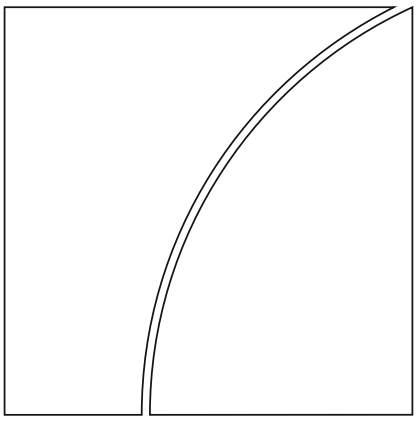

BIS Working Papers

No 1306

Big techs, credit, and digital money

by Markus K Brunnermeier and Jonathan Payne

Monetary and Economic Department

November 2025

JEL classification: E42, E51, G23, L51, O31.

Keywords: Ledgers, platform money, CBDC, currency competition, private currencies, industrial organisation of payments, platforms, big tech, trilemma.

BIS Working Papers are written by members of the Monetary and Economic Department of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the BIS or its member central banks.

This publication is available on the BIS website (www.bis.org).

ISSN 1020-0959 (print)
ISSN 1682-7678 (online)

Foreword

The 24th BIS Annual Conference took place in Basel, Switzerland on 27 June 2025. The event brought together a distinguished group of central bank Governors, leading academics and former public officials to exchange views on the theme "Central banking in times of digitalisation and fragmentation". The papers presented at the conference are released as BIS Working Papers, nos 1306 and 1307.

BIS Paper no 162 contains a speech by Agustín Carstens and remarks from two panel discussions, on "Perspectives on policymaking – a tribute to Agustín Carstens" and "Challenges for central banks in a changing world".

Contents

BigTechs, Credit, and Digital Money

Markus K. Brunnermeier and Jonathan Payne*

November 5, 2025

Abstract

This paper examines how digital payment ledgers operated by BigTech platforms and central banks can expand uncollateralized credit. However, policymakers face a trilemma—no system can simultaneously achieve efficient credit enforcement, limit rent extraction, and preserve user privacy. Monopolistic platforms enforce repayment but compromise privacy and extract rents; public or privacy-respecting ledgers protect users but weaken enforcement; platform co-opetition or programmable public ledgers balance enforcement and rents, but only by reducing privacy.

Keywords: Ledgers, platform money, CBDC, currency competition, private currencies, industrial organization of payments, platforms, Bigtech, trilemma.

*Brunnermeier: Princeton, Department of Economics, Bendheim Center for Finance, markus@princeton.edu. Payne: Princeton, Department of Economics, Bendheim Center for Finance, jepayne@princeton.edu. We are grateful Weiqi Chen and our discussants Maryam Farboodi and Christine Parlour. ChatGPT provided useful editing assistance.

1 Introduction

FinTech promises to overcome long-standing frictions that restrict access to the financial system. Proponents argue that new technologies—machine learning, big data analytics, and automated ledgers—can improve both credit screening and contract enforcement. In principle, these advancements could enable large-scale uncollateralized credit by moving payments, information collection, and contracting onto a shared digital ledger that controls financial flows and can automatically settle loans. This would significantly improve financial inclusion for individuals and businesses that lack sufficient collateral or credit histories to be able to take loans through the traditional banking system.

New technology alone is not enough, though. Private and public institutional arrangements need to ensure that agents have the right incentives to make the system work. A central weakness is the possibility of so-called *side trading*—even when contracts are recorded on a ledger, agents may transact off-ledger using cash or alternative anonymous channels. These side trades allow borrowers to avoid repayment and weaken the effectiveness of ledger-based enforcement. Other potential problems include the need for identity verification, the challenge of setting up and coordinating ledger adoption, and difficulties in standardizing and processing large-scale behavioral data. Without addressing these issues, FinTech cannot scale uncollateralized lending beyond niche or controlled environments.

Building on our academic work in Brunnermeier and Payne (2025), this paper analyzes two institutional responses to these challenges. The first is the emergence of a private BigTech platform that bundles trade and payment functions. Such a platform gathers detailed data on users, enforces contract repayment through closed payment systems, and restricts access to their trading environments. In doing so, it can turn future sales into a form of "digital collateral," thereby sustaining uncollateralized lending without traditional asset pledging. However, its market power also enables rent extraction via markups. Moreover, the viability of such a platform depends on scale: if a platform controls too small a share of trade, it cannot make exclusion costly enough to

deter default and may not find it profitable to operate a ledger at all.

A possible regulatory response to contain rent extraction is to encourage competition between multiple private platforms. However, without coordination, competing platforms may undermine each other's enforcement by allowing defaulting agents to side-trade across ledgers. This creates incentives to fragment information and weakens the viability of uncollateralized lending. We show that to sustain efficient credit markets, platforms must engage in selective cooperation—such as sharing default information and excluding intermediaries that harbor defaulters—while competing on trading and payment services. This requirement for "co-opetition" blurs the standard lines between market competition and regulatory coordination.

The second response is public provision of a programmable government-operated payment ledger. Such a public ledger could be offered as part of programmable central bank digital currency (CBDC). Its role could be to offer such a service to its citizens or simply act as an outside-option threat to limit a private platform's rent extraction and serve as a fallback in crises or cyberattacks. The effectiveness of a public ledger depends on design features such as accessibility, programmability, and integration with the broader financial ecosystem.

In addition to desired features to enhance enforcement of uncollateralized credit and limit rent extraction, digital payment systems raise deeper societal concerns about *privacy*. Who can see payment data, how it is used, and for what purposes are central questions in the design of digital money. Public ledgers that record every transaction may support better enforcement and reduce monopoly rents, but they risk creating surveillance infrastructures that compromise user anonymity. Conversely, privacy-preserving technologies—such as cryptographic techniques that obscure identities and transaction details—may protect users, but they reintroduce enforcement frictions by enabling side trading and default. Governments must also consider compliance with anti-money laundering (AML), know-your-customer (KYC), and tax reporting requirements, which often conflict with strong privacy guarantees. Balancing these concerns is one of the defining design challenges of digital

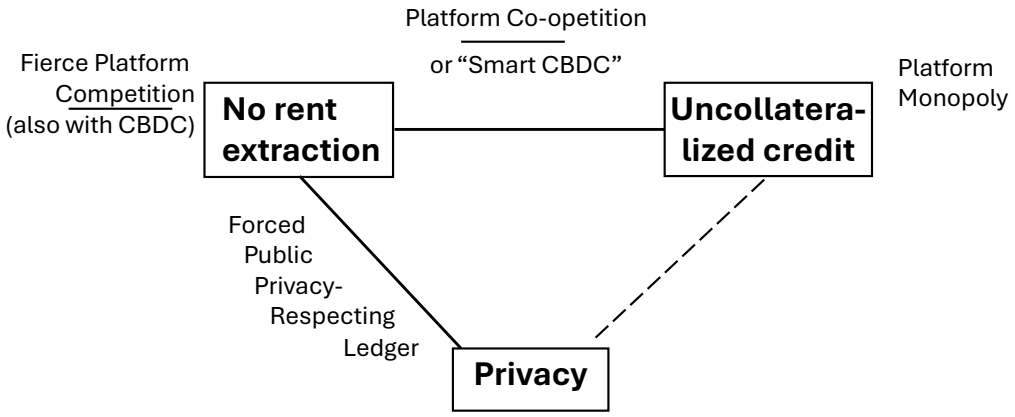

Figure 1: Policy Trilemma

monetary infrastructure.

These tensions crystallize in a fundamental *policy trilemma*: governments cannot simultaneously ensure uncollateralized credit access, minimize rent extraction by private intermediaries, and preserve user privacy. Each institutional arrangement makes trade-offs among these objectives. For example, a monopolistic BigTech platform may successfully enforce credit contracts through exclusion and data leverage, thereby supporting uncollateralized lending, but it does so by extracting rents and compromising user privacy. A privacy-respecting CBDC may protect individual anonymity and limit platform power, but it weakens enforcement, since side trades and defaults become harder to prevent. Meanwhile, appropriately regulated platform co-opetition or a smart, programmable CBDC operated by the central bank could combine efficient contract enforcement with limited rent extraction, but only at the cost of transactional privacy. As illustrated in Figure 1, each policy solution occupies a different vertex or edge of this trilemma, highlighting that no single design can achieve all goals at once. Navigating this constraint requires strategic prioritization and nuanced design choices that reflect societal preferences over privacy, market power, and financial inclusion.

These institutional and policy tensions are further amplified in the inter-

national context. Cross-border adoption of platform money or foreign CBDCs can erode national monetary sovereignty. Platforms operating across jurisdictions may control key components of domestic payment systems, limiting regulatory authority. A country risks losing control not only over the means of payment but also over its unit of account and its monetary transmission mechanism. These geopolitical stakes reinforce the need for strategic thinking in the design and regulation of digital money systems.

In this paper, we develop a conceptual framework to analyze the conditions under which private and public ledger systems emerge, the market structures they create, and the regulatory tools that can guide them toward efficient and equitable outcomes. Our focus is on the evolving industrial organization of money—where platforms, ledgers, enforcement, credit, and privacy intersect—and the trade-offs that define the digital future of finance.

Literature Review. Our paper directly builds on our academic papers Brunnermeier and Payne (2025), which shows that BigTech platforms can ensure uncollateralized credit by bundling the provision of trading and payment technologies, and Brunnermeier and Payne (2023), which focuses on how FinTechs and banks compete on information collection. It is also related to several branches of research. First, our research aligns with studies on how FinTech can increase uncollateralized debt capacity. Mandating ledger use effectively creates "digital collateral" that facilitates automated contracts, as explored in works like Garber et al. (2021), Kahn and van Oordt (2022), Frost et al. (2019), Gambacorta et al. (2023), and Cornelli et al. (2023). Empirical evidence from Liu et al. (2022) showcases the success of uncollateralized lending by BigTech firms in China. Rishabh and Schäublin (2021) observe that in India, borrowers' non-cash revenue decreased after fintech companies issued "digitally collateralized" loans, suggesting increased "cash side traders". Copestake et al. (2025) demonstrate the positive impacts of interoperability following the introduction of India's Unified Payment Interface. Parlour et al. (2022) study the impact of FinTech competition in payment services on banks' information collection and argue that this hurts bank-dependent borrowers.

Second, our analysis relates to the expanding field of digital tokens. We

are most closely aligned with research examining private tech platforms that offer centralized currencies, such as Chiu and Wong (2020), Chiu and Koeppel (2025), Cong et al. (2020), Ahnert et al. (2022), Auer et al. (2022), and Frost et al. (2025). Ozdenoren et al. (2025) focus on how platforms account for seigniorage income when determining markup charges, though their work does not delve into credit market implications. Other relevant literature includes studies on central bank digital currencies like Fernández-Villaverde et al. (2020), Keister and Sanches (2019), and Kahn et al. (2019), as well as decentralized, programmable cryptocurrencies, which are discussed in papers such as Fernández-Villaverde and Sanches (2018), Benigno et al. (2019), Abadi and Brunnermeier (2024), Schilling and Uhlig (2019), Cong et al. (2021), and Auer et al. (2025).

We structure the paper in the following way. Section 2 outlines the FinTech vision. The BigTech solution is provided in Section 3, the public option solution in Section 4. Section 5 examines how to best regulate co-opetition among competing BigTech platforms. Section 6 focuses on privacy consideration. Section 7 stresses the geopolitical challenges in an international context and concludes.

2 FinTech Vision for Lending and Payments

This section outlines a framework to explore—and critique—the "FinTech vision" of how new technologies for information processing and recordkeeping could transform payment and credit services.

Firms often require external credit to finance investments, purchase inputs, and begin production. At a high level, the lending process involves the following steps:

1. Savers assess the likelihood that the business will repay, based on its expected future revenue and assets;

2. Savers decide which loans to fund;

3. Businesses use the funds to produce goods;

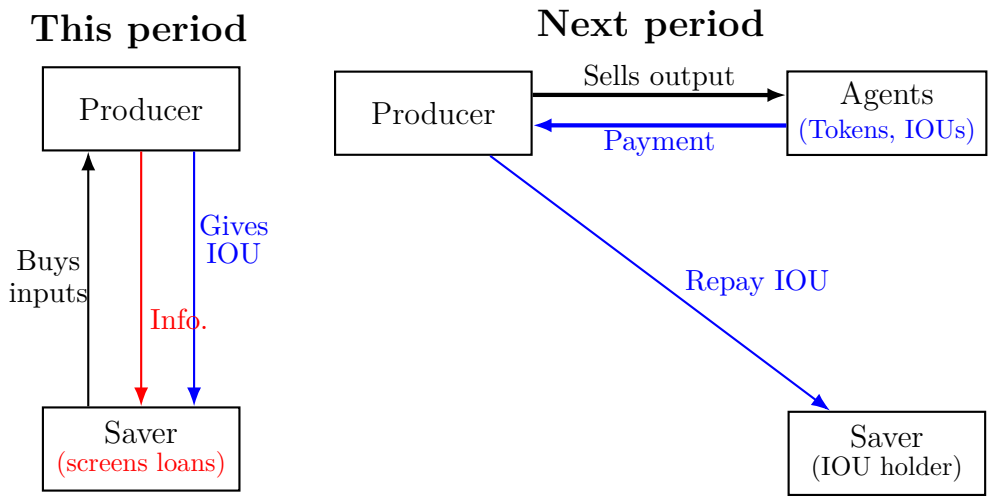

Figure 2: The loan process. The black lines depict the flow of goods. The blue lines depict the flow of financial contracts. The red lines depict the flow of information

4. Businesses sell output and generate revenue;

5. Loans are settled, either through repayment or default.

This process is depicted in Figure 2, where black arrows trace the flow of goods, blue arrows represent financial contracts (with "IOU" used generically to refer to loans), and red arrows denote the flow of information.

To make this process work at scale, savers must be able to screen out low-quality borrowers and enforce repayment from viable ones. Historically, in small communities, this was achieved informally through local knowledge and reputational enforcement. But at scale, personal monitoring breaks down. This led to a financial system centered on collateralized lending, where banks can assess and enforce contracts without needing personal familiarity. Collateral simplifies screening—since it involves standardized assets—and enables enforcement by allowing lenders to seize pledged assets in default.

However, collateralized lending excludes many worthy borrowers—especially new businesses, firms with thin margins, and those whose assets are intangible or illiquid. This leads to widespread credit underprovision and financial exclusion.

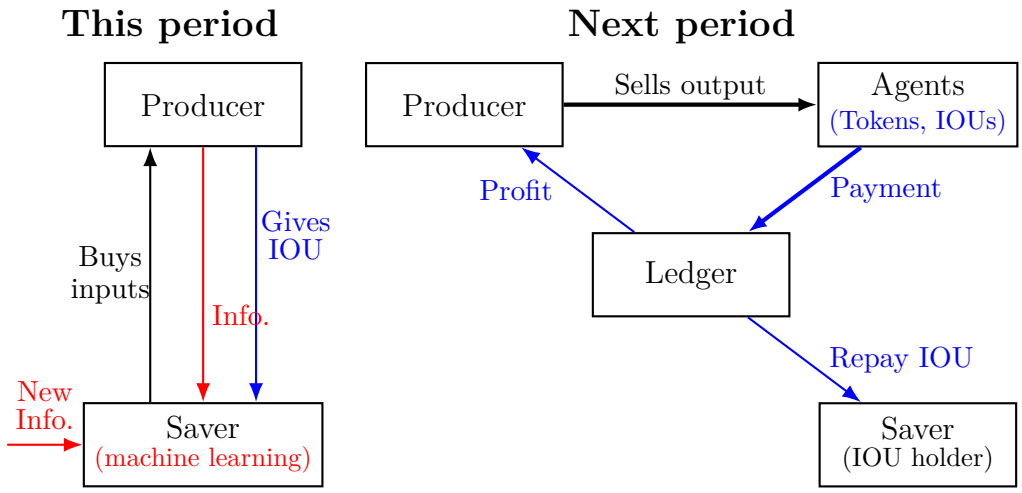

Figure 3: FinTech vision. Black depicts the flow of goods. Blue depicts the flow of financial contracts. Red depicts the flow of information

The FinTech vision seeks to address this by improving both screening and enforcement using new technologies. On the information side, FinTech firms gather large-scale behavioral datasets—so-called "soft" information—and use machine learning to identify creditworthy borrowers. On the contracting side, FinTechs propose using shared digital record keeping systems, or ledgers, that can automatically settle payments and enforce repayment. If all transactions are processed through such a ledger, loans can be repaid before the borrower has the chance to default. This vision is illustrated in Figure 3.

Various real-world attempts reflect components of this vision. Blockchain technologies such as Ethereum aim to move financial activity onto programmable ledgers. In China, platforms like Alibaba use behavioral data to screen borrowers and offer uncollateralized credit to previously unbanked customers. Brazil's Pix payment system facilitates digital settlement and may support contract enforcement. In India, FinTechs are experimenting with linking business revenue directly to loan repayment.

Despite these advances, technology alone has not been sufficient to transform credit provision. Institutional arrangements must also ensure that agents face the right incentives to make the system work. A key challenge is *side trading*: even if contracts are recorded on a ledger, agents may transact off-ledger

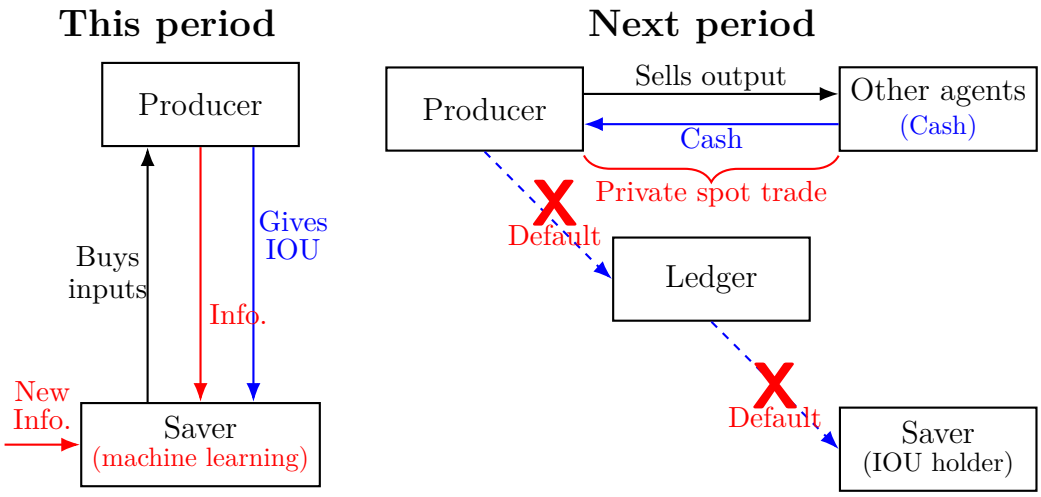

Figure 4: Problems with the FinTech vision.

using cash or anonymous methods, thereby avoiding repayment. Figure 4 illustrates this problem: savers who store cash rather than buy IOUs can offer unrecorded trades, enabling producers to default and still participate in the economy. These hidden trades undermine the ledger's enforcement function and ultimately destabilize uncollateralized lending.

In addition, there are other hurdles the FinTech vision must overcome. Ledger operators must verify user identities, build and coordinate ledger adoption, standardize data collection, and address cognitive or legal limits on information processing. They must also support efficient risk-sharing arrangements and guard against new forms of systemic risk.

The rest of the paper analyzes two institutional models that aim to overcome these barriers and unlock the potential of the FinTech vision: one based on a BigTech platform providing the payment ledger for the economy and another based on the public provision of a common ledger.

3 Response (I): BigTech Platforms

BigTech platforms have the opportunity to bundle the provision of trading and payment technologies. On the trading side, BigTech platforms offer improved

matching between buyers and sellers. On the payment side, they can set up their own ledger for settling financial transactions, creating currency tokens, and executing automatic contracts. As a real-world example, this can be thought of as Amazon or Alibaba offering a programmable ledger in the style of Ethereum. There are many potential synergies between the provision of these services.

One synergy arises because BigTech platforms can exploit "unconventional" information that banks, investment funds, and FinTech startups are unable to access and/or process. These platforms observe a large share of goods trade, enabling them to infer market characteristics such as customer product demand and supplier pricing power. They also collect granular data on individual purchasing habits, website activity, social media usage, and payment behavior. Unless other financial institutions contract with the platforms, they cannot access this information. This gives BigTech platforms the opportunity to exploit machine learning tools and use unconventional information to predict loan default. This is sometimes referred to as making "soft" information sufficiently "hard" to be used for providing financial services. A growing academic literature supports the value of such information: for example, Berg et al. (2020) shows that digital footprints can predict default risk as accurately as credit scores, and improve predictions when used alongside them.

Another synergy is that BigTech platforms can steer users toward their payment systems and discourage the use of cash. Platforms can require users to conduct transactions using their internal ledgers and tokens. In doing so, they create a "walled garden" that restricts off-platform payments. This makes it is hard for producers to sell goods anonymously using cash, default on their loan obligations, and then bring the cash back into the platform to make future purchases. By undermining the universal liquidity of cash, platforms reduce the incentive to hold it. Consequently, savers no longer hold the assets needed to facilitate private side trades, and all transactions are channeled through the platform's ledger, where loan repayments can be enforced automatically. This mechanism is depicted in Figure 5. Importantly, full market coverage is not necessary: since agents must choose their portfolio (cash versus tokens) before

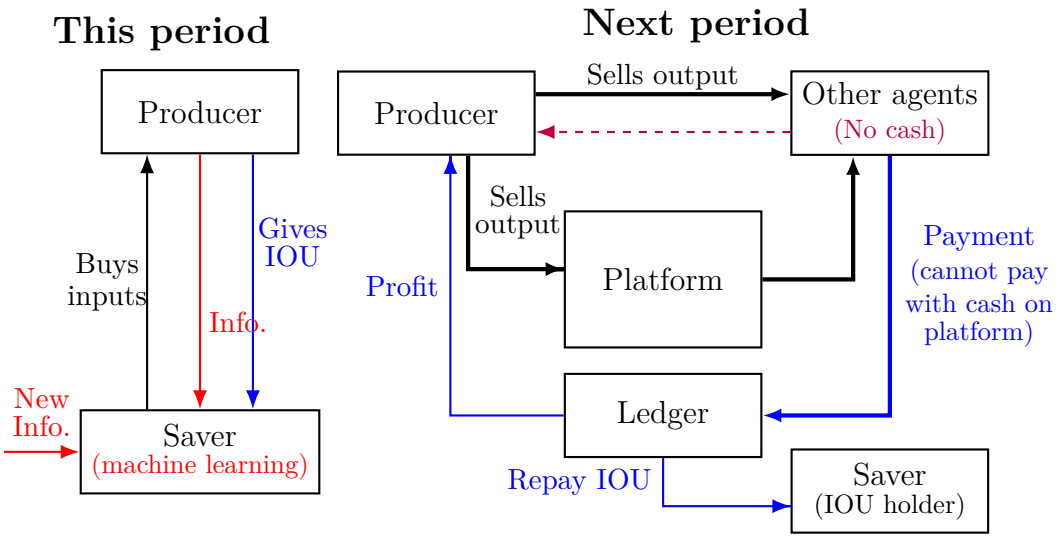

Figure 5: Lending with a platform. The black lines show the flow of goods. The red lines show information flow. The blue lines show the flow of financial assets.

knowing where they will trade, the platform can deter cash holding even when only a fraction of transactions go through the platform.

These insights yield three conceptual takeaways about digital payment ledgers:

(i) **BigTech platforms can "back" ledger use:** Ledger technologies are only effective if agents actually use them. Thus, platforms that control trade in the economy must also support ledger use by mandating it for participants. In this sense, BigTech platforms are natural providers of currency ledgers.

(ii) **BigTech platforms need to destroy the universal liquidity of cash:** Many credit enforcement problems arise when agents can use cash for side trades. Platforms can close off these opportunities by making cash impractical to use, thereby enhancing contract enforceability.

(iii) **The payment technology can collateralize sales revenue:** The method of payment affects whether future sales revenue can be treated as

collateral. Transactions conducted on a common ledger can be diverted to repay loans, functioning like "digital collateral." Off-ledger trades, by contrast, require costly coordination to monitor and exclude defaulters. Platforms can control how effectively future revenue becomes collateral by shaping where transactions occur.

The expansion of BigTech into finance introduces new challenges as well as new opportunities. One issue is the presence of natural monopolies in ledger-based services. For contract enforcement, platforms with greater market share can better enforce repayment, since more trades are routed through the ledger. For information collection, different institutions specialize in different types of data—BigTechs typically excel in trade-related data, while banks specialize in collateral evaluation. Without mechanisms for sharing information, this specialization leads institutions to target borrowers based on the characteristics they observe best, rather than efficiently allocating credit. These dynamics mean that monopoly BigTech platforms can allocate credit efficiently but can also use their market power to extract significant rents.

The inverse challenge is that platforms require some degree of market power in order to be willing to set up the platform. Their revenues come from charging markups on transactions. But these markups also affect incentives: platforms enforce repayment by discouraging cash usage, and excessive markups reduce the attractiveness of using the platform payment system and/or tokens. There is thus a trade-off: higher markups generate revenue but undermine enforcement by incentivizing cash use. A platform that controls a large share of trade can charge a positive markup while still discouraging default. In contrast, a smaller platform may need to subsidize users (i.e., charge negative markups) to enforce repayment, making ledger provision unprofitable. In this case, it prefers to not set up the common ledger.

In short, the extent of platform dominance—measured by the share of trade it intermediates—determines whether the economy suffers from monopoly rent extraction or credit fragility. These observations are reflected in the policy trilemma introduced in Figure 1 in the introduction. Without any regulation, the economy is likely to end up in the top right corner where a BigTech

monopoly provides uncollateralized credit but also extracts large rents. Without any market power, the economy is likely to end up in the top left corner where competition brings down rents but also discourages platforms from setting up the ledger. In principle, a regulator with perfect information could finely tune restrictions on platform markups to achieve both uncollateralized credit provision and low rents. However, doing so would require detailed knowledge of costs and demand. In the following sections, we consider alternative strategies: public provision of a payment ledger and regulated competition between large platforms.

4 Response (II): Public Option

The arguments in Section 3 suggest that payment ledger provision exhibits characteristics of a natural monopoly, and that directly regulating private ledger providers is complex. An alternative policy response is for government agencies, particularly the central bank, to introduce a public payment ledger that competes with or substitutes for commercial payment technologies.

Central banks face several key design decisions in setting up a public ledger. First, should the system be a pure payment infrastructure, or should it also involve the issuance of central bank liabilities? Second, should the government offer a user-facing interface, or just provide backend infrastructure for financial institutions? Third, should access be limited to the banking sector, or extended to other intermediaries? Fourth, should end-users be able to write programmable contracts onto the ledger?

We have seen many different forms of public ledgers (broadly defined to include all payment and settlement systems) that reflect different design choices:

- *FedNow*: in the United States is a real-time payment and settlement system accessible only to banks. It does not involve the issuance of currency and functions as backend infrastructure alongside the Automated Clearing House (ACH) network.

- *Pix*: in Brazil is a real-time payment system open to both banks and

non-bank intermediaries. Unlike FedNow, it includes a public-facing interface.

- *Central bank reserves*: are digital liabilities of the central bank, accessible only to banks.
- *Wholesale Central Bank Digital Currency (CBDC)*: refers to central bank digital currencies that are not accessible to the general public but may be used by non-bank financial institutions. These could be implemented by creating a new class of central bank reserves or by operating a central bank-run blockchain.
- *Retail CBDC*: is a digital central bank liability that can be held by the public.
- *"Smart" CBDC*: by which we mean a programmable version of retail CBDC, operated on a centralized blockchain, where users can write and execute "smart" contracts conditional on certain information recorded on the blockchain. This resembles a the functionality of cryptocurrency platforms like Ethereum but operated by the central bank.

A public ledger can play multiple important roles in the payment and contract system we described in Section 3. First, it offers a superior outside option to physical cash. This is especially true for publicly accessible systems like Pix. On the positive side, this means a public ledger can discipline markup-setting by BigTech platforms and banks, serving as a substitute for direct price regulation. However, it also provides an alternative means of payment that can facilitate side trades, potentially weakening enforcement. As we discuss later in Section 6 this creates complicated policy tradeoffs between improving contract enforcement and protecting privacy.

Second, a public ledger can act as a fallback in emergencies. For instance, in the event of a cyberattack, financial intermediaries could shift settlement operations to the public ledger. Likewise, during financial crises, if private settlement systems fail, the public ledger could maintain basic payment functionality.

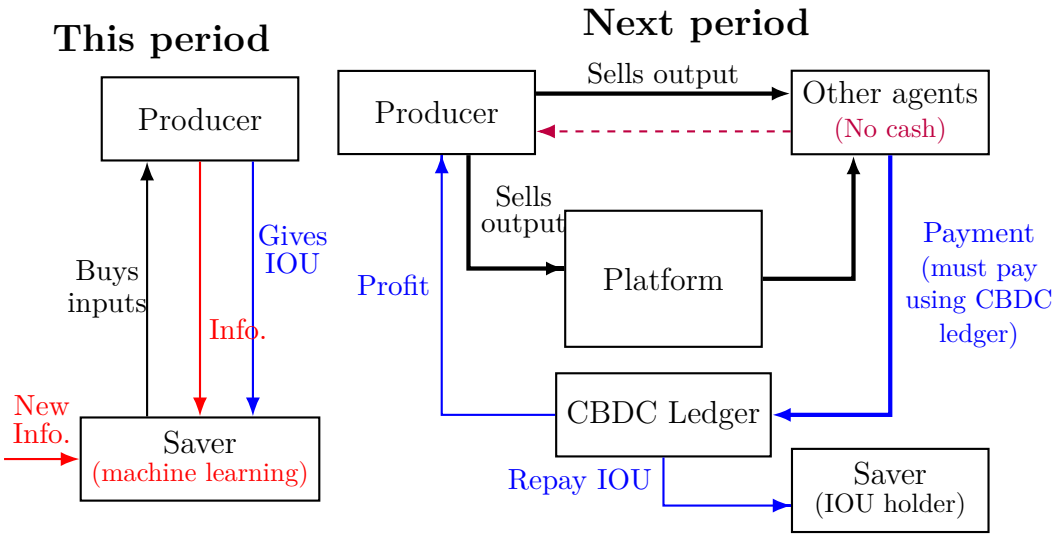

Figure 6: Smart CBDC Ledger (With Platform Competition).

Third, the central bank could offer a public ledger as the exclusive infrastructure for payment and contracting. For example, a smart CBDC could serve as the sole settlement medium in the economy, with physical cash phased out. In this scenario, all transactions would occur on the public ledger, making enforcement universal. This setup is depicted in Figure 6.

Across all these roles, policy makers must balance the benefits of system-wide coordination on the current technology with the need for continued innovation in new technology. Offering a universal public ledger may enhance enforcement and payment efficiency, but it also risks entrenching a government monopoly that could deter technological progress. In recent years, private competition has driven substantial innovation in payment and settlement technologies. Replacing this with a centralized system—no matter how well-designed—may suppress the next wave of advances.

5 BigTech Platforms Co-opetition Regulation

In Section 4 we discussed how the government can offer a public digital payment system alternative with the objective to limit the rent extraction of the

BigTech platform and provide a fallback option (e.g. in case of cyberattack). An alternative regulatory approach is to encourage the entrance of at least two competing BigTech platforms.

To do so, regulators have several potential tools at their disposal. More specifically, the government can: (i) limit markup charges for trading on the platform, (ii) regulate exchange rates between platform ledger tokens and other currencies and (iii) set rules for information collection and sharing. All these tools interaction and involve "co-opetition": fostering competition in some dimensions and encouraging cooperation in other dimensions.

Regulation can foster competition across platforms by eliminating lock-in and walled garden effects. (In Section 4 we discuss a competing public option). Information and interoperability regulation can have large implication on platform competition. For example, if customers "own" the information and can carry it across platforms, platforms' lock-in effects are reduced. This is analogous to the concept of "open banking" in the area of finance. "Open banking" grants agents the right to decide whether to pass on their information to other platform ledgers.

A second form of regulation concerns the exchange rate fees platforms charge when agents want to transfer tokens of one platform to tokens of a competing platform. Requiring interoperability across digital ledgers and ability to swap tokens easily, increases the competition across platforms.

Regulation should also enhance cooperation across compete BigTech ledger operators to ensure efficient credit extension. This concerns in particular information sharing rules. A regulatory environment that focuses exclusively on fostering competition leads to a setting where the BigTech ledgers offer agents an option to default on loans registered in the competing BigTech ledger. That is, like in the FinTech vision (discussed in Section 2) agents would be encouraged by the competing BigTech ledger to default on the other ledger and side-trade with it. As a consequence, the (uncollateralized) credit market would never get off the ground. In addition, the BigTech platforms should earn sufficient rent to make it worthwhile for them to set up credit ledger. Hence, competing BigTech ledgers have to coordinate to exclude financial interme-

diaries that allow clients to store wealth with them after the client defaulted on other intermediaries using the other platform ledger. This requires information sharing. In Brunnermeier and Payne (2025) we examine a setting in which platforms commit when setting up the ledgers ex-ante to exclude financial intermediaries who allow their depositors to default on contracts on the other ledger. The analysis reveals that when both competing platforms are sufficiently efficient in matching agents, then both platforms set up individual ledger tokens. In contrast, if one platform has strictly superior matching technology than the other one, then the former sets up a monopoly ledger (with its token) and the less efficient platform pays a fee for its clients to use the ledger services. Ultimately, it shows that the only viable ledger operators are those that also possess a platform trading technology. That is, there is a natural bundling between offering ledger and trading services. This implies that a stand-alone institution with no trading technology would never provide the ledger in equilibrium.

Overall, while minimizing rent extraction by the platform asks for fierce competition to minimize trading markups, exchange rate fees and information ownership, a functioning credit market requires coordination in credit enforcement. In particular, it requires an element of information sharing across lenders. Agents that default on one platform should not be allowed to transact and make payments in a competing platform. In other words, the welfare optimizing solution requires *co-opetition*. There is some similarity to traditional bank lending. Competition among banks should be fierce, but it is desirable to have coordination via credit bureaus to ensure a functioning credit market.

In any case efficient regulation calls for an integrated approach that integrates BigTech platform trading activities as well as ledger and payment activities.

6 Privacy Considerations

In this section, we now add an additional objective, privacy, which the government has to balance with achieving effective credit enforcement and minimizing

private sector rent extraction.

Historically, physical cash has allowed for private transactions, whereas digital money has generally lacked this feature. Commercial banks—and, indirectly, the government—can monitor bank accounts and other forms of digital bank money. Central banks track who holds reserves. Transactions on blockchains like Bitcoin are publicly recorded and permanently stored, making them non-private by design.

However, recent technical developments have made it possible to create private digital currencies. One approach relies on cryptographic techniques that enable users to send coins without revealing the recipient or transaction amount. Notable examples include zero-knowledge proofs and Pedersen commitments. In the cryptocurrency space, these methods have been implemented by Zerocash, which provides a privacy-preserving digital token.

Deciding whether to offer a private or non-private digital token is one of the most important design choices for a central bank digital currency (CBDC). On one hand, surveys show that many individuals and businesses value privacy.[1] On the other hand, enabling private transactions makes it difficult to meet other government objectives, including:

- **Anti-Money Laundering (AML)**: prohibits the use of financial transactions to conceal the origins of criminal proceeds.
- **Countering the Financing of Terrorism (CFT)**: prohibits the use of financial transactions to fund terrorist activity.
- **Know Your Customer (KYC)**: requires financial institutions to verify the identities of their clients.
- **Anti-Evasion (AE)**: prohibits structuring or other efforts to circumvent reporting requirements.

For example, if the government issued a CBDC in the form of a USD eToken using zero-knowledge proofs to ensure privacy, it would not satisfy AML, CFT,

[1] See Chen et al. (2023), Armantier et al. (2024).

KYC, or AE requirements—much like physical cash does not. Conversely, if the government were to allow anyone to hold an account at the Federal Reserve provided they supply a Social Security number, it would satisfy all of these regulatory requirements but would not preserve user privacy.

The introduction of BigTech platform ledgers provides another reason why privacy poses challenges in the economy. The government must be careful not to offer a public payment option that inadvertently reintroduces private spot trade. A privacy-respecting public payment ledger effectively creates a universally liquid payment technology that does not require agents to hold endowment goods in advance. As a result, agents can always engage in side trades and default on their obligations. By contrast, if the government abandons privacy protections and uses the CBDC ledger to enforce contracts, it can expand access to uncollateralized credit directly. This creates another trade-off: while a public payment ledger that respects privacy can improve the functioning of the payment system, it may also undermine the ability to enforce contracts efficiently.

These observations bring us back to the trade-offs illustrated in Figure 1. A universal programmable CBDC can achieve the two outcomes at the top of the triangle: low rents and uncollateralized credit. A CBDC that respects privacy can deliver the outcomes on the left side of the triangle: low rents and privacy. However, no public ledger can simultaneously maximize uncollateralized credit expansion, minimize rent extraction, and protect privacy. Instead, the government must decide which objectives it wants to prioritize.

Many proposals have been put forward to create hybrid systems that incorporate some form of privacy protection while balancing the trade-offs in the policy trilemma:

1. **Regulating the Interaction with the Financial System.** This proposal envisions a CBDC eToken that uses zero-knowledge proofs to preserve privacy. Agents would be allowed to trade USD eTokens privately with one another. However, AML, CFT, KYC, and AE regulations would apply when agents move CBDCs into the broader financial system (e.g., to purchase financial assets). This approach effectively mirrors how

cash is treated in the current system.

2. **Anonymity Vouchers (ECB 2019 Proposal).** Users provide their identity to the central bank (or an intermediary implementing the CBDC) and receive a pseudonymous identity, which serves as their CBDC network address. They are also granted limited, non-transferable "anonymity vouchers," which allow them to transfer a specific amount of CBDC within a given timeframe without regulatory oversight of transaction data.

3. **Third-Party Authentication.** Users obtain wallet addresses after undergoing an electronic KYC assessment conducted by an approved third-party authenticator. End-users are not anonymous if a homomorphically encrypted AML process triggers compliance flags, or if a court order requires disclosure of information. In addition, wallet balances are subject to upper limits.

4. **Asymmetric Privacy.** In this CBDC design, the privacy of consumers (senders of money) is maximally protected, while the privacy of merchants (receivers of money) is less protected, (i.e. Tinn (2024)).

7 Geopolitical Considerations

The problem of credit provision is even more acute for international financial arrangements that stretch across different legal jurisdictions because information collection is more difficult and foreign collateral is harder to seize. This paper's arguments might suggest that a multinational BigTech platform's ledger or the global adoption of a government's digital ledger could be optimal solutions. Yet, a fundamental trade-off arises: an economically efficient cross-border BigTech ledger, while beneficial, risks a country's loss of sovereignty.

Relinquishing control over a country's payment system means surrendering a strategically vital economic component. Control of this system represents a crucial economic choke point, as shutting it down—to borrow Lenin's term,

a "commanding height of the economy"—would effectively paralyze both the financial system and the broader economy. A nation's sovereignty is compromised if a foreign power controls its payment system. This makes the country vulnerable, as it essentially grants the controlling platform—or implicitly, the platform's governing authority—the ability to impose sanctions.

Foreign BigTech companies can act as Trojan horses, providing a means to penetrate and control another country's payment system. Given that most BigTech platforms operate globally, their ledger tokens extend beyond national boundaries. This leads to the emergence of new "digital currency areas" (as described by Brunnermeier et al. (2019)) that are not confined by country borders.

A government risks losing control not only of its payment system but also of its unit of account, a process often called "dollarization" or "euroization". This means transactions shift from local to foreign currency, rendering the domestic currency no longer the settlement asset. Consequently, the nation suffers a loss of monetary sovereignty, as its monetary policy loses the ability to influence the macroeconomy. Crucially, a BigTech company's control over the payment system significantly simplifies the switch to an alternative unit of account. Therefore, countries may be concerned that allowing foreign BigTech companies to manage their payment systems could ultimately result in the loss of their local unit of account.

The rising popularity of stablecoins, often pegged to the US Dollar, also poses a risk to a country's local unit of account and, consequently, its monetary authority. However, smart regulation of stablecoins can at least ensure that the underlying settlement assets meet crucial safety standards, such as full backing with stable assets.

Many countries view a Central Bank Digital Currency (CBDC) as a defensive measure to prevent losing control over their payment system or even their unit of account. For this to work, the CBDC must be attractive not only for transactions but also as a store of value.

Overall, the main geopolitical challenge for governments is to integrate into international financial systems without sacrificing control over their payment

system or unit of account.

8 Conclusion

The emergence of digital payment ledgers presents a transformative opportunity to expand access to uncollateralized credit, but it also introduces deep trade-offs at the heart of modern financial design. No institutional arrangement can simultaneously achieve efficient enforcement, limit rent extraction, and safeguard user privacy. Whether ledgers are operated by monopolistic BigTech platforms, public central banks, or co-opetitive ecosystems, each approach resolves some dimensions of the trilemma in Figure 1 while compromising others. These tensions are further heightened by geopolitical considerations, as global platforms and foreign CBDCs threaten national monetary sovereignty. Navigating these challenges requires a careful balancing of objectives and a strategic blend of regulation, innovation, and institutional design.

References

Abadi, J. and Brunnermeier, M. (2024). Blockchain economics. Technical report, National Bureau of Economic Research.

Ahnert, T., Hoffmann, P., and Monet, C. (2022). The digital economy, privacy, and CBDC.

Armantier, O., Doerr, S., Frost, J., Fuster, A., and Shue, K. (2024). Nothing to hide? gender and age differences in willingness to share data. *Gender and age differences in willingness to share data (April 26, 2024). Swiss Finance Institute Research Paper*, (24-99).

Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., and Shin, H. S. (2022). Central bank digital currencies: motives, economic implications, and the research frontier. *Annual review of economics*, 14(1):697–721.

Auer, R., Monnet, C., and Shin, H. S. (2025). Distributed ledgers and the governance of money. *Journal of Financial Economics*, 167:104026.

Benigno, P., Schilling, L. M., and Uhlig, H. (2019). Cryptocurrencies, currency

competition, and the impossible trinity. Technical report, National Bureau of Economic Research.

Berg, T., Burg, V., Gombović, A., and Puri, M. (2020). On the rise of fintechs: Credit scoring using digital footprints. *The Review of Financial Studies*, 33(7):2845–2897.

Brunnermeier, M. and Payne, J. (2023). Platform, ledgers, and interoperability. *Princeton Working Paper*.

Brunnermeier, M. and Payne, J. (2025). Strategic money and credit ledgers. *Princeton Working Paper*.

Brunnermeier, M. K., James, H., and Landau, J.-P. (2019). Digital currency areas. Technical report, VoxEU Article.

Chen, S., Doerr, S., Frost, J., Gambacorta, L., and Shin, H. S. (2023). The fintech gender gap. *Journal of Financial Intermediation*, 54:101026.

Chiu, J. and Koeppel, T. (2025). Platform-based digital currencies.

Chiu, J. and Wong, R. (2020). Payments on digital platforms: Resilience, interoperability and welfare.

Cong, L. W., Li, Y., and Wang, N. (2020). Token-based platform finance. *Fisher College of Business Working Paper*, (2019-03):028.

Cong, L. W., Li, Y., and Wang, N. (2021). Tokenomics: Dynamic adoption and valuation. *The Review of Financial Studies*, 34(3):1105–1155.

Copestake, A., Kirti, D., Peria, M. S. M., and Zeng, Y. (2025). Integrating fragmented networks: The value of interoperability in money and payments.

Cornelli, G., Frost, J., Gambacorta, L., Rau, P. R., Wardrop, R., and Ziegler, T. (2023). Fintech and big tech credit: Drivers of the growth of digital lending. *Journal of Banking & Finance*, 148:106742.

Fernández-Villaverde, J., Sanches, D., Schilling, L., and Uhlig, H. (2020). Central bank digital currency: Central banking for all? Technical report, National Bureau of Economic Research.

Fernández-Villaverde, J. and Sanches, D. R. (2018). On the economics of digital currencies.

Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., and Zbinden, P. (2019). Bigtech and the changing structure of financial intermediation. *Economic policy*, 34(100):761–799.

Frost, J., Rochet, J.-C., Shin, H. S., and Verdier, M. (2025). Competing digital monies.

Gambacorta, L., Huang, Y., Li, Z., Qiu, H., and Chen, S. (2023). Data versus collateral. *Review of Finance*, 27(2):369–398.

Garber, P., Green, B., and Wolfram, C. (2021). Digital collateral. (28724).

Kahn, C. and van Oordt, M. R. (2022). The demand for programmable payments. Technical report, http://dx.doi.org/10.2139/ssrn.4218966.

Kahn, C. M., Rivadeneyra, F., and Wong, T.-N. (2019). Should the central bank issue e-money? *Money*, pages 01–18.

Keister, T. and Sanches, D. R. (2019). Should central banks issue digital currency?

Liu, L., Lu, G., and Xiong, W. (2022). The big tech lending model. (30160).

Ozdenoren, E., Tian, Y., and Yuan, K. (2025). Platform money.

Parlour, C. A., Rajan, U., and Zhu, H. (2022). When fintech competes for payment flows. *The Review of Financial Studies*, 35(11):4985–5024.

Rishabh, K. and Schäublin, J. (2021). Payment fintechs and debt enforcement.

Schilling, L. and Uhlig, H. (2019). Some simple bitcoin economics. *Journal of Monetary Economics*, 106:16–26.

Tinn, K. (2024). A theory model of digital currency with asymmetric privacy. *Available at SSRN 4891933*.

Discussion:
BigTechs, Credit, and Digital Money

Markus Brunnermeier & Jonathan Payne

Maryam Farboodi
MIT
BIS 24th Annual Conference, June 2025

Thank you for the opportunity to discuss this thought-provoking paper on the adoption of digital technologies in credit markets–one of the most pressing issues in contemporary financial regulation.

Summery of the paper Only in the past few years has there been a surge in the broad adoption of advanced digital technologies in financial services. The fintech industry–the business ecosystem that builds, sells, and operates technology-enabled financial services–has rapidly developed to cover multiple segments, including payments, banking and deposits, investing and wealth management, insurance, and crypto.

This paper focuses on the widespread adoption of digital ledgers among payment platforms and argues that policymakers face a trilemma in regulating this segment effectively:

- First, the hope is that payment ledgers improve the availability of credit by enabling efficient enforcement, thus, enhancing extension of uncollaterialized credit.
- Second, we want to achieve this outcome while sustaining a high degree of competition, so platforms do not engage in rent extraction.
- Third, it is crucial for consumer privacy to be preserved while obtaining credit.

The authors suggest that a vision of uncollateralized lending via a centralized ledger (as proposed by some fintechs) suffers from side trades and is not self-sustaining, and they propose three (partial) remedies: First, private platforms provided by BigTech solve the first and third problems, but they are prone to rent extraction. Second, a public option such as a CBDC uses a public ledger that preserves consumer privacy and avoids rent seeking, but it cannot credibly guarantee efficient enforcement. Third, in a hybrid "co-opetition" approach among more than two platforms, competition keeps markups low while coordination and information sharing prevent defaulting consumers from using the ledger in the future, thus ensuring contract enforcement. However, the information-sharing requirement violates consumer privacy.

This is an interesting proposal. Naturally, it raises several questions in the context of the most recent advances in digital technology, information-sharing, and payment regulation.

Background It is useful to view these changes in financial technology through the lens of economic logic and the antecedent progress in digital technologies.

On the computer-science side, *cryptography* took center stage during World Wars I and II, followed by the rise of personal computers and digital encryption in the 1970s. *Distributed systems* emerged in the 1980s, enabling more precise and efficient data collection and computation using distributed resources. Over the past two decades, we have witnessed the rapid development of blockchain technology, which leverages cryptography in a distributed ledger to establish a fully decentralized sequence of verifiable events. As such, blockchain is a direct application of computer-science advances to financial-market infrastructure.

To regulate this new technology effectively, it is crucial to understand whether it can be used to overcome two longstanding frictions in credit markets–information asymmetry and contract enforcement. If this technology enables financial institutions to attenuate these frictions, they can actively engage in uncollateralized lending, thereby improving financial inclusion.

Turning to economics: from Industrial Organization, we know that firms have incentives to provide multiple complementary products and services because *bundling* improves their competitive position in attracting consumers. Furthermore, International Economics has thought us that a credible threat of exclusion from financial markets facilitates *contract enforcement* and helps prevent sovereign default. Finally, the Great Financial Crisis of 2007-08 highlighted the value of *netting* obligations to prevent cascades of defaults among financial in-

stitutions, leading to the rise of central clearing parties (CCPs).

These insights strengthens the case for adopting digital ledgers in financial markets. Borrowing and (re)payments can be recorded on-ledger, enabling financial institutions to bundle products and services. The credible threat of exclusion from the ledger reinforces contract enforcement. And a digital ledger can be used for netting payments, resembling the functionality of CCPs in traditional markets. The authors argue that despite these advantages, three challenges remain difficult to address jointly with this technology: (1) efficient enforcement, (2) preventing rent seeking, and (3) user privacy.

In the rest of these comments, I first review recent advances in cryptography that may help address the trilemma. I then provide evidence from a real-world setting on the impact of adopting digital technologies on financial inclusion.

Decentralized verification without privacy violation Zero-knowledge proofs (ZKPs) are used in distributed systems to enhance privacy and security by allowing a party to prove the truth of a statement without revealing any underlying information. Applications include private transactions on blockchains, secure and anonymous identity management, and anonymous verification of jurisdiction.

For instance, Figure 1 depicts anonymous verification of specific attributes (such as being over a certain age or the issuing jurisdiction) as a core privacy feature of using a digital driver's license or ID in Apple Wallet. Using this technology on a distributed ledger *commoditizes* verification and eliminates the need for off-chain verification, enhancing consumer privacy. This, in turn, expands the scope for a wide range of stablecoins to coexist and engage in joint contract enforcement without violating consumer privacy.

Moreover, the "GENIUS Act" (Guiding and Establishing National Innovation for U.S. Stablecoins Act) was signed into law in 2025 as the first federal regulatory framework for payment stablecoins. It aims to provide regulatory clarity, protect consumers, and prevent illicit activity by requiring stablecoin issuers to be regulated. The law further commoditizes blockchain by enforcing compatibility and interoperability among stablecoins and the public blockchain. By doing so, it incentivizes third parties to develop a new ecosystem. As with other waves of innovation, it is reasonable to assume that monopoly rents may be necessary to sustain innovation.

However, concentrated market power can emerge even in environments designed for robust competition (such as cryptocurrencies), potentially harming

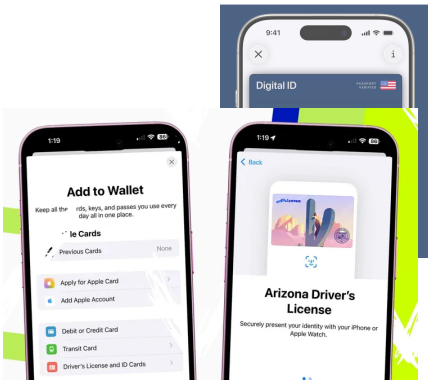

Figure 1: Anonymous identity verification without privacy violation

consumer welfare. Azar et al. (2025) document a high degree of concentration in the Ethereum production network and provides causal evidence of information rents. Thus, it is crucial to consider the economic trade-offs when regulating this novel technology.

Credit market in Brazil: Pix + Open Banking Brazil has been at the forefront of incorporating digital technologies into financial services. More than 75% of the Brazilian population uses Pix. Furthermore, Open Banking is enforced by the Central Bank of Brazil (BCB) through a combination of regulations, mandatory participation rules, and standardized API specifications.

Breza et al. (2025) document preliminary evidence on the impact of Open Banking adoption by banks on credit extension to small businesses. Their sample includes more than 18 million observations of loans extended by the largest lenders to retail borrowers during 2017-2024. They compare unsecured and super-secure loans within banks to estimate the impact. The underlying assumption is that super-secure loans have a fiduciary lien that makes repossession straightforward in the event of default; as such, they are information-insensitive and thus unaffected by Open Banking.

They show that the adoption of Open Banking by the banking sector does not significantly change the total amount of credit extended. However, it is associated with a redistribution of credit: more retailers borrow from each bank, but each borrows a smaller amount.

This redistribution raises the question of who the new borrowers are and whether Open Banking provides access to customers who have been tradition-

ally excluded from the market. To address this, Breza et al. (2025) examine whether borrowers are new or existing customers of the bank. They find no evidence of financial inclusion and show that the redistribution of credit is limited to existing customers.

Existing theoretical work provides some intuition for the counter-intuitive empirical finding that Open Banking does not necessarily improve credit access for the under-served. Farboodi et al. (2025) theoretically analyze redistribution under mandatory data-sharing policies such as Open Banking and show that these policies can harm financial inclusion. The customers who benefit are predominantly those whose data already reside within the financial sector–that is, customers who already have access to good financial products and services, which then improve further when banks adopt Open Banking. By contrast, the cheap availability of data on these customers reduces banks' already low incentives to acquire information about the under-served, thereby harming inclusion.

To conclude, we are facing a wave of technological progress that interacts strongly with incentives, unfolding at an unusually rapid pace. Optimal adoption and effective policy design are far from obvious. Economists should stay informed about the frontier of innovation and accelerate assessment of the impact of these technologies' adoption. This will enable us to provide timely input to computer scientists and help guide the direction of future innovation.

References

Azar, Pablo D, Adrian Casillas, and Maryam Farboodi, "Natural Centralization in Decentralized Finance," Working Paper 2025. 4

Breza, Emily, Bernardus Van Doornik, Maryam Farboosi, Dimas Fazio, and Janis Skrastins, "Open banking and credit allocation," Working Paper 2025. 4, 5

Farboodi, Maryam, Peter Kondor, and Pablo Kurlat, "Equilibrium Spillover of Big Data," Working Paper 2025. 5

Comments on BigTechs, Credit and Digital Money[1]
Policy Paper by Markus K. Brunnermeier and Jonathan Payne

This policy paper presents an economic framework to address an interesting and topical set of issues and speculates on how technology will change uncollateralized lending. It is important to recognize that as production shifts from brick and mortar factories to more knowledge-based industries, the ability to obtain funding against non-traditional, and also illiquid assets will be increasingly important – both to fund new business models and to provide backing for borrowers who do not have wealth or physical assets, just good ideas.

In this world, any rational lender is concerned with the ability of the borrower to repay. There are two ways to think about why borrowers might be credit risks. First, some borrowers are chronically late or never repay. These bad credit types can typically be identified by sifting through their credit histories, i.e., by processing information. Second, some borrowers are hit by adverse shocks, or unexpectedly develop different priorities. In order to ensure that such borrowers repay, lenders would be well served if they have some method to enforce repayment, such as by having access to the borrower's cashflows.

The authors posit that there are two potential solutions to these frictions. The first is an economy that is dominated by BigTech platforms. If all business is conducted on such platforms then uncollateralized lending is easier because future sales can be used as collateral and making enforcing repayment much easier. Of course, BigTech platforms are not a panacea as they wield tremendous monopoly power, which in and of itself constitutes an economic distortion. Additionally, if all transactions occur on a BigTech platform, they have effectively created a closed playment system. The second approach is for regulators to establish and operate a government ledger as a utility. Anyone could participate on such a ledger and exchange value with a common central bank digital currency (CBDC). While efficient, such a common, transparent system would remove the veil of privacy from transactions.

This paper and the proposed solutions are forward looking. Toe evaluate them, it is useful to consider the economic assumptions on which these solutions are built and then armed with these to speculate on other possible ways in which unsecured credit might be extended. In the authors' framework, data are ephemeral and are not portable, i.e, they cannot be credibly stored and reported. Thus, the world is one without credit registries or transaction

[1] Comments by Christine Parlour, Sylvan C Coleman Chair of Finance and Accounting University of California, Berkeley, Haas School of Business

histories. Additionally, in the authors' framework, transactions are settled and consumed instantaneously. That is, there are no invoice goods or relationships that are long lasting both for the consumer (no durable goods) and the producer. I'll consider these assumptions, and evaluate possible solutions or examples where they do not obtain.

There is a role for regulators in a world in which transaction data are currently ephemera. In the authors' framework, this gives generates market power to BigTech platforms. Indeed, if the only person who has concrete proof that a transaction has occurred is the transaction processor, they have a wealth of credit sensitive information. One approach that a regulator could take to the quality of data and the processors' natural monopoly power would be to find a way to make information about transactions a commodity. Such a solution would require carefully deciding who should have property rights over the information, but as a first step making the information portable is a way to solve the monopoly processor problem.

What about settlement delays? The authors' framework does not give them flexibility to address some implications. In the real world, there is typically a lag between contract and settlement and in the real world, there is a vibrant factoring market in which effectively, future sales are digital collateral. In as much as this market allows firms to borrow from their future success, a useful government response would be to make factoring as easy as possible by ensuring that recipts are standardized, and contracts enforced so future sales can in fact, be used as effective collateral for firms. It is interesting to note that future consumption is also used to discipline buyers. For example, PayGo lockout technology used for Solar Panels in East Africa or similar schemes used in mobile phone contracts. If future consumption benefits are used to ensure repayment on the part of consumers there is definitely a role for government to play to ensure that consumers are not exploited, i.e., that there are switching options. These examples for both firms and consumers suggest that there are examples in which creative government engagement can be used to facilitate markets that are backed by future sales or consumption.

Now, consider the authors' vision of a BigTech platform with private money. What do recent developments suggest about the possibilities of a "walled garden." The private sector has experimented with various versions. Concretely, products such as JPMCoin have been successful partially because they are effectively an internal messaging system. By contrast, if the enabling legislation of the US GENIUS act leads to a plethora of stablecoins

all backed by the same high quality liquid assets, then one could envisage either regulators or the private sector enabling highly swap markets. In such a scenario, although privately issued, such payment means would readily mutually exchangeable, and also exchangeable for fiat. In such a future, private monies would not be "walled."

A final reflection, on peering into the future, is the thought that any future payment platform, be it private or governmental requires significant resources. The Brazilian instant payment system, Pix has been remarkable successful, but probably only possible with the direction of the central bank. In other jurisdictions, the government/regulators have either mandated interoperability of private systems such as the Singaporean universal QR code, or the set of principles embodied in the India Stack. Of course, sufficiently concentrated private markets have also enabled new payment rails (such as Swish). These examples suggest that neither solely private or solely public solutions are inevitable.

Ultimately, we are uncertain what the future holds. It is therefore incumbent on regulators to reflect on the most important economic frictions that we know affect credit worthiness, and develop an appropriate regulatory response.

Previous volumes in this series

1305 November 2025	The asymmetric and heterogeneous pass-through of input prices to firms' expectations and decisions	Fiorella De Fiore, Marco Jacopo Lombardi and Giacomo Mangiante
1304 November 2025	The life experience of central bankers and monetary policy decisions: a cross-country dataset	Carlos Madeira
1303 November 2025	FX debt and optimal exchange rate hedging	Laura Alfaro, Julián Caballero and Bryan Hardy
1302 November 2025	Consumer preferences for a digital euro: insights from a discrete choice experiment in Austria	Helmut Elsinger, Helmut Stix and Martin Summer
1301 November 2025	Competing digital monies	Jon Frost, Jean-Charles Rochet, Hyun Song Shin and Marianne Verdier
1300 October 2025	The aggregate costs of uninsurable business risk	Corina Boar, Denis Gorea and Virgiliu Midrigan
1299 October 2025	Mapping the space of central bankers' ideas	Taejin Park, Fernando Perez-Cruz and Hyun Song Shin
1298 October 2025	Exploring household adoption and usage of generative AI: new evidence from Italy	Leonardo Gambacorta, Tullio Jappelli and Tommaso Oliviero
1297 October 2025	The BIS multisector model: a multi-country environment for macroeconomic analysis	Matthias Burgert, Giulio Cornelli, Burcu Erik, Benoit Mojon, Daniel Rees and Matthias Rottner
1296 October 2025	Predicting the payment preference for CBDC: a discrete choice experiment	Syngjoo Choi, Bongseop Kim, Young-Sik Kim, Ohik Kwon and Soeun Park
1295 October 2025	Pricing in fast payments: a practical and theoretical overview	José Aurazo, Holti Banka, Guillermo Galicia, Nilima Ramteke, Vatsala Shreeti and Kiyotaka Tanaka
1294 October 2025	Parsing the pulse: decomposing macroeconomic sentiment with LLMs	Byeungchun Kwon, Taejin Park, Phurichai Rungcharoenkitkul and Frank Smets
1293 October 2025	International risk sharing and wealth allocation with higher order cumulants	Giancarlo Corsetti, Anna Lipińska and Giovanni Lombardo

All volumes are available on our website www.bis.org.