subsection D). To address this, electronic cash is accompanied by its transfer record in a tamper-resistant format so that service providers can retrospectively identify fraudulent users.

➢ For example, if two instances of electronic cash with the same serial number SN_i are detected and are as follows: For $\sigma_{i(\ell-1)} (= \mathrm{Sign}_{\mathrm{sk}_{U_1}}(\sigma_{i(\ell-2)} \parallel \mathrm{pk}))$, if the public key contained in the message section is pk_{U_2} in one instance and pk_{U_3} in the other instance, it can be determined that the signer of $\sigma_{i(\ell-1)}$ (the user corresponding to public key pk_U) sent the same electronic cash to two different users (pk_{U_4} and pk_{U_5} are the following users' public keys).

$$\sigma_{i(\ell)} = \mathrm{Sign}_{\mathrm{sk}_{U_2}}(\mathrm{Sign}_{\mathrm{sk}_{U_1}}(\sigma_{i(\ell-2)} \| \mathrm{pk}_{U_2}) \| \mathrm{pk}_{U_4}). \quad (1)$$

$$\sigma_{i(\ell)} = \mathrm{Sign}_{\mathrm{sk}_{U_3}}(\mathrm{Sign}_{\mathrm{sk}_{U_1}}(\sigma_{i(\ell-2)} \| \mathrm{pk}_{U_3}) \| \mathrm{pk}_{U_5}). \quad (2)$$

- **Measures against duplication of electronic cash for the same user**
  (To prevent fraud where the legitimate owner or a third party duplicates electronic cash and uses it by resending it to the same user): This can be addressed by adding one-time attributes, such as time stamps, to the transfer record, or by implementing the transmission process of electronic cash as a challenge-response mechanism.[30]

D. Considerations on Security

1. Tamper resistance of devices

The security of electronic cash systems largely depends on the security of digital signatures, and as such, the use of devices capable of securely managing the private keys used for digital signatures is a prerequisite. A tamper-resistant device makes it difficult even for its legitimate owner to illicitly extract the private key stored within or to tamper with the application. This ensures that fraud, such as double spending of electronic cash, can be prevented. However, malicious users may deliberately use non-tamper-resistant devices to commit fraud. Therefore, service providers may need to verify the tamper resistance of user devices. For example, user registration could be allowed only if the tamper resistance of the user's device is confirmed, thereby excluding users who attempt fraud.

Nonetheless, as attack techniques against device security mechanisms evolve, tamper resistance may degrade over time. In such a scenario, even if the aforementioned measures are implemented, it may no longer be possible to prevent double spending of electronic cash. Additionally, service providers design their applications based on the assumption that the security features built into devices will function as expected. However, cases where these features fail to operate as intended make it difficult to con-

30. A method that uses randomly generated values by the verifier each time to counter replay attacks. A replay attack is a type of attack where intercepted data from a communication channel is reused to impersonate a legitimate party. The random value sent by the verifier is called the challenge, and the response provided by the prover is called the response.

duct proper risk assessment and management of applications, as noted by Isobe and Une (2021). To address the potential degradation of tamper resistance, electronic cash systems incorporate transfer records in a tamper-resistant format within electronic cash itself. By checking the serial numbers of circulated electronic cash, service providers can retrospectively detect double spending by users.[31]

2. Relationship between users, devices, and keys

To prevent fraud such as the unauthorized duplication and use of electronic cash by others, electronic cash is designed to be usable (e.g., transferable to other users) only with the "private key" linked to the electronic cash. In this context, the relationship between the "user (person)" and the "device" storing the private key can be classified into the following patterns:

- Case A: Anyone in possession of the device can use the electronic cash stored in it (an *n*-to-1 relationship).
- Case B: Only the legitimate owner of the device can use the electronic cash stored in it (a 1-to-1 relationship).

Case A resembles the use of physical cash and may seem to offer higher usability. However, to ensure post-fraud detection and transparency of electronic cash, the system assumes the use of Case B. In Case B, electronic cash is tied to the "user (person)," allowing only the corresponding user to utilize the electronic cash. To implement Case B, methods such as restricting device usage to its legitimate owner or adopting a mechanism where only the owner can generate the private key may be employed.[32]

E. Considerations on Privacy Protection and Transparency

1. Balancing privacy protection and transparency

There is a prevailing opinion that payment services must account for users' privacy. For instance, the Financial Research Study Group (2018) identified that one of the conditions for the acceptance of new payment methods is that they should provide a level of safety and security equivalent to physical cash. It recommends that service providers strive to protect privacy and personal information.

On the other hand, from the perspective of AML/CFT, there may be cases where it is necessary to retrospectively trace the flow of funds. In such cases, ensuring traceability becomes critically important (Noda 2022). While physical cash lacks traceability, its physical constraints in storage and circulation somewhat limit its use as a medium for money laundering. However, given the risks associated with electronic transfer and payment methods as potential media for money laundering, measures that enable retrospective tracking are essential.

As such, achieving a balance between privacy protection and transparency is crucial

31. One of the methods for conducting electronic payments is called the "balance management scheme," which is similar to that adopted in electronic money, where monetary value received from other users is aggregated, stored, and managed within a device for making payments. However, even in the balance management scheme, if tamper resistance is compromised, it becomes possible to manipulate the data within the device fraudulently and use it to create unlimited monetary value. To detect such fraud retrospectively, it is necessary to manage all transactions using a server-side ledger (Soyama 2020).
32. For example, a private key may be generated each time from the biometric information of the user using Public Biometric Infrastructure (PBI) (Takahashi 2021).

for businesses providing payment services. The following discussion addresses privacy protection for users against other users and against service providers, respectively.

2. Privacy protection against other users

As summarized in Subsection D, during the transmission and receipt of electronic cash, the sending and receiving users verify each other's certificates. Consequently, if personally identifiable information (such as name or address) is included in a certificate, it could enable identification of the counterpart user.[33] In cases such as payments at retail stores, where identifying the counterpart user is unnecessary, certificates should ideally exclude personally identifiable information.

Additionally, electronic cash is transmitted and received along with its transfer record, which includes the public keys of users who previously owned the cash. Even if the public key (or certificate) does not contain personally identifiable information, the public key itself could serve as a user ID, enabling the association of various pieces of information. For instance, if information about the transaction counterpart is obtained through a separate channel (e.g., face-to-face payment), it would become possible to identify the relationship between a user and their public key, potentially enabling the identification of connections among the electronic cash instances used by the user. To ensure anonymity and unlinkability of electronic cash, public keys should be updated for each transaction (Nakayama *et al*. 1997).[34] Furthermore, cryptographic techniques known as zero-knowledge proofs could be employed to prove ownership of electronic cash without disclosing the certificate itself. Protocols utilizing zero-knowledge proofs are discussed in Section IV.

3. Privacy protection and transparency for service providers

When issuing electronic cash, service providers verify the certificates of users receiving the cash. However, by ensuring that personally identifiable information is not included in the certificates, users' privacy can be safeguarded as long as the service provider does not collude with the certification authority.

Moreover, since electronic cash transactions occur exclusively between users, service providers cannot access transaction details in real time. While service providers may verify the transfer record of electronic cash upon redemption, the only information available from the transfer record is the public key of users. Without collusion with the certification authority, it is not possible to identify individual users, thus preserving the anonymity of electronic cash.

As a means of strengthening measures against fraud at certification authorities, separating the functions of user information management and certificate issuance could be considered. For details on certificate issuance methods under such functional separation, refer to Appendix 1. Additionally, it is technically possible to ensure that users who double spend electronic cash can be identified from redeemed electronic cash, while ensuring that no information is revealed about other users. Methods for enhancing privacy protection for service providers are discussed in Section IV.

33. It is possible to design the application in a way that does not disclose the content of received data to the user. However, with a certain level of technical skill, it is possible to duplicate data transmitted between smartphones. Therefore, it is important to consider the potential impact that transmitted and received data may have on users' privacy.
34. There are other methods (for example, Chaum 1983) to protect users' privacy by using electronic cash only once, but they do not satisfy the need to freely transfer electronic cash.

As noted in Subsection E.2, transaction counterparts may have the potential to associate a user with their public key. Thus, by colluding with such a transaction counterpart, service providers could identify a user's transactions based on redeemed electronic cash. To meet the requirements of anonymity and unlinkability of electronic cash even in such cases of collusion, it is necessary, as with the privacy protection measures for other users, to update public keys for each payment transaction.

From the perspective of transparency, it is desirable to periodically review the transfer record of electronic cash. For instance, a design could be adopted where electronic cash is returned to the service provider if it exceeds x transfers or after y periods since issuance. Such measures would enable the service provider to monitor suspicious activities related to electronic cash. Furthermore, in cases such as high-value transfers, where it is necessary to collect real-time information, one possible measure is to permit high-value transfers only when an Internet connection is available, while automatically transmitting a copy of the electronic cash transaction from the application to the service provider. Additionally, by creating a block list for electronic cash, the circulation of cash with suspicious records could be restricted. These measures can be implemented using the programmability embedded in electronic cash.

III. Practical Evaluation of Electronic Cash Systems

A. Past Demonstration Experiments

Demonstration experiments based on electronic cash systems have been conducted multiple times in the past. These experiments primarily involved storing electronic cash on contact-based IC cards and sending it via the Internet to stores or other users. The electronic cash was issued by financial institutions in the form of withdrawals from deposit accounts and could be used in both virtual (Internet-based) and physical stores. The purpose of these experiments was to examine whether such electronic cash scheme could function as a new payment method to replace physical cash and to identify challenges for its practical implementation as a service.

1. Internet Cash (1998)

The demonstration experiment for Internet Cash (September 1998–February 2000) was conducted with the cooperation of four financial institutions and approximately 10,000 participants from the general public. Internet Cash, stored on IC cards, could be used for payments to virtual stores or transfers to other users via reader-writers connected to personal computers. Additionally, Internet Cash could be circulated among users. Internet Cash issued by financial institutions could also be refunded to deposit accounts (Cyber Business Council 2000).

2. Super Cash (1999)

The Super Cash demonstration experiment (April 1999–May 2000) involved the cooperation of 24 financial institutions, approximately 1,000 stores, and about 22,000 participants. As this experiment focused on usability in real-world scenarios, Super Cash was usable not only in virtual stores but also in physical stores. Users could also recharge their IC cards using charge machines installed at financial institutions or via public telephones. However, the Super Cash used in stores was designed to transmit

data to a central data center, and its transferability was not evaluated in this experiment (NTT Communications Corporation 2000).

While the demonstration experiments for Internet Cash and Super Cash provided overviews of their respective implementations, they did not document the time required for transmitting and receiving electronic cash. Considering the IC card specifications and communication environments at that time, it is presumed that ensuring usability posed significant challenges.

B. Overview of the Practical Evaluation

Approximately 25 years have passed since the aforementioned demonstration experiments, and the technological environment surrounding us has changed significantly.[35] Therefore, this study seeks to evaluate the usability of electronic cash system based on current technological standards. In this evaluation, the focus is placed on the transmission processing of electronic cash as a starting point for the study of implementing the electronic cash system. Although comprehensive usability evaluation also includes factors such as application operability, this study evaluates usability primarily based on the time required to transmit electronic cash.

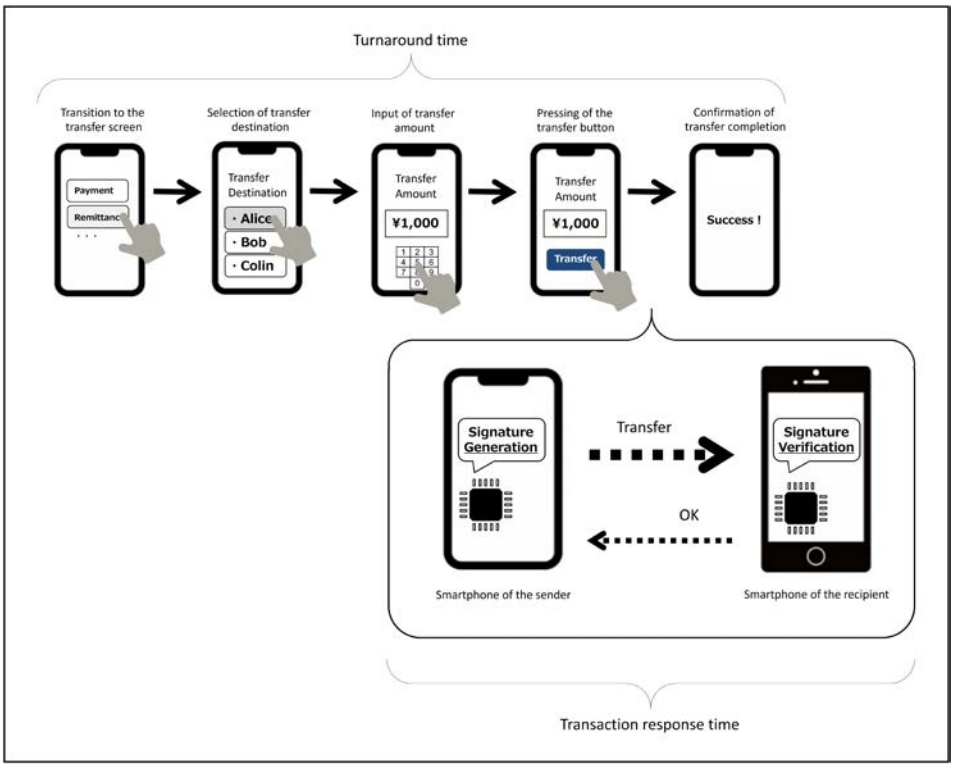
1. Specifications of devices used

To implement electronic cash system, devices need to include tamper-resistant hardware for storing sensitive information such as private keys, as well as communication capabilities for transmitting and receiving electronic cash. Since smartphones are equipped with an embedded Secure Element (eSE) as tamper-resistant device[36] and offer multiple communication functionalities such as mobile data, Wi-Fi,[37] Bluetooth,[38] and Near Field Communication (NFC), this evaluation assumes the use of smartphones. As of 2024, smartphones have an adoption rate of 97% in Japan (NTT Docomo Mobile Society Research Institute 2024), making them a widely used device. The cryptographic algorithm used for the electronic cash system is ECDSA (Certicom Research 2000), a cipher recommended for e-government.

.....

35. In 2000, the Internet usage rate was 37.1%, and telephone dialup was the predominant method. The Asymmetric Digital Subscriber Line (ADSL), which began commercial service in 2000, had a maximum transmission speed of 50 megabits per second downstream and 5 megabits per second upstream. On the other hand, the Internet usage rate in 2023 was 84.9%, and the maximum communication speed of the fifth-generation mobile communication system (5G) launched in 2020 was 4.2 gigabits per second downstream and 218 megabits per second upstream, 84 times and about 43 times higher than ADSL, respectively. The high-performance IC card developed by NTT Corporation around 1999 had a central processing unit (CPU) clock frequency of 15 megahertz, a random-access memory (RAM) capacity of 2 kilobytes, and a flash memory capacity of 512 kilobytes. In contrast, the current general smartphone has a multi-core structure with a CPU clock frequency of several gigahertz, with RAM capacity of several gigabytes and flash memory capacity of several hundred gigabytes. Many of these devices have built-in SEs, which have tamper resistance similar to IC cards. The ST54K (manufactured by ST Microelectronics), the eSE used in the 2022 smartphone (Google Pixel 7), has a CPU clock frequency of 100 megahertz, 64 kilobytes of RAM, and 2,048 kilobytes of flash memory. Google Pixel is a trademark or registered trademark of Google LLC.
36. As of 2024, about 90% of Android smartphones sold in Japan are equipped with GP-SE. GP-SE refers to an SE that complies with the standard specifications of the Global Platform, which promotes the standardization of IC card technologies.
37. Wi-Fi is a registered trademark of the Wi-Fi Alliance.
38. Bluetooth is a registered trademark of Bluetooth, SIG Inc.

Figure 3 Operations related to electronic cash processing



2. Assumptions for the practical evaluation

a. Transaction response time

The time required for processing electronic cash transmission (turnaround time) is defined as the time from selecting the recipient and entering the transfer amount on the application menu screen to the completion of the transfer. Of this, the time from pressing the "Send" button to the transition to the transfer completion screen is the total of the processing time on the sender's and recipient's smartphones and the data communication time (referred to as the transaction response time) (refer to Figure 3). Specifically, this includes: (1) the time required to update the transfer record (signature generation), (2) the time required for the transmission of electronic cash, and (3) the time required to verify the electronic cash and transfer record (signature verification).

b. Processing for signature generation and verification

For updating the transfer record (1), the sender first verifies the recipient's certificate and then generates a digital signature. If the sender is transmitting m items of electronic cash,[39] m items of signature generation processing are required. Letting the processing times for certificate verification and signature generation per item be t_{vs} and t_s (seconds), respectively, the time required for transmission processing is $t_{vs}+t_s \cdot m$ (seconds). For the verification of electronic cash and transfer record (3), the recipient verifies the

39. It is assumed that the system is programmed to send at a minimum number of items depending on the amount to be remitted.

sender's certificate and the transfer record (digital signature verification). If the number of post-issuance transfers for m items of electronic cash is n_m for each item, and the processing time per item for signature verification is t_v (seconds), the time required for reception processing is $t_{vs} + t_v \cdot \sum_m (n_m + 1)$ (seconds). Thus, the total time for (1) and (3) in a single transaction is $2t_{vs} + t_s \cdot m + t_v \cdot \sum_m (n_m + 1)$ (seconds).

To optimize the implementation of electronic cash system, a hybrid architecture is envisaged, in which only signature generation processing, which requires private keys, is performed on tamper-resistant devices such as SEs, while signature verification processing, which does not require private keys, is performed in isolated execution environments such as TEEs. Comparing the processing capabilities of each execution domain, the isolated execution environment can use the same computing resources as the normal environment, while the tamper-resistant devices (especially the eSEs installed in smartphones) have low computing power per unit of time due to the limited computing resources available[40] and incur additional overhead for calls from higher layers.

Since digital signature generation involves more computation than signature verification, the signature generation process is likely to be the bottleneck in performance when implemented on tamper-resistant devices. Therefore, this study focuses on the time required for signature generation (t_s).

c. Processing for electronic cash transmission

Among the communication functions built into smartphones, short-range communication can still function during disasters or communication outages. Ensuring payment functionality even in environments where the Internet is inaccessible is one of the requirements for electronic cash (Section II.B, property (7)). Therefore, this evaluation uses short-range wireless communication technology to transmit electronic cash. It is expected that if usability can be confirmed for face-to-face payments, usability for payments using faster Internet communication can also be assured.

Modern smartphones are generally equipped with Bluetooth, Wi-Fi Direct,[41] and NFC as standard features (refer to Table 1) Bluetooth is a short-range communication standard with a range of approximately 10 meters and is primarily used to wirelessly connect peripheral devices to smartphones. Bluetooth includes two variations: Bluetooth Classic, which supports high-speed transmission of large amounts of data, and Bluetooth Low Energy (Bluetooth LE), characterized by low data transfer speeds and ultra-low power consumption. Wi-Fi Direct is a standard that enables devices equipped with Wi-Fi functionality, such as PCs and smartphones, to connect wirelessly to one another without the need for a wireless LAN router. NFC is a short-range wireless communication technology with a range of about 10 centimeters, enabling communication between contactless IC cards and devices, as well as device-to-device interaction.

When comparing these technologies, NFC is widely used for electronic money transactions and similar applications but has slower communication speeds compared

.....

40. According to specification sheets of eSEs available in the market as of 2024, CPU clock frequencies are in the order of 10 to 100 megahertz (single core), and RAM is in the order of 10 to 100 kilobytes, which result in lower computing power compared to normal or isolated execution environments.
41. Wi-Fi Direct is a trademark or registered trademark of the Wi-Fi Alliance.

Table 1 Comparison of short-range wireless communication technologies

	Short-range wireless communication technologies			
	Bluetooth Classic	Bluetooth Low Energy	Wi-Fi	NFC
Maximum transmission rate specification (per second)	3 megabits (EDR PHY (8DPSK))	2 megabits (LE 2M PHY)	9.6 gigabits (Wi-Fi 6)	106 kilobits (Type-A/B) 424 kilobits (Type-F)
Connection between iOS*1 and Android*2	Not possible*3	Possible	Possible*4	Possible
Connection authentication	Required	Not required	Required	Not required
Encryption of communication data	Yes	Yes (if connection is authenticated)*5	Yes	No*6

Notes: *1 iOS is a trademark or registered trademark of Cisco Systems, Inc. in the United States and/or other countries.
*2 Android is a trademark of Google LLC.
*3 As of June 2024.
*4 Pust be designed so that the Android side becomes the group owner.
*5 Possible to design encryption at the application layer even when connection authentication is not performed.
*6 Possible to design encryption at the application layer.

to Bluetooth and Wi-Fi Direct.[42] Furthermore, Bluetooth Classic differs in supported profiles between iOS and Android, and as of the time of writing (October 2024), cross-platform[43] communication between applications is not feasible. Consequently, to enable the transmission and reception of electronic cash between smartphones of different models, Bluetooth Low Energy and Wi-Fi Direct are considered viable options.

C. Results of the Practical Evaluation

1. Time for signature generation

The time required for generating one digital signature using ECDSA was measured using evaluation boards for three types of eSEs.[44] The results showed significant variation depending on the chip vendor and version: 112 milliseconds for Company A, 102 milliseconds for Company B (Version 1), and 35 milliseconds for Company B (Version 2) (refer to Table 2). With the fastest eSE from Company B (Version 2), theoretically, it would take less than 1.0 second to generate all signatures (update the transfer record) for 28 items of electronic cash.

On the other hand, there may be a need to send larger amounts of electronic cash in one transaction. For larger-scale transactions, a method introduced in Section IV.A constructs a Merkle tree with messages to be signed as leaves and applies a signature only to the root value (root hash). Using this method, regardless of the number of items transmitted, the number of signature generations required for updating the trans-

42. If the data size per electronic cash item is about 4 kilobytes, the data size for sending 50 electronic cash is about 200 kilobytes (= 1.6 megabits). The theoretical maximum transmission bandwidth for NFC is 424 kilobits per second, which means it would take about 3.8 seconds to send 50 items.
43. A program that runs applications with the same specifications on different operating systems (OSs).
44. The eSEs used in the verification were products of two major chip vendors (Company A and Company B). Company B (Version 2) is a successor to Company B (Version 1).

Table 2 Comparison of signature generation time (Average time of 50 attempts)

	Types of eSEs		
	Company A	Company B (Version 1)	Company B (Version 2)
Signature generation time	112 milliseconds	102 milliseconds	35 milliseconds

Table 3 Electronic cash delivery time comparison (Average time of 50 attempts)

		Delivery size (Bytes)	Transmission time in milliseconds (not including connection establishment time)	
			Bluetooth Low Energy	Wi-Fi Direct
No. of items	1	3,380	590	2
	50	169,000	5,580	62
	100	338,000	10,700	160

Notes: *Size of electronic cash and transfer record assuming 5 transfers since issuance. Since the size of the electronic cash (signed by the service provider) is 580 bytes and the transfer record is 560 bytes, the total is 580 + 560*5 = 3,380 bytes. The test data for evaluation were prepared by estimating the size as follows. Data related to electronic cash: 580 bytes = signature size 96 bytes + message size 484 bytes (public key, serial number, etc.); data related to transfer record: 560 bytes = signature size 96 bytes + message size 464 bytes (public key, etc.)

fer record can be reduced to one. For Company B's (Version 2) eSE, this means the signature generation time remains 35 milliseconds, irrespective of the number of items sent.

2. Time for electronic cash transmission

The evaluation measured the time required to transmit electronic cash using Bluetooth Low Energy and Wi-Fi Direct with an Android smartphone. The transmission times were measured for 1, 50, and 100 items of electronic cash, excluding the time required for establishing connections.

The results showed that for transmitting 100 items, Bluetooth Low Energy took 10.7 seconds (10,700 milliseconds), while Wi-Fi Direct completed the transmission in just 0.16 seconds (160 milliseconds). This confirms that Wi-Fi Direct is more efficient for transmitting electronic cash (refer to Table 3).

3. Transaction response time

Using Company B's (Version 2) eSE and leveraging Merkle tree-based optimization, the signature generation time for sending 100 items of electronic cash can be reduced to 35 milliseconds. Assuming a similar time for signature verification at the recipient's end, the total processing time for both the sender's and recipient's applications would be approximately 70 milliseconds. Since Wi-Fi Direct enables transmission to the recipient in 160 milliseconds, the total transaction response time for sending 100 items of electronic cash is approximately 230 milliseconds (0.23 seconds).

A study suggests that a transaction response time of less than 1.0 second is desirable (Nielsen 2010). Compared to credit card contactless payments (0.5 seconds, Visa 2014) or public transportation electronic money payments (0.2 seconds, Ootsuki 2011),

a response time of 0.23 seconds is evaluated as offering sufficient usability. However, unlike contactless payments, electronic cash system involves smartphone operation and requires connection authentication and encryption for Wi-Fi Direct, necessitating further consideration of the time required for these processes.

IV. Considerations for Enhancing the Efficiency of Electronic Cash Systems

This section discusses methods to improve the efficiency of the processes involved in sending and receiving electronic cash, as well as the redemption of electronic cash. Specifically, the focus is on two aspects: (1) a method for batch processing the update of transfer records when transmitting multiple electronic cash, and (2) an efficient method to verify digital signatures issued by the same signer during the redemption process, which is conducted by service providers.

In addition, under the electronic cash system described in Section II, if the user does not possess the exact amount of electronic cash required for a transaction, they need to receive change. This means that in a fixed-denomination electronic cash system, two transfer processes are often necessary for a single transaction. Therefore, as a method to enhance efficiency, this section considers a variable-denomination system, which allows users to flexibly split and aggregate their electronic cash for transmission (Section II.B, property (2)). Although variable-denomination systems have been studied in the past (e.g., Okamoto and Ohta 1992), the approach here differs from existing methods by employing digital signature algorithms (e.g., ECDSA or EdDSA)[45] as components. This configuration allows the use of arbitrary signature algorithms and offers flexibility, such as adaptability to cryptographic migration challenges.[46]

Furthermore, under the electronic cash system described in Section II, users were required to update their public keys for each transaction to ensure unlinkability. This section proposes a method to satisfy unlinkability using zero-knowledge proofs, thereby streamlining the process of updating public keys.

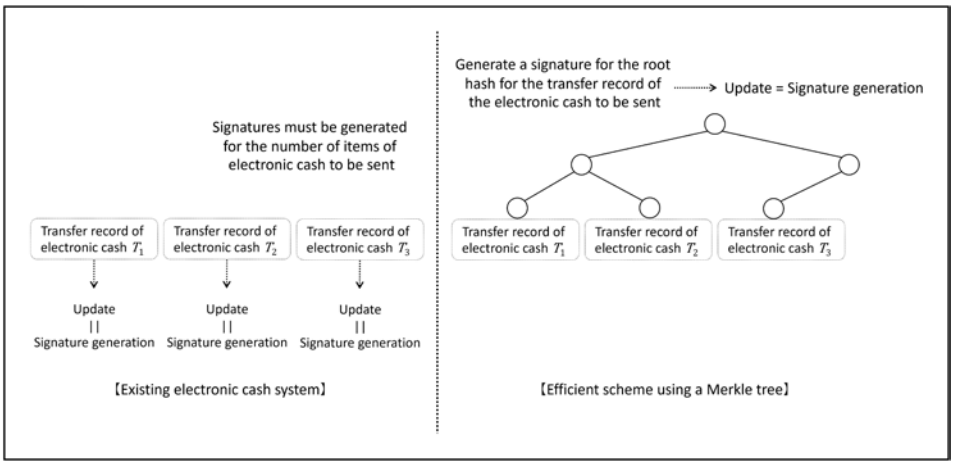
A. Enhancing the Efficiency of Electronic Cash Transmission and Receipt

From a usability improvement perspective, this section explores ways to optimize the process of sending electronic cash. Under the electronic cash system in Section II, the transfer record of each item of electronic cash being sent need to be individually updated. Since the transfer record must be secured with digital signatures to prevent tampering, the processing time for sending electronic cash increased in proportion to the number of items being sent.

To address this, the following protocol introduces the use of Merkle trees to improve the efficiency of digital signature generation. A Merkle tree is a tree structure

45. EdDSA is one of the e-Government recommended ciphers. It is a digital signature scheme using the Edward curve.
46. It should be noted, however, that when the signature size is drastically changed, such as in quantum-resistant cryptography, it is necessary to change the message size in the communication protocol. In the financial field, studies on the transition to quantum-resistant computer cryptography are progressing (Une 2023), and it is important to make the configuration aware of the future transition to cryptography.

Figure 4 Efficient scheme using a Merkle tree



where each leaf node is labeled with the hash value of data, and each internal node is labeled with the hash value of its child nodes' labels. In this method, a signature is generated for the root value (root hash) of the Merkle tree constructed from the transfer record of the electronic cash being sent. As a result, the number of signature generations required can be reduced to one, regardless of the number of items being sent (refer to Figure 4).

The process for transferring electronic cash from user U to user V is as follows:

(1) User U requests a certificate Cer_V from the recipient user V and verifies its validity.
(2) When sending m items of electronic cash $\{T_i\}_{1\le i\le m}$, with serial number SN_i, user U calculates $h_i \leftarrow H(\sigma_{i(n_i)})\,(1 \le i \le m)$ for the transfer records $\{\sigma_{i(\ell)}\}_{1\le i\le m, 0\le \ell\le n_i}$. Here, n_i represents the number of transfers that the electronic cash T_i has undergone, and $\sigma_{i(\ell)}$ represents the ℓ-th transfer record of T_i. The initial transfer record at the time of issuance of T_i is $\sigma_{i(0)}$. Additionally, user U constructs a Merkle tree L with $\{h_i\}_{1\le i\le m}$ as leaf nodes and computes the root value h (refer to Appendix 2.A for details on constructing a Merkle tree).
(3) To update the transfer record, user U generates a digital signature $\sigma \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(h \,\|\, \mathrm{pk}_V)$ for h and user V's public key pk_V. Note that sk_U is the private key of user U.
(4) User U sends the electronic cash with the updated transfer record to user V. The data sent includes $\{\mathrm{SN}_i, T_i, \sigma, \sigma_{i(\ell)}\}_{(1\le i\le m, 0\le \ell\le n_i)}$ and the public keys in the transfer record.
(5) User V verifies the validity of the electronic cash using the digital signature and stores the received electronic cash in their device.

Through this protocol, user V, the recipient of the electronic cash, only needs to perform a single signature verification for the transfer record updated by user U, regardless of the number of electronic cash received. However, previous transfer records $\sigma_{i(\ell)}\,(0 \le \ell \le n_i)$ still require verification as before. For details on this protocol, refer

to Appendix 3.

B. Enhancing the Efficiency of Electronic Cash Redemption

During redemption, service providers must verify that all transfer records of the redeemed electronic cash have been correctly generated since issuance. If the electronic cash has been transferred *n-th* times since issuance, the transfer record will contain $n+1$ linked digital signatures, all of which must be verified. As the number of redeemed electronic cash increases, the processing load on the service provider also increases proportionally.

In the EdDSA signature scheme, the number of elliptic curve multiplications required during signature verification can be reduced by linearly combining multiple verification equations from the same signer (Bernstein *et al*. 2012, Fujisaki 2020). The processing load for verifying transfer records can be reduced by aggregating the signatures of large-scale users, such as financial institutions or retailers, within the redeemed transfer records.[47] For further details on the EdDSA algorithm, refer to Appendix 2.B.

C. Considerations for a Variable Denomination Scheme

The electronic cash system discussed in Section II has fixed denominations, meaning that users cannot split their electronic cash into smaller amounts. This section introduces a method to enable flexible denomination splitting, as well as representing arbitrary amounts with a tree structure whose leaves correspond to the smallest units (e.g., 1 yen). Specifically, a user can create an N-ary tree ($N \geq 2$) where the leaves represent 1 yen, and the service provider issues electronic cash as a digital signature for the root value of this N-ary tree. When a user wishes to send part of their electronic cash, they create a subtree corresponding to the desired amount and send this subtree (with its root value and signature) as electronic cash.[48] Thus, in this scheme, both the electronic cash and its transfer record are updated with each transaction. Additionally, the method introduced in Subsection A which uses Merkle trees, can also be applied to reaggregate split electronic cash for transmission.

The following section describes the protocol for issuing and sending electronic cash with $N = 2$, using specific examples.[49]

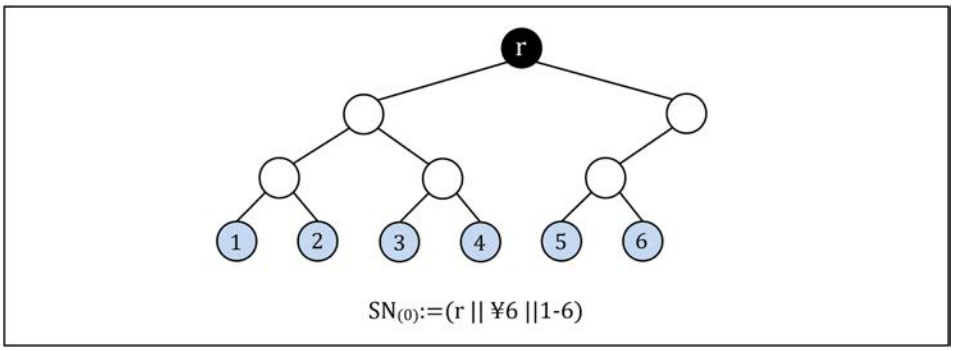
1. Issuance of electronic cash

A process where a service provider issues electronic cash worth 6 yen to user U is as follows:

(1) The service provider generates a pair of private and public keys $(\mathrm{sk}_I, \mathrm{pk}_I)$ and

47. Comparing the signature verification process that applies batch processing to multiple signatures by the same signer and the signature verification process without batch processing, using an ordinary laptop PC, the execution time when batch processing was applied was about 45% of that when batch processing was not applied (average value for 1 million attempts).
48. As a method to implement the variable denomination scheme, it is conceivable to include amount information in the message portion of a signature, similar to transactions in Bitcoin. However, this protocol instead transmits electronic cash in units of 1 yen, distinguishable from one another, rather than in monetary values. This allows for the identification of which specific electronic cash were double spent, even in cases where double-spent electronic cash becomes mixed. Notably, Bitcoin uses a ledger-based system, which promptly performs double-spending checks, making it unlikely for double-spent bitcoins to mix at their destination.
49. The protocol for detection by service providers of double spending of electronic cash is omitted, but as with the existing method, service providers store all redeemed electronic cash and check for duplicates.

Figure 5 Method for generating serial numbers for electronic cash in the variable denomination scheme (Example of constructing 6 yen using a binary tree)



publishes the public key along with a certificate issued by the certification authority.

(2) The service provider generates a binary tree of depth 3 = ($\lceil \log_2 6 \rceil$) to represent 6 yen and assigns labels to the leaves. The labels represent the position of the leaves in the binary tree, numbered sequentially from left to right as 1, 2, 3, and so forth.

(3) The service provider generates a random number r and assigns it to the root of the binary tree.

(4) The service provider generates serial number $\mathrm{SN}_{(0)} := (r \,\|\, ¥6 \,\|\, 1\text{-}6)$ for the electronic cash representing 6 yen.[50] The serial number $\mathrm{SN}_{(n)} := (r \,\|$ amount $\|$ left-right) uniquely identifies the tree structure of the electronic cash, consisting of the random number r assigned to the root, the amount, and information specifying the range of the leaves (from the leftmost label left to the rightmost label right) for 6 yen (refer to Figure 5). Here, n represents the number of transfers of the electronic cash after issuance.

(5) The service provider generates electronic cash $T_{(0)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_I}(\mathrm{SN}_{(0)} \| ¥6)$ representing 6 yen and its transfer record $\sigma_{(0)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_I}(\mathrm{SN}_{(0)} \,\|\, ¥6 \| \mathrm{pk}_U)$, and sends $(\mathrm{SN}_{(0)}, T_{(0)}, \sigma_{(0)})$ to user U. The electronic cash comprises a digital signature on the serial number ($\mathrm{SN}_{(0)}$) and the amount (¥6), and the transfer record includes the recipient user's public key (pk_U).

(6) The service provider registers the issued electronic cash ($T_{(0)}$) in the Issued Electronic Cash DB, ensuring $T_{(0)}$ can be retrieved using r as an index.

(7) User U verifies the validity of the received $(T_{(0)}, \sigma_{(0)})$ by checking the following:
- ➢ Both $T_{(0)}$ and $\sigma_{(0)}$ are signatures by the service provider on the same serial number ($\mathrm{SN}_{(0)}$),
- ➢ $\mathrm{SN}_{(0)}$ is correctly structured based on the issued amount, and
- ➢ $\sigma_{(0)}$ is a signature by the service provider on pk_U, the user's public key.

50. In generalization, the serial number is represented as $\mathrm{SN}_{i\,(0)} := (r_i \,\|\, ¥6 \,\|\, 1\text{-}6)$ for a random number r_i.

2. Transmission of electronic cash

A process where user U sends 4 yen of the 6 yen electronic cash issued by the service provider, to user V is as follows:[51]

(1) User U reconstructs the binary tree indicated by the serial number $\mathrm{SN}_{(0)}$ of $T_{(0)}$ and assigns r_0 to the root of the subtree representing the 4 yen to be sent (leaves labeled 1–4) by calculating $r_0 \| r_1 \leftarrow G(r)$,[52] where G is a common function that generates $2m$-bit pseudo-random numbers from an m-bit input.

(2) User U generates a new serial number $\mathrm{SN}_{(1,1)} \leftarrow (r_0 \| ¥4 \| 1\text{-}4)$ for the sent electronic cash. Here, $\mathrm{SN}_{(n,k)}$ denotes the serial number assigned to the k-th electronic cash generated by splitting $T_{(n-1,x)} (x \geq k)$ (refer to Figure 6). To update the electronic cash and transfer record, user U generates $T_{(1,1)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(T_{(0)} \| \mathrm{SN}_{(1,1)} \| ¥4)$ and $\sigma_{(1,1)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(\sigma_{(0)} \| \mathrm{SN}_{(1,1)} \| ¥4 \| \mathrm{pk}_V)$ for the recipient's public key pk_V, and sends $(\mathrm{SN}_{(1,1)}, T_{(1,1)}, \sigma_{(1,1)}, \mathrm{SN}_{(0)}, T_{(0)}, \sigma_{(0)})$ along with public key pk_U and its certificate to user V. The message part of the signatures by the users includes the pre-split electronic cash $T_{(0)}$ and transfer record $\sigma_{(0)}$ respectively, creating a linked signature chain. Measures such as one-time identifiers or challenge-response methods are employed to prevent duplication of electronic cash for the same user.

(3) User U saves the unused portion of $T_{(0)}$ (labels 5–6) along with $(T_{(0)}, \sigma_{(0)})$ on their device.

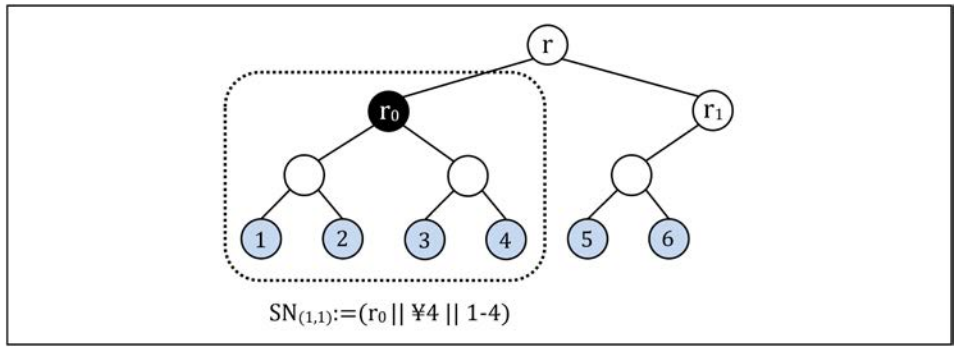
➢ For subsequent transfers of the remaining 2 yen or any part of it, user U follows the same procedure as in Step 2 to create the corresponding electronic cash and transfer record based on $(T_{(0)}, \sigma_{(0)})$.

(4) User V verifies the validity of the received $(\mathrm{SN}_{(1,1)}, T_{(1,1)}, \sigma_{(1,1)}, \mathrm{SN}_{(0)}, T_{(0)}, \sigma_{(0)})$ by checking the following:

➢ $\mathrm{SN}_{(1,1)}$ is correctly generated:

- For $r \in \mathrm{SN}_{(0)}$, $x \leftarrow G(r)$ ensures the upper m bits of x are elements of $\mathrm{SN}_{(1,1)}$,

Figure 6 Method for splitting electronic cash in the variable denomination scheme (Splitting and sending 4 yen out of 6 yen)



51. When sending an amount such as 5 yen out of 6 yen, the tree composed of the leaves corresponding to the amount to be sent becomes the entire tree. In such cases, pseudo-random numbers generated by G are unnecessary, and the first element of the serial number generated in Step 2 will be the root value r, of the tree.
52. r_1 generated by $G(r)$ is used to send partial trees with leaves labeled 5 to 6.

➢ $T_{(1,1)}$ and $\sigma_{(1,1)}$ are correctly generated:
  - Both are signed by the sender U,
  - $\sigma_{(1,1)}$ includes a signature on the recipient's public key pk_V,

➢ $T_{(0)}$ and $\sigma_{(0)}$ are correctly generated:
  - Both are signatures by the service provider on the same serial number ($\mathrm{SN}_{(0)}$),

➢ $\sigma_{(0)}$'s message contains the public key pk_U, of the signer of $\sigma_{(1,1)}$.

D. Electronic Cash Scheme with Enhanced Privacy

As summarized in Section II, to achieve unlinkability in electronic cash scheme, it is necessary to change the public key each time electronic cash is sent or received. However, frequent updates to public keys would significantly increase the certificate issuance and management costs on the part of the certification authority, while also leading to processing delays and reduced usability. This section considers a method to enhance user privacy without increasing the certificate issuance and management costs for the certification authority.[53] However, since this method utilizes zero-knowledge proofs, the processing and communication costs for sending and receiving electronic cash become relatively higher. It should be noted that the implementation of this method requires improvements in the performance of user devices and communication speed.

The following three requirements must be addressed from a privacy protection standpoint when implementing the enhanced privacy electronic cash scheme:

Requirement (1) Unlinkability of electronic cash transactions carried out by the same user:

➢ If the same public key is included in the transfer record of multiple items of electronic cash, information related to the user corresponding to that public key (e.g., purchasing history) could be leaked.

Requirement (2) Verifiability of legitimate transactions even under anonymity and unlinkability: Even when anonymity and unlinkability are ensured, the recipient of the electronic cash must be able to confirm that the transaction was conducted by a legitimate user registered with the certification authority.

➢ Traditionally, this confirmation was achieved by verifying the certificate issued by the certification authority. The enhanced privacy scheme must also meet this requirement.

Requirement (3) Identification of users engaging in double spending: Even when anonymity and unlinkability are ensured, the service provider must be able to identify users who engage in double spending.

➢ Similar to conventional electronic cash systems, the ability to identify fraudulent users is essential.

.....

53. Since the method discussed in this section does not support the variable denomination scheme described in Subsection C, it is necessary to consider the enhancement of the privacy of the variable denomination scheme separately.

To enhance privacy, the proposed scheme introduces a transaction-specific public key in addition to the public key registered with the certification authority. By allowing users to update their transaction-specific public key for each transaction, the scheme protects user privacy from service providers and other users (Requirement (1)). Furthermore, the transaction-specific public key is associated with the certificate issued by the certification authority, and their relationship is verified to confirm that the user is conducting transactions with a valid key registered with the certification authority (Requirement (2)). Additionally, as with the basic electronic cash scheme in Section II, this enhanced privacy scheme leverages the properties of zero-knowledge proofs to identify users from double spent electronic cash (Requirement (3)).

In this scheme, the sender and recipient of electronic cash execute a non-interactive protocol based on the Σ protocol, a type of zero-knowledge proof (see Appendix 3. A). The Σ protocol allows the prover to demonstrate to the verifier that certain secret information satisfies a specific condition without revealing the information itself. In this scheme, the Σ protocol is used to satisfy Requirement (2), wherein the sender of the electronic cash acts as the prover, and the recipient acts as the verifier.

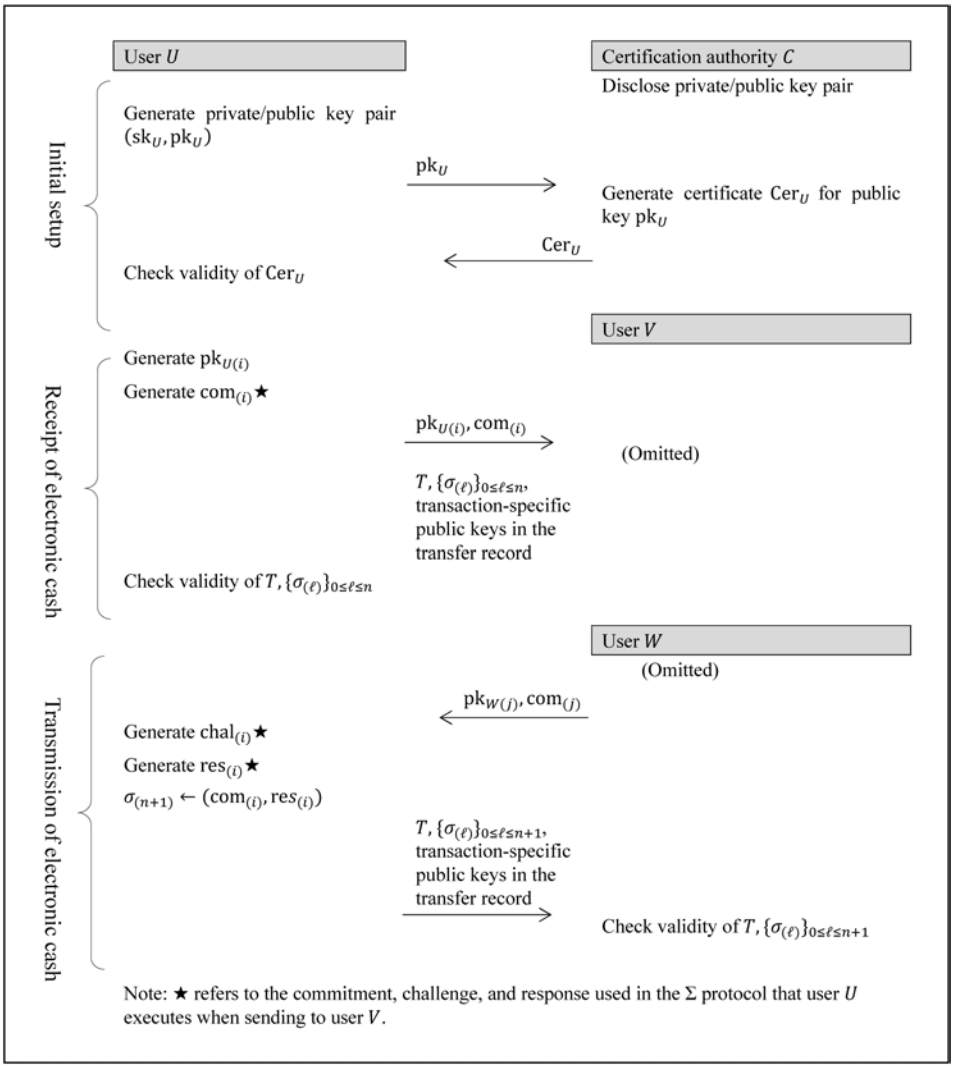
In the non-interactive setting, the prover generates and transmits three types of data to the verifier: commitment, challenge, and response. A notable property of the Σ protocol is that if two different challenges and responses exist for the same commitment, the prover's secret information is exposed. The proposed scheme uses this property to identify users who double spend the electronic cash. Specifically, the commitment generated by the user is embedded in the digital signature (transfer record of the electronic cash) in a tamper-proof format. As a result, even in cases of double spending, the commitment remains identical. To achieve this, the commitment is generated when the electronic cash is received, not when it is sent. As in the basic electronic cash system in Section II, the electronic cash T and its transfer record σ are transmitted and received as a set in this scheme.

The requirements (1)–(3) mentioned above are fulfilled through the following methods:

- Generation and update of transaction-specific public key $\mathrm{pk}_{(i)}$: Users generate their own transaction-specific public keys and update them for each i-th transaction.
- Certificate issuance and self-signing: Users obtain a certificate Cer for their public key pk from the certification authority and generate a self-signed certificate $\mathrm{Cer}_{(i)}$ for the transaction-specific public key $\mathrm{pk}_{(i)}$ using their private key sk. By proving that Cer and $\mathrm{Cer}_{(i)}$ correspond to the same public key, it can be verified that the transaction through $\mathrm{pk}_{(i)}$ was conducted by a legitimate user registered with the service provider. Additionally, anonymity against the service provider is ensured by using zero-knowledge proofs to conceal the public key pk and certificate Cer.
- Identification of fraudulent users: The service provider leverages the properties of zero-knowledge proofs to identify the public key pk of users who engage in double spending.

The specific procedures are summarized in 1.-4. (refer to Figure 7) For details of

Figure 7 Privacy-enhanced electronic cash transmission and reception protocol



the protocol, refer to the Appendix 3.B.3.

In this method, unless double spending occurs, the user's public key is not disclosed to the service provider.[54] Therefore, from the perspective of AML/CFT, a potential approach might involve intentionally simulating double spending for high-value transactions on the application level, allowing the service provider to identify the user (Otsuka 2022).

54. In this method, even service providers find it difficult to determine the user's public key from the transfer record of redeemed electronic cash. Therefore, even if the service provider, rather than the certification authority, handles user registration and manages user information, it is still possible to satisfy the anonymity and unlinkability of electronic cash.

1. Initial setup

The certification authority and users prepare the key pairs and the certificates as follows:

(1) The certification authority generates a pair of private and public keys $(\mathrm{sk}_C, \mathrm{pk}_C)$ and publishes them along with its self-signed certificate.
(2) User U generates a key pair $(\mathrm{sk}_U, \mathrm{pk}_U)$ and sends pk_U to the certification authority.
(3) The certification authority issues a certificate Cer_U for the public key pk_U and provides it to user U.

2. Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

(1) User U randomly generates a transaction-specific public key $\mathrm{pk}_{U(i)}$, where i is the transaction ID for U.
(2) User U creates a self-signed certificate $\mathrm{Cer}_{U(i)}$ for $\mathrm{pk}_{U(i)}$ using sk_U.
    ➢ Public key $\mathrm{pk}_{U(i)}$ is generated specifically for the transaction involving the electronic cash received from user V.
(3) User U sends the transaction-specific public key $\mathrm{pk}_{U(i)}$ to be used for electronic cash T and commitment $\mathrm{com}_{(i)}$ to user V upon the latter's request.[55]
    ➢ $\mathrm{com}_{(i)}$, generated by user U, is intended for use in the Σ protocol[56] when the electronic cash is later sent to user W. However, it is generated at this stage and sent to user V to enable identification of double-spending users.
(4) User U receives the electronic cash T, its transfer record $\{\sigma_{(\ell)}\}_{0\leq\ell\leq n}$, and the transaction-specific public keys of previous users included in the transfer record, from user V.
    ➢ $\sigma_{(n)}$ consists of the commitment $\mathrm{com}_{(k)}$ and response $\mathrm{res}_{(k)}$ from user V under the Σ protocol.[57] Here, n represents the number of times the electronic cash T has been transferred.
(5) User U verifies the validity of T and $\{\sigma_{(\ell)}\}_{0\leq\ell\leq n}$. If the verification is successful, user U accepts the electronic cash; otherwise, rejects it. When transferring m items of electronic cash, this process is repeated m times.

3. Transmission of electronic cash

A process user U sends the electronic cash T received from user V to user W is as follows:

(1) User U requests the transaction-specific public key $\mathrm{pk}_{W(j)}$ and commitment $\mathrm{com}_{(j)}$ from user W, where j is the transaction ID for user W.
(2) User U discloses $\mathrm{pk}_{U(i)}$ and generates a challenge $\mathrm{chal}_{(i)}$ and a response $\mathrm{res}_{(i)}$. Using the previously generated $\mathrm{com}_{(i)}$, along with $(\mathrm{chal}_{(i)}, \mathrm{res}_{(i)})$, user U proves

55. A commitment to x refers to data generated in such a way that when user U sends the commitment to user V, it is difficult for user V to determine the value of x from the commitment, and user U cannot alter the value of x after sending the commitment. Additionally, the function used to compute the commitment is referred to as a commitment function.
56. Σ protocol in which the prover is user U and the verifier is user W.
57. Σ protocol in which the prover is user V and the verifier is user U.

that they are a legitimate user registered with the certification authority (i.e., they possess the private key corresponding to the public key registered with the certification authority). While $\mathrm{pk}_{U(i)}$ is disclosed, neither the self-signed certificate $\mathrm{Cer}_{U(i)}$, the public key pk_U, nor the certificate Cer_U are revealed. User U demonstrates that:
  - ➢ they possess the self-signed certificate $\mathrm{Cer}_{U(i)}$ corresponding to $\mathrm{pk}_{U(i)}$ and the public key pk_U corresponding to the private key used to generate $\mathrm{Cer}_{U(i)}$,
  - ➢ they possess the certificate Cer_U issued for the above public key pk_U, and
  - ➢ that $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)}, T)$ have not been tampered with.

(3) User U generates $\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})$ and sends $(T, \{\sigma_{(\ell)}\}_{0\leq\ell\leq n+1})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.

(4) User W verifies the validity of T and $\{\sigma_{(\ell)}\}_{0\leq\ell\leq n+1}$. If the verification is successful, user W accepts the electronic cash; otherwise, rejects it. This process is repeated m times when receiving m items of electronic cash.

4. Detection of double spending

The service provider determines that electronic cash is double spent if its serial number is not found in the Issued Electronic Cash DB. Leveraging the properties of the Σ protocol, the service provider can identify the public key of the user who engaged in double spending and verify the corresponding user with the certification authority.

V. Conclusion

In this paper, we focused on electronic cash system, a payment system that does not rely on a ledger and revisited its characteristics while conducting practical verification based on widely used contemporary devices. During the experimental trials of the 1990s, the usability of electronic cash system was likely limited due to significant constraints on the performance of IC cards and communication environments at the time. In contrast, the present verification, conducted with the assumption of smartphone usage, demonstrated that, in theory, transactions involving the transfer of 100 items of electronic cash could be processed in approximately the same amount of time as existing contactless IC card payment systems. However, it should be noted that this verification measured only transaction response times; in practice, additional time for application operations and establishing smartphone connections must also be taken into account. This evaluation was limited to the processes of sending and receiving electronic cash items, leaving numerous issues for further consideration. For instance, in this study, we assumed the presence of an independent institution responsible for user identity verification and certificate issuance to enhance privacy protection from service providers. However, to achieve practical implementation, a review of compliance with existing laws will also be required. Additionally, while this paper focused on the retrospective traceability of electronic cash items for AML/CFT purposes, further studies are necessary to explore other potential methods of compliance.

As part of our future-oriented discussions, we also considered a scheme enabling the division and aggregation of electronic cash items into arbitrary amounts. Such a

scheme would eliminate the need for transactions involving change or currency exchange, thereby improving usability. Moreover, the proposed scheme, which treats electronic cash items for each unit amount independently, differs from methods that merely aggregate monetary values during division or aggregation. It enables tracing of doubly spent electronic cash items even if mixed with other items. Detailed evaluations of the security of this variable denomination scheme and practical verification on actual devices are planned going forward.

We also explored a protocol designed to enhance privacy. This protocol ensures that even service providers cannot easily obtain information about users' transactions from redeemed electronic cash items. However, processing with zero-knowledge proofs incurs higher computational costs and larger signature sizes compared to conventional digital signatures. Thus, improved device performance and communication speeds are prerequisites for its implementation. At present, this aspect remains a theoretical exploration, but it is expected to be valuable for future discussions.

The rapid advancement of information and communication technology is likely to continue reshaping our devices, network structures, and lifestyles. Moving forward, we aim to continue evaluating the feasibility of electronic cash system through practical verification while also exploring new possibilities in anticipation of future technological advancements. We hope that the results of this study will contribute to the realization of more efficient and user-friendly payment services.

References

Bernstein, Daniel J., Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. "High-Speed High-Security Signatures." *Journal of Cryptographic Engineering* 2 (2012): 77–89.

Certicom Research. 2000. "SEC 1: Elliptic Curve Cryptography (Version 1.0)." The Standards for Efficient Cryptography Group. Accessed July 1, 2026. https://www.secg.org/SEC1-Ver-1.0.pdf.

Chaum, David. "Blind Signatures for Untraceable Payments." *Proceedings of CRYPTO '82, Lecture Notes in Computer Science* 1440. Springer, 1983. 199–203.

Consumption and Distribution Policy Division, Commerce and Service Industry Policy Group, Ministry of Economy, Trade and Industry (METI). 2018. "Cashless Vision." Ministry of Economy, Trade and Industry. Accessed July 1, 2026. http://www.meti.go.jp/policy/mono_info_service/cashless/image_pdf_movie/cl_vision.pdf. (in Japanese).

Cyber Business Council. "Internet Cash Verification Report." E-Japan Council. 2000 (in Japanese).

Financial Research Study Group. 2018. "Development of a Cashless Society and the Role of the Financial System." Japanese Bankers Association. Accessed July 1, 2026. https://www.zenginkyo.or.jp/fileadmin/res/news/news300437_1.pdf.

Fujisaki, Eiichiro. 2020. "Study and Evaluation of the Security of the Digital Signature EdDSA Configuration." 2020 Cryptographic Research Report, CRYPTREC. Accessed July 1, 2026. https://www.cryptrec.go.jp/exreport/cryptrec-ex-3002-2020.pdf (in Japanese).

Furuichi, Mineko. "Genkin, Kinsen ni Kansuru Hoteki Ichikosatsu (Legal Discussion on Cash and Money)." *Kin'yu Kenkyu* 14, no. 4 (1995): 101–52 (in Japanese).

Hojo, Masashi, and Junichiro Hatogai. "Kessai Shisutemu ni Okeru Puroguramabiriti no Jitsugen (Programmability of Payment and Settlement Systems)." Bank of Japan Review No. 2022-J-12. Bank of Japan, 2022 (in Japanese).

Isobe, Kohei, and Masashi Une. "Sumaatofon-to no Sumato Debaisu ni okeru Sekyuriti: Purattofoomu-ka ni yoru Risuku no Genjo to Tenbo (Security in Smartphones and Other Smart Devices: The Current State and Prospects of Risks Associated with Platforms)." *Monetary and Economic Studies* 40, no. 3 (2021): 77–102 (in Japanese).

Ministry of Economy, Trade and Industry. 2024. "2023-nen no Kyasshuresu Kessai Hiritsu o Sanshutsu Shimashita: Kyasshuresu Kessai Hiritsu wa 39.3%, 2025-nen no Mokuhyo-nen ni Mukete Kencho ni Kakudai (Cashless Payment Ratio Calculated for 2023: 39.3%, Cashless Payment Ratio Expanding Steadily Toward 2025)." Accessed July 1, 2026. https://www.meti.go.jp/press/2023/03/20240329006/20240329006.html (in Japanese).

Nakata, Masao. "Taimen Kessai no Kyasshuresuka no Shinten ni Tomonatte Kentosubeki Shomondai to Sono Taio no Hokosei (Issues to be Examined in Conjunction with the Advancement of Cashless Face-to-Face Payments and the Directions for their Support)." *Journal of Research on Social and Economic Life* 61, no. 2 (2021): 32–55 (in Japanese).

Nakayama, Yasushi, Hidemi Moribatake, Masayuki Abe, and Eiichiro Fujisaki. "An Eletronic Money Scheme—A Proposal for a New Electronic Money Scheme which is both Secure and Convenient—." IMES Discussion Paper No. 97-E-4. Bank of Japan 1997.

Nielsen, Jakob. 2010. "Website Response Times." Nielsen Norman Group. Accessed July 1, 2026. https://www.nngroup.com/articles/website-response-times/.

Noda, Kohei. "Kanryu Suru Chika Shikin: Hanzai, Tero, Kakukaihatsu Mane to no Tatakai: 12 Shusho: Dejitaru Kakumei to Chika Shikin (Recirculation of Underground Funds: The Fight Against Crime, Terrorism, and Nuclear Development Money: Chapter 12: Digital Revolution and Underground Funds)." *The Finance* 2022 July Edition (2022): 40–50 (in Japanese).

NTT Corporation. "Denshi Genkin Hoshiki no Jikken Shisutemu o Kaihatsu: Ango Gijutsu ni Yotte, Riyosha no Puraibashi Hogo to Takai Anzensei o Jitsugen (Development of Experimental System for an Electronic Cash System Using Cryptography to Enable Privacy Protection of Users and High Level of Safety)." *NTT NEWS RELEASE*, NTT, 1995 (in Japanese).

———, "Atarashii Denshi Mane Jikken Shisutemu o Shisaku: Anzensei, Shinraisei, Koritsu-sei o Ichidan to Takameta Shin Hoshiki o Saiyo (Prototype of a New Electronic Money System:

Adopting a New System with Higher Level of Safety, Reliability and Efficiency).” *NTT NEWS RELEASE*, NTT. 1996 (in Japanese).

NTT Communications Corporation, “Denshi Mane ‘Supa Kyasshu’ ni Kansuru Kongo no NTT Komyunikeshonzu no Torikumi ni Tsuite (Future Initiatives of NTT Communications Regarding the Electronic Money ‘Super Cash’).” 2000 (in Japanese).

NTT Docomo Mobile Society Research Institute. 2024. “2024-nen Chosa Sumaatofon Hiritsu 97%: 2010-nen wa Yaku 4% (2024 Smartphone Use Ratio 97%: About 4% in 2010).” NTT DoCoMo Mobile Society Research Institute. Accessed July 1, 2026. https://www.moba-ken.jp/project/mobile/20240415.html (in Japanese).

NTT Network Service Systems Laboratories. 2023. “6G/IOWN Jidai no Yugo Kyosho Nettowaku: Inkurushibu Koa (Inclusive Core: Integrative and Cooperative Network Architecture for the 6G/IOWN Era).” White Paper, NTT. Accessed July 1, 2026. https://www.rd.ntt/ns/inclusivecore/whitepaper_ver1.html (in Japanese).

Okamoto, Tatsuaki, and Kazuo Ohta. “Universal Electronic Cash.” Advances in Cryptology—*Proceedings of CRYPTO’91, Lecture Notes in Computer Science* 576, Springer, 1992. 324–337.

Okamoto, Tatsuaki, and Kazuo Ohta. “Risoteki Denshi Genkin Hoshiki no Ichihouhou (An Ideal Method for the Electronic Cash System).” *IEICE Transactions* J76-D-I, no. 6 (1993): 315–23 (in Japanese).

Ootsuki, Satoshi. “Suica Shisutemu no Gaiyo (Outline of the Suica System).” *Journal of the Institute of Electrical Installation Engineers of Japan* 31, no. 6 (2011): 408–11 (in Japanese).

Otsuka, Akira. “Tai Tanpa Sei ni Motoduku Dejitaru Tsuka Uoretto no Kenkyu Doko: Tokumei Sei to Tomei Sei no Ryoritsu ni Mukete (Research Trends in Tamper-Resistant Digital Currency Wallets: Balancing Anonymity and Transparency).” IMES Discussion Paper No. 2022-J-9. Bank of Japan 2022 (in Japanese).

Soyama, Tomoyuki. 2020. “Suica ni okeru Deta to Sabisu no Arikata: Onrain to Ofurain no Haiburiddo (Suica Data and Services: Hybrid Online and Offline).” Future Forum on Payment and Settlement, Digital Currency Subcommittee: Lecture on Digital Payments in the Post-Covid19 Era, Payment and Settlement Systems Department, Bank of Japan. Accessed July 1, 2026. https://www.boj.or.jp/paym/outline/mirai_forum/data/rel200911b8.pdf (in Japaese).

Takahashi, Kenta. “Dejitaru Torasuto Jidai no Seitai Ninsyo Kiban: Public Biometric Infrastructure (PBI) to Kanren Gijutsu (Biometric Authentication Infrastructure in the Era of Digital Trust: Public Biometric Infrastructure (PBI) and Related Technologies).” Lecture Material at the 22nd Information Security Symposium, Institute for Monetary and Economic Studies, Bank of Japan. 2021 (in Japanese).

Tamura, Yuko, and Masashi Une. “IC Kaado o Riyoshita Honnin Ninsyo Shisutemu ni okeru Sekyuriti Taisaku Gijutsu to Sono Kento Kadai (Security Countermeasures for IC Card-based Identity System and Issues to Consider).” *Kin’yu Kenkyu* 26, no.1(2007): 53–100 (in Japanese).

Une, Masashi. “Ryoshi Konpyuta ga Ango ni Oyobosu Eikyo ni Do Taisho Suru ka: Kaigai ni okeru Torikumi (How to Cope with the Impact of Quantum Computers on Cryptography: Overseas Initiatives).” IMES Discussion Paper No. 2023-J-13, Institute for Monetary and Economic Studies, Bank of Japan, 2023 (in Japanese).

Visa. 2014. “Contactless Payments,” VISA Canada. Accessed July 1, 2026. https://www.visa.ca.dam/VCOM/regional/na/canada/merchants/documents/visa-paywave-put-your-customer-in-the-fast-lane-en.pdf.

APPENDIX 1: CERTIFICATE ISSUANCE PROCEDURE WHEN THE FUNCTIONS OF THE CERTIFICATION AUTHORITY ARE DIVIDED

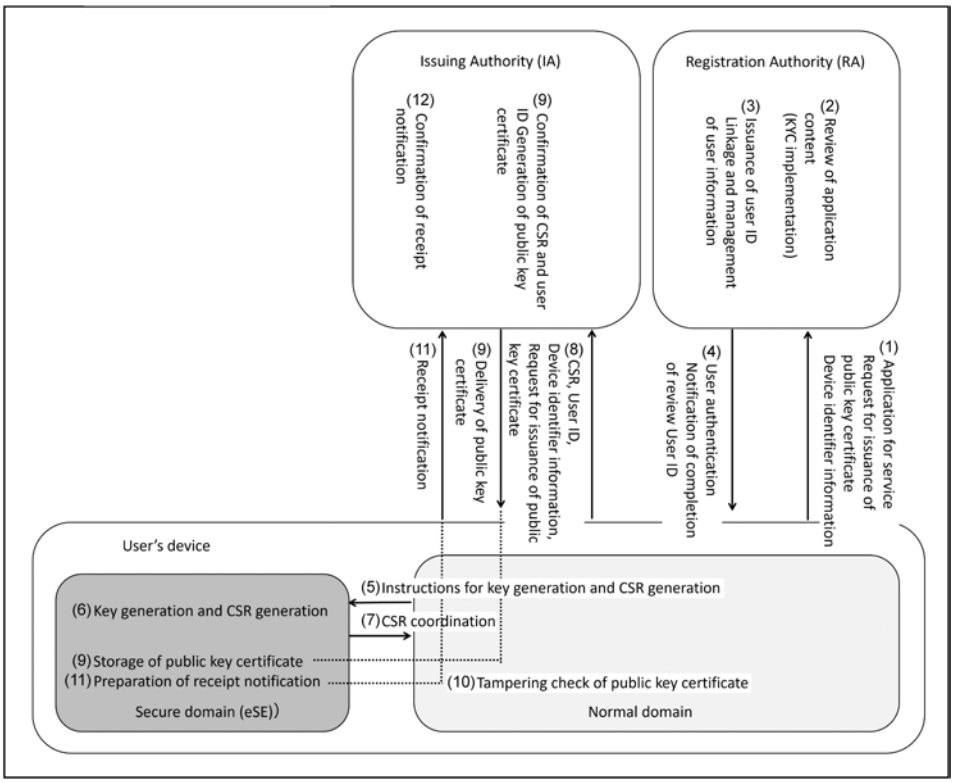
This section outlines the procedure for user registration and certificate issuance when the tasks of managing user information and issuing certificates are handled separately, as discussed in Section II.C (refer to Figure A-1). Here, the entity managing the user information is referred to as the Registration Authority (RA), the entity issuing and managing certificates is referred to as the Issuing Authority (IA), and the combined entities are collectively referred to as the Certification Authority (CA).

(1) The user applies for the service via an application installed in the normal domain of their device (hereafter referred to as the normal domain app) and sends a certificate issuance request to the RA. At this stage, the RA requests the user's device identifier information[58] from the device.
(2) The RA reviews the contents of the submitted application form.[59] If necessary, the RA conducts identity verification.
(3) If the RA finds no issues in the review, it issues a user identification code to the normal domain app and links it to the user information submitted by the user.
(4) The RA sends a notification of the completed review and the user identification code to the normal domain app.
(5) Upon receiving the review completion notification, the normal domain app instructs the application installed in the secure domain (hereafter referred to as the secure domain app) to generate a key pair and create a Certificate Signing Request (CSR).
(6) The secure domain app generates the key pair and the CSR.
(7) The secure domain app links the CSR generated within the secure domain to the normal domain app.
(8) The normal domain app sends the CSR, the user identification code, and the device identifier information to the IA, requesting the issuance of a certificate.
(9) The IA verifies that there are no issues with the received CSR and user identification code (e.g., no duplication) and generates the certificate.
(10) The secure domain app performs an integrity check on the public key and stores the certificate in the secure domain.
(11) The secure domain app generates a receipt notification within the secure domain and sends it to the IA via the normal domain app.
(12) The IA confirms the receipt notification.

.....

58. Information that can be used as device identifier information includes the International Mobile Equipment Identity (IMEI) and IDs assigned to each device's eSE. The choice should be made based on the security and usability requirements of the service.
59. An assessment is conducted to ensure there are no issues with allowing the user to access the service. For example, this may involve verifying that the user has not previously violated the terms of service.

Figure A-1 Certificate issuance procedure when the functions of the certification authority are divided



APPENDIX 2: OPTIMIZATION OF ELECTRONIC CASH SYSTEMS

A. Enhancing the Efficiency of Electronic Cash Transmission and Receipt

This section elaborates on the detailed protocol for optimizing the transmission and receipt of electronic cash as outlined in Section IV.A.

1. Initial setup (Three algorithms)

The method using a Merkle tree (refer to Figure A-2) employs the following three algorithms: MHTree, MHPath, and MHVer.

- $(L, h) \leftarrow \text{MHTree}(D)$
  - ➢ The function MHTree takes a dataset D as input and outputs a Merkle tree L, with the elements of D $(= \{(i, h_i)\})$ as leaf nodes, and the root value h. A Merkle tree is a tree structure generated by repeatedly assigning the hash values of two child nodes to their parent node. Here, i is the node identifier, and h_i denotes the value labeled on the node. For example, the identifiers of the leaf nodes at depth 3 are represented by 3-digit binary numbers, sequentially numbered as 000, 001, ... , 111. If the number of elements in D is insufficient for constructing a full binary tree, the algorithm outputs a Merkle tree where the remaining nodes are labeled with h_i = "00...". Using a hash function H, the tree assigns $H(h_{000}, h_{001})$ to h_{00}, $H(h_{00}, h_{01})$ to h_0, and so forth. Figure A-2 illustrates a tree where the value of the node identified by i is represented as h_i.
- $(AP, h) \leftarrow \text{MHPath}(D, D')$
  - ➢ The MHPath function takes a dataset D and its subset $D'(\subset D)$ as inputs and outputs the path AP required to calculate from D' the root h of the Merkle tree generated from D, as well as the root value h.
  - ➢ For example, if $D' = \{(000, h_{000}), (100, h_{100}), (101, h_{101})\}$, the algorithm outputs $\text{AP} = \{(001, h_{001}), (01, h_{01}), (11, h_{11})\}$ and h for the input of D' (refer to Figure A-3).
- $1/0 \leftarrow \text{MHVer}(D', AP, h)$
  - ➢ The MHVer function takes a dataset D', a path AP, and a root value h as inputs. It verifies whether the root value of the Merkle tree with $D' \cup \text{AP}$ as the node matches h. The function returns 1 if they match and 0 otherwise.

2. Processing of electronic cash transmission and receipt

The specific steps for user U to transfer electronic cash to user V are as follows:

(1) User U requests and verifies the certificate Cer_V from the recipient user V.

(2) User U calculates $h_i \leftarrow H(\sigma_{i(n_i)})(1 \le i \le m)$ for the m electronic cash $T_i\,(1 \le i \le m)$ being transmitted and their respective transfer records $\sigma_{i(\ell)}\,(1 \le i \le m, 0 \le \ell \le n_i)$. Here, n_i denotes the number of transfers for T_i and $\sigma_{i(\ell)}$ represents the transfer record at the ℓ-th transfer. $\sigma_{i(0)}$ is the initial transfer record assigned at issuance of T_i. The Merkle tree L with $\{h_i\}_{1 \le i \le m}$ as leaf nodes and root value h are computed using $(L, h) \leftarrow \text{MHTree}(\{(i, h_i)\}_{1 \le i \le m})$.

(3) User U updates the transfer record by generating a digital signature $\sigma \leftarrow \text{Sign}_{\text{sk}_U}(h \parallel \text{pk}_V)$ for root h and pk_V, the public key of user V.

(4) User U sends their certificate Cer_U, the m electronic cash, and their transfer

Figure A-2 Structure of Merkle trees

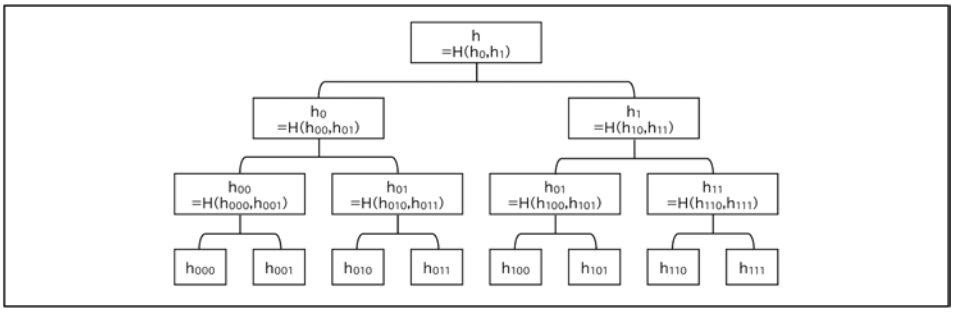
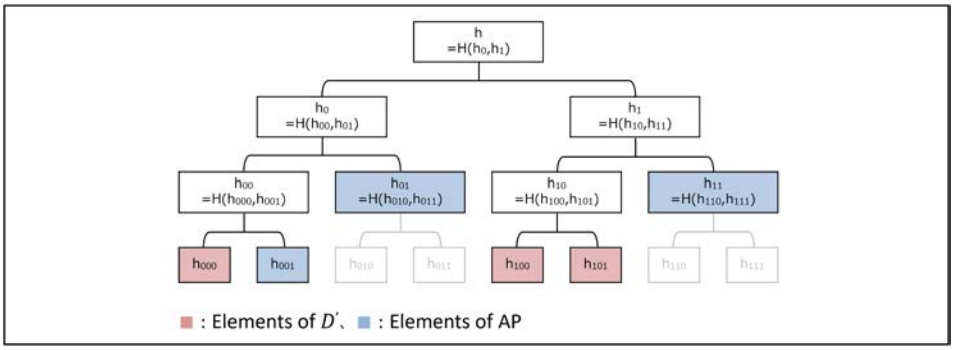


Figure A-3 Relationship between input (D′) and output (AP) of the MHPath function



records to user V. The transmitted data include $(\{T_i\}_{1\le i\le m}, \sigma, \{\sigma_{i(\ell)}\}_{1\le i\le m, 0\le \ell\le n_i})$, along with $(\mathrm{AP}_j, h_j) \leftarrow \mathrm{MHPath}(\{\sigma_j\}, \sigma_{i(n_i-1)})$, which is necessary to verify previous transfer records $\sigma_{i(\ell)} (0 \le \ell \le n_i)$. Here, $\{\sigma_j\}$ represents the transfer record of electronic cash $\{T_j\}(\ni T_i)$ sent upon receiving electronic cash T_i from user U_j in the the past.

- ➢ The updated transfer record σ is common across the m items of electronic cash T_i and represented as $\sigma = \sigma_{1(n_1)} = \sigma_{2(n_2)} = \cdots = \sigma_{m(n_m)}$.

(5) User V verifies the validity of Cer_U, confirms that the received electronic cash was correctly transmitted, and saves it to their device.

- ➢ This involves calculating $(L, h) \leftarrow \mathrm{MHTree}(\{(i, \sigma_{i(n_i)})\}_{1\le i\le m})$ and verifying that σ is a valid signature for h by user U.
- ➢ Using $\mathrm{MHVer}(\sigma_{i(n_i)}, \mathrm{AP}_j, h_j)$, user V verifies the validity of h_j and confirms that $\sigma_{i(n_i)}$ is a valid signature for h_j. This process is repeated for all transfer records $\sigma_{i(\ell)} (1 \le i \le m, 0 \le \ell \le n_i)$.

B. Enhancing the Efficiency of Electronic Cash Redemption

EdDSA consists of three algorithms (key generation, signature generation, and signature verification) under the following parameter settings (Bernstein *et al*. 2012, Fujisaki 2020).

Parameter settings:

The parameters used in EdDSA are as follows:

- Odd prime number q, finite field $\mathbb{F}_q$.
- Positive integer b: the length of the public key. Note that $q < 2^{b-1}$.
- Hash function $H\colon \{0,1\}^* \to \{0,1\}^{2b}$.
- Encoding function: $\mathbb{F}_q \to \{0,1\}^{b-1}$ (converts elements of $\mathbb{F}_q$ into $(b-1)$ bit representation).
- (Twisted) Edwards curve over $\mathbb{F}_q$:
  $E(\mathbb{F}_q)\colon \{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q\colon ax^2 + y^2 = 1 + dx^2y^2\}$.
  a: quadratic residue over $\mathbb{F}_q$, d: (non-zero) quadratic non-residue over $\mathbb{F}_q$.
  If $q \equiv 1 \pmod 4$, then $a = -1$; if $q \equiv 3 \pmod 4$, then $a = 1$.
  The order of E, denoted $\#E = 2^c * \ell$, where $c = 2 \text{ or } 3$, and 2^c is called the cofactor.
- Base point $B \in E, B \neq (0,1), \ell B = (0,1)$, where ℓ is a prime number. The cyclic group generated by B has order $\#B = \ell$.

When the addition on the Edwards curve is defined as follows, E becomes an additive group with the identity element $O = (0,1)$:

$$(x_1, y_1) + (x_2, y_2) := \left(\frac{(x_1y_2 + x_2y_1)}{1 + dx_1x_2y_1y_2}, \frac{(y_1y_2 + x_1x_2)}{1 - dx_1x_2y_1y_2} \right). \tag{A-1}$$

Key generation:

A user generates the private key k and public key A as follows:

- $k \leftarrow \{0,1\}^b$.
- $(h_0, h_1, \ldots, h_{2b-1}) \leftarrow H(k)$.
- $a \leftarrow 2^{2b-2} + \sum_{3 \le i \le b-3} 2^i h_i \in \{2^{2b-2}, 2^{2b-2} + 8, \ldots, 2^{2b-1} - 8\}$.
- $A \leftarrow aB$.

Private key: k
Public key: $\underline{A} := aB$ (where $\underline{A}$ is the encoded value of A)

Signature generation:

The signer uses $(h_b, \ldots, h_{2b-1})\,(= H(k))$ (derived from k) to generate the signature $(\underline{R}, \underline{S})$ for message M as follows:

- $r \leftarrow H(h_b, \ldots, h_{2b-1}, M) \in \{0, 1, \ldots, 2^{2b} - 1\}$.
- $R \leftarrow rB$.
- $S \leftarrow (r + H(\underline{R}, \underline{A}, M)\, a) \mod \ell$.

Signature verification:

The verifier uses the public key $\underline{A}$ of the signer to confirm the validity of the signature $(\underline{R}, \underline{S})$ for message M by checking the following equation:

- $2^c S B = 2^c R + 2^c H(\underline{R}, \underline{A}, M) A$.

Batch verification:
For multiple signatures $(\underline{R_i}, \underline{S_i})$ corresponding to messages M_i by public keys A_i, batch verification can be performed by linearly combining the signature verification equations as follows:

- Select random integers z_i based on the parameters and the number of signatures and compute $H_i = H(R_i, A_i, M_i)$.
- Confirm the validity of the following equation:
$$(-\Sigma_i z_i S_i \bmod \ell)\, B + \Sigma_i z_i R_i + \Sigma_i\, (z_i H_i \bmod \ell)\, A_i = 0.$$

APPENDIX 3: PRIVACY-ENHANCED ELECTRONIC CASH PROTOCOL

Here, in addition to the protocol proposed in Section IV.D, two alternative methods are introduced: (1) a method where the user's private key is registered with the service provider, and malicious actors are identified using the user's private information, and (2) a method where only the user's public key is registered with the service provider, and malicious actors are identified using the user's private information. Compared to the method introduced in Section IV, these approaches are less secure in terms of operational safety but offer the advantage of lower computational costs.

A. Σ Protocol

The Σ protocol is a zero-knowledge proof protocol that demonstrates knowledge of a witness w for x, which belongs to the language $L_R = \{x \mid \exists w, (x, w) \in R\}$ (proof that x belongs to language L), by exchanging the data called "commitment," "challenge," and "response" between the prover and the verifier.

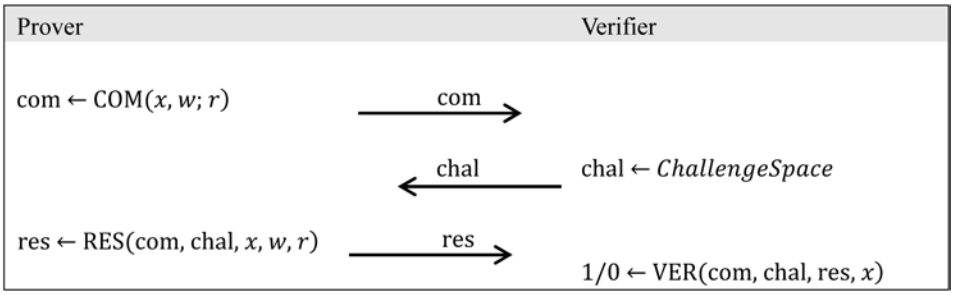
The prover first sends a commitment com to the verifier, which is generated using public information x, the witness w, and a random number r. The verifier then sends a challenge chal, generated using a sufficiently secure random number generation function, to the prover. Finally, the prover sends a response res to the verifier. If the prover knows the witness w for x, it can generate res using a function RES such that $1 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$ in response to the exchanged com and chal. For a user who does not know w, the probability of generating res that satisfies $1 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$ is negligibly small, and with overwhelming probability, becomes $0 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$ (refer to Figure A-4).

Additionally, the function $\mathrm{EXT}(x, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ returns the witness w satisfying $\mathrm{com} \leftarrow \mathrm{COM}(x, w; r)$ from the inputs (chal, res) and (chal′, res′), which use the same commitment in two zero-knowledge proofs.

The above Σ protocol can be converted into a non-interactive proof using hash function H. Specifically, replacing $\mathrm{chal} \leftarrow H(\mathrm{com})$ allows the prover to generate res without interacting with the verifier.

The privacy-enhanced electronic signature scheme is composed of the following functions:

Figure A-4 Σ Protocol



- $(\mathrm{sk}, \mathrm{pk}) \leftarrow \mathrm{Gen}(1^{\delta})$: Gen generates a key pair $(\mathrm{sk}, \mathrm{pk})$, where sk is the private key and pk is the public key. δ is the security parameter.
- $c \leftarrow \mathrm{Commit}(x\,; r)$: Commit generates a commitment c for x using a random number r.
- $\sigma \leftarrow \mathrm{Sign}_{\mathrm{sk}}(m)$: Sign generates a digital signature σ for the message m using the private key sk.
- $1/0 \leftarrow \mathrm{Verify}_{\mathrm{pk}}(m, \sigma)$: Verify verifies the digital signature σ of the message m using the public key pk. It outputs 1 if σ is a valid signature and 0 otherwise.
- $\mathrm{com} \leftarrow \mathrm{COM}(x, w\,; r)$: COM generates a commitment com for the witness w of x in the Σ protocol to prove the possession of the witness w for x. r is a random number.
- $\mathrm{chal} \leftarrow H(\mathrm{com})$: H is a hash function used to generate challenges in the Σ protocol.
- $\mathrm{res} \leftarrow \mathrm{RES}(\mathrm{com}, \mathrm{chal}, x, w, r)$: RES generates a response res in the Σ protocol to prove the possession of the witness w for x.
- $1/0 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$: VER verifies whether com and res is a valid pair in the Σ protocol to prove the possession of the witness w for x. It outputs 1 if $(\mathrm{com}, \mathrm{res})$ are valid and 0 otherwise.
- $w \leftarrow \mathrm{EXT}(x, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$: EXT extracts the witness w satisfying $\mathrm{com} \leftarrow \mathrm{COM}(x, w\,; r)$ from the inputs $(\mathrm{chal}, \mathrm{res})$ and $(\mathrm{chal}', \mathrm{res}')$, which use the same commitment in two zero-knowledge proofs.

B. Three Implementation Methods

1. Method 1 (Registering the private key with the certification authority and identifying double-spending users via the private key)

Method 1 involves registering the user's private key sk with the certification authority instead of the public key pk. The certification authority then issues a certificate Cer for the private key sk. The three requirements outlined in Section IV.D. are satisfied using the methods described below:

- Generation and update of transaction-specific public key $\mathrm{pk}_{(i)}$: Users generate their own transaction-specific public keys and update them for each i-th transaction. Transaction-specific public key $\mathrm{pk}_{(i)}$ is generated based on the private key sk.
- Certificate issuance for the private key: The user obtains a certificate Cer for the private key sk from the certification authority. By proving that both Cer and $\mathrm{pk}_{(i)}$ are derived from the same private key, it is demonstrated that transactions using $\mathrm{pk}_{(i)}$ are conducted by the legitimate user registered with the certification authority. Additionally, by utilizing zero-knowledge proof, both the private key sk and the certificate Cer can remain concealed, thereby satisfying anonymity requirements for service providers.
- Identification of fraudulent users by service providers: Service providers can leverage the characteristics of zero-knowledge proof to identify the private key sk of users who have engaged in double spending of electronic cash.

a. Initial setup

The certification authority and users prepare the key pairs and the certificates as fol-

lows:

(1) Certification authority C generates a pair of private and public keys, $(\mathrm{sk}_C, \mathrm{pk}_C) \leftarrow \mathrm{Gen}(1^\delta)$, and publishes the public key along with its self-signed certificate.
(2) Certification authority C randomly selects the private key $\mathrm{sk}_U \in \{0,1\}^\lambda$ for user U, and issues $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{sk}_U)$ to user U through a secure channel. Here, λ is the security parameter.
(3) User U computes $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{sk}_U, \mathrm{Cer}_U)$. If the result is 1, the user accepts $(\mathrm{sk}_U, \mathrm{Cer}_U)$; otherwise, rejects it.

b. Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

(1) User U selects a random number $r_{U(i)} \in \{0,1\}^\lambda$ and computes transaction-specific public key $\mathrm{pk}_{U(i)} \leftarrow \mathrm{Commit}(\mathrm{sk}_U; r_{U(i)})$.
- $\mathrm{pk}_{U(i)}$ is the public key used by user U for the i-th transaction.

(2) User U selects another random number $r_{(i)} \in \{0,1\}^\lambda$ and computes $\mathrm{com}_{(i)} \leftarrow \mathrm{COM}((\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}); r_{(i)})$.
(3) User U sends $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ to user V and receives $(T, \{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, from user V. Here, T is the electronic cash issued by user V and signed with its serial number by the service provider. $\sigma_{(n)}$ represents the transfer record of T, where n indicates the number of previous transfers of T.
- $\mathrm{com}_{(k)}$ is generated by user V upon receiving T from another user under the public key $\mathrm{pk}_{V(k)}$ (corresponding to Step 2 of this protocol performed by user U). It represents the k-th transaction for user V.
- $\mathrm{res}_{(k)}$ is generated by user V upon receiving $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ from user U (corresponding to Step 3 of protocol for sending electronic cash performed by user U).

(4) User U verifies T and computes $\mathrm{VER}(\mathrm{com}_{(k)}, \mathrm{chal}_{(k)}, \mathrm{res}_{(k)}, (\mathrm{pk}_{V(k)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash, otherwise, rejects it. Here, $\mathrm{chal}_{(k)} \leftarrow H(\mathrm{com}_{(k)})$ is the hash value of $\mathrm{com}_{(k)}$.

c. Transmission of electronic cash

A process user U sends electronic cash T to user W is as follows:

(1) User U receives $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)})$ from user W.
- For user W, this corresponds to Steps 1–2 of the protocol for receiving electronic cash and represents the j-th transaction.

(2) User U computes $\mathrm{chal}_{(i)} \leftarrow H(T, \mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)})$.
- $\mathrm{com}_{(i)}$ is generated by user U upon receiving T from user V (Step 2 of the protocol for receiving electronic cash).

(3) User U computes $\mathrm{res}_{(i)} \leftarrow \mathrm{RES}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}), r_{(i)})$. The Σ protocol proves that $(\mathrm{pk}_{U(i)}, \mathrm{pk}_C)$ belong to the following language L, $L := \{(\mathrm{pk}_{U(i)}, \mathrm{pk}_C) | \exists (\mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}), \mathrm{com}(\mathrm{sk}_U; r_{U(i)}) = \mathrm{pk}_{U(i)} \wedge \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{sk}_U, \mathrm{Cer}_U) = 1\}$.

(4) User U sends $(T, \{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.
(5) User W verifies T and computes $\mathrm{VER}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, \mathrm{res}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C))$ for $\{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash; otherwise, rejects it. Here, $\mathrm{chal}_{(i)} \leftarrow H(\mathrm{com}_{(i)})$ is the hash value of $\mathrm{com}_{(i)}$.

d. Detection of double spending

A process the service provider identifies the double-spend of electronic cash is as follows:

(1) If the serial number of the returned electronic cash T is not in the Issued Electronic Cash DB, the service provider determines that it has been double spent and retrieves T and its record σ' with the same serial number from the Redeemed Electronic Cash DB.
(2) The service provider computes the private key $\mathrm{sk}_U \leftarrow \mathrm{Ext}(\mathrm{pk}_{U(i)}, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ based on the two transfer records σ and σ'.
(3) By inquiring with the certification authority, the service provider identifies the user associated with private key sk_U.

2. Method 2 (Registering the public key with the certification authority and identifying double-spending users via the private key)

Method 2 involves the issuance of a certificate for a user's public key rather than their private key. As no transmission of private keys occurs between the certification authority and the user, the risk of key leakage is reduced. However, the computational cost associated with the transmission and receipt of electronic cash increases compared to Method 1. The three requirements outlined in Section IV.D are satisfied using the methods described below:

- Generation and update of transaction-specific public keys: The user generates the transaction-specific public key $\mathrm{pk}_{(i)}$ and updates it for each i-th transaction.
- Issuance of public key certificates: The user obtains a certificate Cer issued by the certification authority for their public key pk. By demonstrating that the transaction-specific public key $\mathrm{pk}_{(i)}$ and the public key pk are both derived from the same private key, it can be proven that the transaction using $\mathrm{pk}_{(i)}$ was conducted by a legitimate user registered with the certification authority.
  ➢ The key difference from Method 1 is that the certificate issued by the certification authority applies to the public key. Consequently, the propositions to be proven under the Σ protocol differ, requiring changes to the generation methods for commitments and responses.
- Identification of fraudulent users by service providers: Service providers can leverage the characteristics of zero-knowledge proof to identify the private key sk of users who have engaged in double spending of electronic cash.

a. Initial setup

The certification authority and users prepare the key pairs and the certificates as follows:

(1) Certification authority C generates a pair of private and public keys,

$(\mathrm{sk}_C, \mathrm{pk}_C) \leftarrow \mathrm{Gen}(1^\delta)$, and publishes the public key along with its self-signed certificate.

(2) User U randomly selects private key $\mathrm{sk}_U \in \{0,1\}^\lambda$.

(3) User U selects a random value r_U and computes the public key $\mathrm{pk}_U \leftarrow \mathrm{Commit}(\mathrm{sk}_U; r_U)$.

(4) User U sends pk_U to the service provider and receives certificate $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{pk}_U \| *)$ for pk_U.

(5) User U verifies Cer_U by calculating $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$. If the result is 1, the user accepts $(\mathrm{pk}_U, \mathrm{Cer}_U)$; otherwise, rejects them.

b. Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

(1) User U selects a random value $r_{U(i)} \in \{0,1\}^\lambda$ and computes the transaction-specific public key $\mathrm{pk}_{\mathrm{U}(i)} \leftarrow \mathrm{Commit}(\mathrm{sk}_U; r_{U(i)})$.

(2) User U selects another random value $r_{(i)} \in \{0,1\}^\lambda$ and computes $\mathrm{com}_{(i)} \leftarrow \mathrm{COM}((\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}, r_U); r_{(i)})$.

(3) User U sends $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ to user V and receives $(T, \{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, from user V.

(4) User U verifies T and calculates $\mathrm{VER}(\mathrm{com}_{(k)}, \mathrm{chal}_{(k)}, \mathrm{res}_{(k)}, (\mathrm{pk}_{V(k)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash; otherwise, rejects it. Here, $\mathrm{chal}_{(k)} \leftarrow H(\mathrm{com}_{(k)})$ is the hash value of $\mathrm{com}_{(k)}$.

c. Transmission of electronic cash

A process user U sends electronic cash T to user W is as follows:

(1) User U receives $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)})$ from user W.

(2) User U calculates $\mathrm{chal}_{(i)} \leftarrow H(T, \mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)})$.

- $\mathrm{com}_{(i)}$ is generated by user U upon receiving T from user V (Step 2 of the protocol for receiving electronic cash).

(3) User U calculates $\mathrm{res}_{(i)} \leftarrow \mathrm{RES}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}, r_U), r_{(i)})$. The Σ protocol proves that $(\mathrm{pk}_{U(i)}, \mathrm{pk}_C)$ belong to the following language L, $L := \{(\mathrm{pk}_{U(i)}, \mathrm{pk}_C) | \exists (\mathrm{pk}_U, \mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}, r_U), \mathrm{Commit}(\mathrm{sk}_U; r_{U(i)}) = \mathrm{pk}_{U(i)} \wedge \mathrm{Commit}(\mathrm{sk}_U; r_U) = \mathrm{pk}_U \wedge \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U) = 1\}$.

(4) User U sends $(T, \{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.

(5) User W verifies T and calculates $\mathrm{VER}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, \mathrm{res}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C))$ for all $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash; otherwise, rejects it. Here, $\mathrm{chal}_{(i)} \leftarrow H(\mathrm{com}_{(i)})$ is the hash value of $\mathrm{com}_{(i)}$.

d. Detection of double spending

A process the service provider identifies the double-spend of electronic cash is as follows:

(1) If the serial number of the returned electronic cash T is not in the Issued Electronic Cash DB, the service provider determines that it has been double spent and retrieves T and its circulation record σ' with the same serial number from

the Redeemed Electronic Cash DB.
(2) The service provider computes $\mathrm{sk}_U \leftarrow \mathrm{Ext}(\mathrm{pk}_{U(i)}, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ based on the two transfer records σ and σ'.
(3) By inquiring with the certification authority, the service provider identifies the user associated with private key sk_U.

3. The method introduced in Section IV (Registering the public key with the certification authority and identifying double-spending users via the public key)
Detection of double spending in Methods 1 and 2 relies on exposing the private key that was fraudulently used to identify the user. However, since anyone who has the two electronic cash involved in double spending can expose the private key, there is a risk that the user who obtained the private key may conduct further fraudulent acts. In contrast, this method is characterized by the ability to identify the offending user solely through public information.

a. Initial setup
The certification authority and users prepare the key pairs and the certificates as follows:

(1) Certification authority C generates a pair of private and public keys, $(\mathrm{sk}_C, \mathrm{pk}_C) \leftarrow \mathrm{Gen}(1^\delta)$, and publishes them together with its self-signed certificate.
(2) User U generates a pair of private and public keys, $(\mathrm{sk}_U, \mathrm{pk}_U) \leftarrow \mathrm{Gen}(1^\delta)$.
(3) User U sends their public key pk_U to certification authority C, and receives certificate $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{pk}_U \| *)$ for pk_U.
(4) User U computes $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$, and accepts $(\mathrm{pk}_U, \mathrm{Cer}_U)$ if the result is 1, otherwise, rejects it.

b. Receipt of electronic cash
A process user U receives electronic cash T from user V is as follows:

(1) User U randomly selects a transaction-specific public key $\mathrm{pk}_{U(i)} \in \{0,1\}^\lambda$.
(2) User U computes $\mathrm{Cer}_{U(i)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(\mathrm{pk}_{U(i)})$.
(3) User U selects a random value $r_{(i)} \in \{0,1\}^\lambda$ and computes $\mathrm{com}_{(i)} \leftarrow \mathrm{COM}((\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{Cer}_{U(i)}, \mathrm{Cer}_U); r_{(i)})$.
(4) User U sends $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ to user V and receives $(T, \{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, from user V.
(5) User U verifies T and computes $\mathrm{VER}(\mathrm{com}_{(k)}, \mathrm{chal}_{(k)}, \mathrm{res}_{(k)}, (\mathrm{pk}_{V(k)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash, otherwise, rejects it.

c. Transmission of electronic cash
A process user U sends electronic cash T to user W is as follows:

(1) User U receives $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)})$ from user W.
(2) User U computes $\mathrm{chal}_{(i)} \leftarrow H(T, \mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)})$.
- $\mathrm{com}_{(i)}$ is generated by user U upon receiving the electronic cash T from user V (refer to Step 3 of the protocol for receiving electronic cash).

(3) User U computes $\mathrm{res}_{(i)} \leftarrow \mathrm{RES}(\mathrm{com}_{(i)},\ \mathrm{chal}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{Cer}_{U(i)}, \mathrm{Cer}_U))$. The Σ protocol proves that $(\mathrm{pk}_{U(i)}, \mathrm{pk}_C)$ belong to the following language L, $L \coloneqq \{(\mathrm{pk}_{U(i)}, \mathrm{pk}_C) \mid \exists(\mathrm{pk}_U, \mathrm{Cer}_{U(i)}, \mathrm{Cer}_U),\ \mathrm{Verify}_{\mathrm{pk}_U}(\mathrm{pk}_{U(i)}, \mathrm{Cer}_{U(i)}) = 1 \wedge \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U) = 1\}$.

(4) User U sends $(T, \{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.

(5) User W verifies T and computes $\mathrm{VER}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, \mathrm{res}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash, otherwise, rejects it.

d. Detection of double spending

A process the service provider identifies the double-spend of electronic cash is as follows:

(1) If the serial number of the returned electronic cash T is not in the Issued Electronic Cash DB, the service provider determines that it has been double spent and retrieves T and its circulation record σ' with the same serial number from the Redeemed Electronic Cash DB.

(2) The service provider computes $\mathrm{pk}_U \leftarrow \mathrm{Ext}(\mathrm{pk}_{U(i)}, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ from the two transaction records σ and σ'.

(3) By inquiring with the certification authority, the service provider identifies the user associated with public key pk_U.

Institute for Monetary and Economic Studies (IMES)

Bank of Japan, 2–1–1, Nihonbashi-Hongokucho,
Chuo-ku, Tokyo 103–8660, Japan
Phone: +81–3–3279–1111, Fax: +81–3–3510–1265
E-mail: imes.journals-info@boj.or.jp
URL: https://www.imes.boj.or.jp

IMES was founded in October 1982 as an internal organ of the Bank of Japan, in commemoration of the Bank's centennial. In carrying out its research activities, IMES benefits from the advice given by the Board of Councillors and Honorary Advisers from abroad.

✣ *Purpose* ✣

IMES conducts a wide range of studies on the theoretical, institutional, and historical aspects of monetary and economic issues with the aim of establishing an appropriate background for monetary policy. It functions as an important vehicle for the exchange of views with academic circles at home and abroad, and collects and provides the public with monetary and economic research. IMES has also tried to create both an atmosphere of enthusiasm for research and an environment conducive to informal discussions of prominent economic policy issues.

✣ *Councillors and Honorary Advisers* ✣

IMES invites distinguished Japanese and international scholars to assume the posts of Councillor and Honorary Adviser, which entail advising the Director-General of IMES on the institute's research activities and information exchange *vis-à-vis* academic circles.

✣ *Research Activities* ✣

IMES research is conducted in the following areas: theoretical and empirical analysis of monetary and economic issues; studies of legal, accounting and central banking issues; studies of information technology; and historical studies of monetary and economic issues and numismatics.

✣ *Conferences* ✣

IMES organizes domestic and international conferences; the latter, scheduled annually, is attended by central bankers, researchers from international institutions, and distinguished scholars from various countries. IMES also invites scholars and other professionals to lecture at the institute, and sponsors occasional symposiums.

✣ *Research Consignment* ✣

When in-depth study cannot be conducted at IMES due to limited materials or the highly specialized knowledge required, IMES consigns such study to scholars outside the institute.

✣ *Visiting Scholars* ✣

A special feature of IMES is its system of visiting scholars, which has led to significant interaction between Japanese and foreign researchers, and thereby stimulated the institute's research. Under the system, a visiting scholar conducts research at IMES and submits a written report. The main theme is chosen in consultation with the Director-General of IMES and should contribute to the better understanding of either domestic or international aspects of economic and financial issues in Japan. Interested researchers should write to the Head of Economic and Financial Studies Division, at IMES.

✣ *English Publications* ✣

IMES Discussion Paper Series: Working papers published on an *ad hoc* basis.
Monetary and Economic Studies: A journal published each year.
Proceedings of the international conferences:

- *Growth, Integration, and Monetary Policy in East Asia* (*Monetary and Economic Studies*, Vol. 25, No. S-1, 2007): This special issue considers a wide range of economic and financial topics in East Asian economies. Those topics include financial integration, accumulation of net foreign assets, economic growth, and monetary policy in the region.
- *Financial Markets and the Real Economy in a Low Interest Rate Environment* (*Monetary and Economic Studies*, Vol. 24, No. S-1, 2006): This special issue aims to deepen the understanding of the interaction between financial markets and the real economy in a low interest rate environment and learn lessons for the future conduct of monetary policy from the recent experiences of major advanced countries.
- *Incentive Mechanisms for Economic Policymakers* (*Monetary and Economic Studies*, Vol. 23, No. S-1, 2005): This special issue focuses on incentive mechanisms for economic policymakers in five areas: a monetary policy committee in a central bank, prudential policy, domestic financial markets, international financial markets, and fiscal policy.
- *Challenges for Sustained Economic Growth under Changing Economic, Social, and International Environments* (*Monetary and Economic Studies*, Vol. 22, No. S-1, 2004): This special issue focuses on how to achieve and promote sustained economic growth in the world economy, amid the considerable changes taking place in the economic, social, and international environments.
- *Exchange Rate Regimes in the 21st Century* (*Monetary and Economic Studies*, Vol. 20, No. S-1, 2002): This special issue discusses exchange rate regimes and the role of central banks in the 21st century, taking account of recent major changes, such as the launch of circulation of euro banknotes and coinage in 2002, an increased move toward dollarization in the Americas, and frequent currency crises in the emerging market economies since the latter half of the 1990s.

The Role of Monetary Policy under Low Inflation: Deflationary Shocks and Policy Responses (*Monetary and Economic Studies*, Vol. 19, No. S-1, 2001): This special issue investigates the role that monetary policy can and should play when there are defiationary shocks, such as the collapse of an asset price bubble occurring in an environment of low inflation.

Monetary Policy in a World of Knowledge-Based Growth, Quality Change and Uncertain Measurement (Palgrave, 2001): This book seeks optimal monetary policy in the world economy currently changing fundamentally by confronting a trend toward an increasingly conceptual and intangible form of output.

Towards More Effective Monetary Policy (Macmillan Press, 1997): This volume explores the operational and institutional framework for effective implementation of monetary policy against the background of recent developments in economics and central banking practice.

Financial Stability in a Changing Environment (Macmillan Press, 1995): This book reviews recent changes in the financial system and examines how to maintain financial stability, considering an optimal design of prudential policy and the role of central banks.

Price Stabilization in the 1990s: Domestic and International Policy Requirements (Macmillan Press, 1993): This book investigates various aspects of inflation: its recent history and sources; its measurement; the indicators of future inflation; and the policy implications to achieve and maintain price stability.

The Evolution of the International Monetary System: How Can Efficiency and Stability Be Attained? (University of Tokyo Press, 1990): This book examines the future course of the international monetary system, considering the background of financial globalization, as well as recent trade imbalances among major countries and declining confidence in the U.S. dollar.

Toward a World of Economic Stability: Optimal Monetary Framework and Policy (University of Tokyo Press, 1988): This book seeks to identify the causes of economic instability after 1973, including the large international payment imbalances among major industrialized countries in the 1980s, and discusses the development of an optimal monetary regime.

Financial Innovation and Monetary Policy: Asia and the West (University of Tokyo Press, 1986): This book investigates the background of recent financial innovation and the role it plays in the financial system and monetary policy.

Monetary Policy in Our Times (MIT Press, 1985): This book tackles a wide range of aspects of the theory and practice of monetary policy, such as its evaluation, role, and related issues.

✣ *Archives* ✣

The Archives opened in 2002 as a section within the IMES. The Archives serves as the official repository for the Bank's historical records. The Archives preserves the corporate memory of the Bank of Japan by acquiring, preserving, and making accessible records of continuing value that describe the Bank's origins, policies, interests, evolution, functions, and activities.

✣ *Currency Museum* ✣

IMES has been collecting and studying Japanese currencies dating from ancient times until today, as well as materials related to money. In the Currency Museum, visitors can view authentic Japanese coins, notes, and currency-materials. Some of the historical materials are publicly available mainly on the website.

Hours: 9:30–16:30 (no entry after 16:00).
Groups of more than 20 people are kindly requested to make reservations in advance.
Please check the latest information on our website before visiting.
Closed: Mondays (open when Monday is a holiday), January 1–4, and December 29–31.
Admission: Free.