Ho, Annetta; Darbha, Sriram; Gorelkina, Yuliya; García, Alejandro

Working Paper

The relative benefits and risks of stablecoins as a means of payment: A case study perspective

Bank of Canada Staff Discussion Paper, No. 2022-21

Provided in Cooperation with:
Bank of Canada, Ottawa

Suggested Citation: Ho, Annetta; Darbha, Sriram; Gorelkina, Yuliya; García, Alejandro (2022) : The relative benefits and risks of stablecoins as a means of payment: A case study perspective, Bank of Canada Staff Discussion Paper, No. 2022-21, Bank of Canada, Ottawa, https://doi.org/10.34989/sdp-2022-21

This Version is available at:
https://hdl.handle.net/10419/297067

BANK OF CANADA
BANQUE DU CANADA

Staff Discussion Paper/Document d'analyse du personnel — 2022-21

Last updated: December 19, 2022

The Relative Benefits and Risks of Stablecoins as a Means of Payment: A Case Study Perspective

by Annetta Ho,[1] Sriram Darbha,[2] Yuliya Gorelkina[1] and Alejandro Garcia[1]

[1]Financial Stability Department
[2]Information Technology Services
Bank of Canada
sdarbha@bankofcanada.ca, ygorelkina@bankofcanada.ca,
agarcia@bankofcanada.ca

DOI: https://doi.org/10.34989/sdp-2022-21 | **ISSN** 1914-0568

Acknowledgements

The authors thank John Bitzan, Nikil Chande, Éric Chouinard, Han Du, Scott Hendry, Bena Lands, Steven Lavergne, Zhentong Lu, Cyrus Minwalla and Ariel Olivares for their helpful suggestions and comments. We also thank Visvanathan Srinivasan and K. Vijayakumar from the Reserve Bank of India for fact-checking our representation of the UPI system. All remaining errors are our own. The views expressed are our own and do not necessarily reflect those of the Bank of Canada. At the time of publication of this paper, Annetta Ho is on secondment outside the Bank of Canada.

Abstract

Our paper contributes to the discussion about the utility of stablecoins for retail payments through an objective, evidence-based approach that compares stablecoins with traditional retail payment methods. The paper also provides insights that could be useful in the design of central bank digital currencies. We identify the potential benefits, risks and costs of stablecoin arrangements used for retail payments relative to traditional retail payment methods. We select three real-world examples for comparison: (i) a Mastercard credit card payment through a traditional bank; (ii) a Unified Payments Interface fast payment through Paytm (a technology-enabled payments company regulated as a limited-purpose bank); and (iii) a stablecoin retail transaction using USD Coin and a BitPay wallet. We find that certain stablecoin arrangements offer end users greater control of their privacy, facilitate more rapid innovation and have the potential to increase transaction speeds, particularly for cross-border payments. At the same time, stablecoins may provide less consumer protection for fraud, present higher risks to the payment system and to efforts to combat financial crime (partly because of the more nascent regulatory framework), and be costlier relative to traditional payment arrangements. Our findings suggest that stablecoin arrangements do not currently serve as substitutes for the suite of traditional payment arrangements but instead address niche use cases or user segments that value their benefits and can accept their risks or costs.

Topics: Digital currencies and fintech; Payment clearing and settlement systems
JEL codes: D78, O38

Résumé

Notre étude vient enrichir la discussion sur l'utilité des cryptomonnaies stables pour les paiements de détail, grâce à une comparaison objective et basée sur des faits des cryptomonnaies et des méthodes de paiement de détail traditionnelles. L'étude fournit également des informations qui pourraient s'avérer utiles lors de la création de monnaies numériques de banque centrale. Nous identifions les possibles avantages, risques et coûts de l'utilisation de dispositifs de cryptomonnaie stable lors de paiements de détail, et les comparons à ceux des méthodes de paiement de détail traditionnelles. Nous prenons trois exemples concrets pour nos comparaisons : i) un paiement effectué à l'aide d'une carte de crédit Mastercard par l'entremise d'une banque traditionnelle; ii) un paiement rapide effectué dans le système Unified Payments Interface par l'intermédiaire de Paytm, une entreprise de services de paiement propulsée par la technologie et régie en tant que banque spécialisée; et iii) une transaction de détail réglée avec une cryptomonnaie stable par l'entremise de USD Coin et d'un portefeuille BitPay. Nous constatons que certains dispositifs de cryptomonnaie stable offrent aux utilisateurs finaux plus de contrôle en matière de confidentialité, favorisent la rapidité des innovations, et pourraient augmenter la vitesse à laquelle s'effectuent les transactions, surtout les paiements transfrontaliers. Parallèlement, les cryptomonnaies stables pourraient moins bien protéger les consommateurs contre la fraude. Elles pourraient

engendrer plus de risques pour le système de paiement et nuire aux efforts de lutte contre les crimes financiers (en raison notamment du cadre réglementaire peu développé), et elles pourraient être plus coûteuses que les méthodes de paiement de détail traditionnelles. Il ressort de notre étude que, à l'heure actuelle, les dispositifs de cryptomonnaie stable ne servent pas de substituts aux méthodes de paiement de détail traditionnelles dans leur ensemble. Ils conviennent plutôt à des cas d'utilisation spécialisés ou à des segments d'utilisateurs qui valorisent leurs avantages et sont prêts à accepter leurs coûts et risques.

Sujets : Monnaies numériques et technologies financières; Systèmes de compensation et de règlement des paiements
Codes JEL : D78, O38

Summary

The rise of stablecoins as a potential new form of money invites questions around their usefulness compared with traditional payment methods: Why would a person make a payment using a stablecoin instead of a traditional payment method? What are the trade-offs in terms of benefits and risks? And how quickly are these trade-offs changing as technology improves and regulation catches up?

Using a case study approach that compares real-world models of different retail payment methods, this paper provides concrete examples of the potential benefits, risks and costs of stablecoins relative to traditional digital payment methods.[1] Specifically, we compare the attributes of three types of digital payment methods:

- a Mastercard payment through a traditional bank
- an India-based Unified Payments Interface (UPI) fast payment through Paytm, a technology-enabled payments company regulated as a limited-purpose bank
- a USD Coin (USDC) retail transaction carried out using a BitPay wallet

We focus on retail payments as opposed to wholesale payments between financial institutions. This allows us to control the scope of the paper and to help central bankers understand how private stablecoins can be improved, potentially through a retail-purpose central bank digital currency (CBDC).

Our findings suggest that certain stablecoin arrangements (SAs) that are similar to retail payments do not necessarily substitute, but can instead complement, the suite of traditional payment instruments currently available to retail end users. Like any payment instrument, a stablecoin has a unique profile of benefits and risks and is unlikely to satisfy all attributes or use cases equally. With the caveat that our findings are based on the case studies selected and are not generalizable to all stablecoins or traditional payment arrangements, our key results are as follows:

- **Compared with traditional payment arrangements, certain SAs can offer end users greater control over their privacy.** Pseudonymous access and fewer intermediaries allow for greater privacy, which can protect freedom of association (e.g., contributions to political parties) and prevent merchants from commercializing data that may lead to consumer harm (e.g., through high prices). However, disintermediation also shifts liability to end users in terms of fewer end-user protections that would have been provided by intermediaries, such as access to recourse in instances of fraud or loss. The mechanisms for achieving greater privacy

[1] All references to traditional payment methods in this paper refer to traditional *digital* payment methods.

can also be used for money laundering and terrorist financing, which are proving more challenging to regulate for non-custodial or unhosted wallets.

- **In contrast to traditional payment arrangements that have more tiered participation structures and centralized governance, the higher degree of access to certain stablecoin platforms can facilitate more rapid innovation.** The combination of openness[2] with new blockchain technology could lead to entirely new products and services that are not yet feasible or that would require significant changes to traditional payment systems. At the same time, this openness could make it easier for malicious actors to create and deploy applications on the blockchain that harm users or steal their funds.
- **Relative to traditional payment arrangements, reduced intermediation in certain stablecoin payment chains and 24/7 availability of the blockchain have the potential to increase payment speeds.** Participants in blockchain-based systems can transact directly with one another under a single network without relying on a chain of intermediaries across different geographies and time zones. This is particularly beneficial for addressing the technical challenges associated with cross-border payments. However, the transaction costs to achieve those speeds on the blockchain could be high, given the current transaction pricing system, which auctions the blockchain's computational resources to the highest-paying users. As demand for blockchain use grows, blockchain computing efficiency or incentive mechanisms will need to be improved.

Going forward, SAs could carve out certain payment niches for themselves where traditional payment methods have not ventured or have failed to meet end-user needs. Policy-makers should ensure that as the collective payment system evolves to support new kinds of economic activity, both on and off the blockchain, the payment system continues to be safe and efficient.

[2] *Openness* refers to the ability to deploy any smart contract on the blockchain and not to the open-source programming of the blockchain protocols or code itself, which can improve the safety and efficiency of the blockchain over time.

A case study approach

To assess the potential benefits and risks of the payment aspects of SAs, we use a case study approach and compare one in-market SA with two traditional in-market retail payment arrangements, evaluating them on a common set of attributes. This method is analogous to developing and comparing stylized models and makes the analysis more tractable, given the diversity of payment designs. Our attributes framework helps to ensure the case studies are assessed comprehensively and consistently.

We select attributes that are desirable for a well-functioning payment system from the perspective of a central bank or public authority. As a baseline, we start with attributes that have been shown in the payments literature to be key for end-user adoption, since end-user interests are important to public authorities. As Kosse, Lu and Xerri (2020) note, these include:

- fraud
- speed
- convenience
- cost
- privacy

We then include other attributes that are important to public authorities themselves:

- payment system risk and public safety
- access
- financial inclusion[3]

For each payment arrangement, we use a quantitative scoring approach that follows papers such as Chapman et al. (2015) and Kosse, Lu and Xerri (2020). We assign a set of objectively measurable features to each attribute and give each feature a score from 1 to 3 (see **Table A-3** in the Appendix). The purpose of scoring is to help objectively identify potential relative advantages and disadvantages of SAs along specific dimensions (attributes). We do not calculate a weighted overall score or rank the case studies along each attribute.[4] Instead, we use differences in the feature scores for each attribute as a basis for understanding potential advantages, disadvantages and trade-offs. **Figure A-2** provides a visual representation of our scoring results. We also consider qualitative factors where scoring is difficult (e.g., speed of innovation resulting from broader access) or data are lacking.

We choose case studies that represent different types of back-end payment systems and front-end service providers that meet certain criteria, regardless of their geographic location.

[3] These were identified as potential payment motivations for issuing a CBDC in a paper authored a group of central banks, including the Bank of Canada (see Bank for International Settlements 2020). It is notable that this paper reviews the access policies of the back-end payment system as a proxy for payment diversity.

[4] Weights for each feature can vary by perspective (e.g., consumer, merchant, public policy) and even within each perspective, depending on the importance assigned to those features.

However, to ensure the case studies are comparable, they must address at least one of the use cases typically addressed by current SAs: person-to-person (P2P) or person-to-business (P2B). We also include other criteria:

- Adoption—Providers have to be successfully adopted or relatively well adopted compared with their peers, as measured by their name recognition, market penetration and maturity.
- Features—Selected providers need to be relatively advanced in terms of their functionality within their category or be best-of-breed in terms of features offered for their type. This allows us to understand how these payment systems compare near the leading edge of feature functionality.
- Availability of information—Sufficient publicly available information is needed to conduct our analysis. Detailed information on the technical design of payment systems is considered valuable.

For each case study, we specify a front-end and a back-end service provider, since both ends impact the attributes we are interested in comparing but can be performed by different intermediaries. The front-end service provider faces the end user and is involved in the initiation or authorization of a payment instruction, which it transmits through its connection to the back end. The back-end service provider is the multilateral payment system that performs clearing and settlement of financial obligations arising from those instructions.[5] We note that the payments chain can involve additional intermediaries, and the delineation between front and back may not always be clear. For the purposes of this paper, we use the categorization and level of detail shown in **Table 1**. **Figure A-1** and **Table A-2** in the Appendix provide additional details on processing flows and key features, respectively, for the three case studies.

[5] We do not consider on-us payments, which do not require multilateral payment systems. On-us payments exist in traditional payment arrangements and occur when the sending and receiving intermediaries are the same entity.

Table 1: Case studies

Case study	Front-end service provider	Back-end service provider	Dominant use cases (P2P or P2B)
1	Bank	Mastercard (credit card)	P2B
2	Paytm (non-bank payment service provider or PSP)	UPI (fast retail payment system)	P2P and P2B
3	BitPay (pure crypto wallet provider)	USDC on Ethereum (SA)	P2P and P2B

Note: P2P is person-to-person; P2B is person-to-business; PSP is payment service provider; UPI is Unified Payments Interface; USDC is USD Coin; SA is stablecoin arrangement.

Bank–Mastercard: The first case study consists of a bank and a credit card system. Credit cards are arguably the oldest retail electronic payment system.[6] The first credit card (Diners Club) was introduced in 1950, and electronic processing became possible a decade or so later (Hyman 2021).[7] Banks were traditionally the main participants in the credit card system, exchanging payment instructions electronically within the card network. For our case study, we did not choose a specific bank because we believe front-end services for credit cards are fairly uniform across banks, given credit card rules and the maturity of these arrangements.

Paytm–UPI: The second case study uses a non-traditional bank or payment service provider (PSP) and a fast payment system in India.[8] Fast payment systems are a new type of high-speed "account-to-account" system in which a payment is initiated directly from the account sending or receiving funds.[9] Fast retail payment systems are defined by their 24/7/365 operations and near–real time funds availability for end users.[10] Although banks also typically participate in fast retail payment systems, we choose to study a PSP as the front-end service provider to examine a greater diversity of front-end systems. Compared with traditional banks, PSPs typically operate on more modern, flexible technology that allows them to adopt

[6] Electronic payments are generally understood to be any type of payment that is not made with paper (cash or cheque). Indeed, while the credit card itself is still physical, payment instructions are transmitted electronically between participants in the card network. Note that digital payments are a subset of electronic payments and are fully electronic in that the payment is initiated from a digital device, such as a mobile phone or computer.

[7] Electronic card processing became possible after the invention of the magnetic stripe in the 1960s.

[8] The Brazilian fast retail payment system Pix, launched in 2020, has recently been the focus of increasing media attention. We view Pix as highly similar to UPI and do not believe we lose any significant rich functionality by studying the UPI system. For more information on Pix, see Banco Central do Brasil (2020).

[9] Although we could have studied an older type of slower account-to-account system (sometimes known as retail batch systems), we selected an alternative system that addressed P2P use cases.

[10] For more details, see Bank for International Settlements (2016).

and offer innovations to the market more quickly (e.g., PayPal was the first to provide payment solutions for e-commerce in 1998).

BitPay–USDC: The third case study involves an SA and a crypto wallet provider. The SA is a new type of payment system that uses distributed ledger technology (DLT) to clear and settle payments. A crypto wallet provider can be a bank or non-bank that also provides crypto payment services. However, we choose BitPay, a pure (non-bank) crypto wallet provider, to maximize contrast across our case studies, since we already consider banks in the case study with Mastercard. BitPay provides a non-custodial wallet, which means that the end user—not BitPay or another third party—holds the private keys associated with the digital assets in the wallet. The private key proves ownership of the digital assets and is necessary to maintain control and conduct transfers.

USDC is the second largest stablecoin by market capitalization (behind Tether). We choose it so that we can focus on stablecoins that are similar to traditional retail payments. USDC is issued by Circle and operated by a consortium known as Centre. The coin aims to be pegged one-to-one to the US dollar. In theory, Circle issues 1 USDC for every US$1 exchanged, and it holds in reserve or reinvests US dollars received to support future redemption requests. Since a reserve of assets denominated in fiat currency supports the value of USDC, USDC is considered a "fiat-backed" stablecoin.

USDC is attracting major payment system players to its ecosystem. For example, in March 2021, the Visa network announced plans to expand its pilot program for acceptance of USDC for crypto-native card issuers. Visa explained that USDC had the necessary demand, stability and security given its "track record of clear compliance and regulatory engagement" (Visa 2021). Later that year, MoneyGram International Inc., a major cross-border remittance company, also announced a project to enable settlement in USDC so that customers could seamlessly convert USDC to cash and vice versa (MoneyGram International Inc. 2021).

We note that USDC runs natively on eight different blockchains (Ethereum, Algorand, Solana, Stellar, TRON, Hedera, Flow and Avalanche) using their respective open token standards.[11] To make the analysis tractable, we focus on Ethereum and its ERC-20 standard (**Box 1**), since BitPay uses this blockchain to process USDC transactions (BitPay 2019). Moreover, Ethereum is the predominant blockchain used by decentralized finance (DeFi) applications, and the ERC-20 token standard is used for a number of other major stablecoins.[12]

[11] USDC also provides developers with application programming interfaces for swapping USDC across blockchains. For more information, see Centre (2022).

[12] For more details, see U.S. Department of the Treasury (2021a).

Box 1: ERC-20 token standard

Cryptocoins are issued on Ethereum through the creation of smart contracts that present a set of operations, such as to issue coins, track the total supply and balances of users, and transfer coins between users. Before ERC-20 was established, each coin issuer would write a smart contract that differed slightly from other contracts. Crypto wallet providers and exchanges would have to implement custom code to be able to operate on the contract of each new cryptocoin. With the proliferation of cryptocoins, this became untenable.

The crypto community developed ERC-20—Ethereum Request for Comments #20—as a standard for interoperability of fungible assets on the Ethereum blockchain specifying the mandatory and optional operations that a smart contract for a fungible asset must support. With respect to payments, the relevant operation or function is a transfer. Now exchanges and wallet providers that support ERC-20 can recognize and operate on *all* coins issued using contracts that adhere to that standard without requiring code changes each time a new coin is issued.

Benefits and use cases of stablecoins as a means of payment

This section identifies attributes for which the BitPay–USDC arrangement may have benefits or advantages compared with the bank–Mastercard and Paytm–UPI arrangements. It also discusses some of the potential use cases for stablecoins given these benefits.

Privacy: Greater personal freedoms and lower social costs

Privacy relates to the collection and use of personal information, including disclosure of that information to third parties. Personal information is data about an identifiable individual that, on its own or in combination with other pieces of data, can identify the individual (Office of the Privacy Commissioner of Canada 2018). The payment industry generates a large amount of commercially valuable personal information about transaction histories and spending habits that can be linked back to identifiable individuals.

Traditional payment methods require "real-world identification" or non-digital identity credentials, such as government-issued passports or driver's licenses. For regulatory reasons (see section on financial crime risks), front-end service providers in these arrangements—namely financial institutions or non-bank PSPs—must always adhere to know-your-customer requirements. This involves collecting and verifying real-world identity data before the provider can open accounts and provide payment services to its customers. Front-end service providers subsequently create identifiers, which we call "payment system identifiers," such as account or credit card numbers. These numbers are sensitive because they are one piece of

information end users need to access their funds, but they also serve as addresses that must be shared among payment intermediaries for routing purposes. Back-end service providers—such as Mastercard and UPI—do not collect end users' personal information or addresses but do collect individual payment values. Historically, credit card systems shared the credit card numbers of customers with merchants, which allowed savvy merchants to identify unique customers and track their spending habits or patterns. With newer payment technologies, credit card users can sometimes protect their privacy by opting to tokenize or hide their credit card number from merchants.[13] In the UPI system, UPI-specific addresses (virtual payment addresses) are shared between end users and subsequently resolved into account numbers by front-end service providers for routing, reducing the sensitivity of information shared between end users. This can enhance privacy and security for the end user.

SAs go further and can transfer assets without real-world identifications and, as a result, offer relatively greater privacy than traditional arrangements. In our SA case study, this can occur under certain circumstances. **Table 2** lists the identification information collected by BitPay, USDC and Ethereum. Unless a user is sending a personal payment greater than US$3,000 or receiving a payment as a business, the information collected is relatively non-sensitive—it would require some effort to trace or link this information to a verified identity. The USDC smart contract and Ethereum network track only a user's blockchain address.[14] However, if a user wishes to exchange fiat for USDC directly with the USDC issuer Circle, the user would need to have their identity verified. To protect their privacy, a user could transfer their USDC to a non-custodial wallet like BitPay so that subsequent transaction activity cannot be directly linked to their identity.

[13] Mobile wallets such as Apple Pay often tokenize credit card numbers.

[14] The USDC smart contract and Ethereum network are considered pseudonymous, not anonymous, because if the real-world identity associated with an address were to become known (due to factors extraneous to the network), that individual's transactions from that address would be known.

Table 2: Identity information collected

Entity	Information collected
BitPay	Personal:[15] • when sending amounts less than US$3,000—name and email address • when sending amounts greater than US$3,000—name, email address and one identification document (e.g., passport, driver's license or identity card) Business: registered company name, corporate email address, address, beneficial owner(s), bank account information (optional)
USDC	None—blockchain address is the identifier
Ethereum	None—blockchain address is the identifier

Note: USDC is USD Coin.

With advanced cryptographic technology, privacy can be further enhanced to hide all identifiers and valuable transaction information, achieving degrees of privacy provided only by cash today. For example, Zcash is a cryptocurrency that uses advanced cryptography to hide the sending and receiving addresses and amount of every transaction.[16] Although Zcash is not a stablecoin, the cryptographic techniques it employs could be used to implement a stablecoin. It is also possible that, when combined with other properties of the blockchain, more innovative payment products and services can emerge that provide a higher degree of privacy (see **Box 2**).

[15] See BitPay (2022a).

[16] The public Zcash ledger records only that a cryptographically verifiable transaction took place, without revealing any details. For more information, see Zcash (2021).

Box 2: Tornado Cash—a custom contract that delivers enhanced privacy

Tornado Cash offers a service on Ethereum that severs the link between the source and destination addresses of an ERC-20 payment, thereby enhancing the degree of privacy for users. Tornado Cash is part of a class of software known as mixers, which are designed to conceal or obfuscate the source or owner of virtual assets.

Although services like Tornado Cash facilitate greater privacy, they also increase the risks of financial crime and make enforcement of anti–money laundering regulations more challenging (see section on financial crime). In August 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control sanctioned Tornado Cash as an open-source software tool.[17] Following the format of the unprecedented sanctions against the mixer Blender[18] several months earlier, the sanctions focused on Tornado Cash's website and addresses, rather than a person. The effectiveness and legal enforceability of such sanctions remain to be seen (Brito and Van Valkenburgh 2022).

Apart from the fact that individual preferences vary and some people value privacy more than others do, legitimate reasons or uses do exist for greater privacy in payments. One such reason is that privacy can be considered a precondition for other freedoms, such as freedom of association and freedom of speech.[19] For instance, individuals may want to keep their contributions to political parties or advocacy groups (e.g., pro-life or pro-choice groups, organizations for the legalization of drug use) anonymous, particularly if they live under authoritarian regimes. Individuals may also value privacy for payments that are more personal, such as those for treating health or medical conditions. Another more economics-based motivation to improve privacy is that individuals may not bear the full cost of failing to protect their privacy, leading to negative externalities for others (e.g., merchants using data from less-private individuals to price discriminate against or target their advertising toward more-private individuals) (Garratt and van Oordt 2019). Lastly, security risk is another factor, in that minimizing the amount of personal information shared can reduce risk of identity theft. **Table 3** compares the level of privacy in each of the three case studies.

[17] See U.S. Department of the Treasury (2022a).

[18] See U.S. Department of the Treasury (2022b).

[19] See European Data Protection Supervisor (2019).

Table 3: Comparison of privacy across case studies

Bank–Mastercard	Paytm–UPI	BitPay–USDC
• Identity collected by bank and verified with proof of identification • Unless tokenized, credit card account numbers shared with merchants	• Identity collected by Paytm and verified with proof of identification • Virtual payment addresses, rather than account numbers, shared between end users	• If payment exceeds a threshold, identity collected by BitPay and verified with proof of identification; otherwise, only name and email required • Blockchain addresses shared between end users

Note: UPI is Unified Payments Interface; USDC is USD Coin.

Access: More rapid innovations

Access refers to the ease with which an entity can participate directly or indirectly in the back-end payment system. In a payment system, front-end service providers are given access to the back-end application and can build their own applications on top of it. In this way, payment products and services are made up of multiple applications that interact with one another to form a single payment experience.

Traditional payment systems have tiered access arrangements in which only a closed group of participants are permitted to participate. Increasingly, access to traditional payment systems is broadening to include non-financial institutions. However, participants still need to be licensed or regulated. For example, Mastercard permits only those financial institutions or other legal entities authorized to engage in financial transactions to be issuers or acquirers, and UPI permits only banks (full- and limited-purpose) to become members.[20] Third parties without access would need to develop a commercial relationship with the payment system participant, which would allow them to leverage the back-end payment system for their product or service. The types of products and services that can clear and settle using a traditional payment system are therefore dictated by the multi-layered access policies of back-end service providers and their direct participants.

Access also refers to the openness of application programming interfaces (APIs), which can reduce barriers to entry and facilitate innovation. APIs establish a standard set of rules and specifications for software programs to communicate with each other, forming an interface between different programs to facilitate their interaction.[21] Open APIs are public and can

[20] See National Payments Corporation of India (2022a).

[21] In other words, an API is a programmable access point that can be used by one application to invoke another application.

therefore be more easily adopted by a wide set of market participants.[22] Provided the standard becomes ubiquitous, a payment product or service developer needs to integrate its new product or service only with the open API to access all front- or back-end applications that use that API. This can reduce costs for developers, who no longer need to create custom instructions for communicating with each application.

The public library of open APIs within traditional payment arrangements is growing. The Mastercard Developers program allows issuers, merchants and their acquirers or service providers to integrate Mastercard's APIs into their services to improve the customer experience.[23] In India, UPI provides a common set of APIs for sending and receiving payments between banks and non-banks (Carrière-Swallow, Haksar and Patnam 2021). UPI participants like Paytm can then provide additional APIs to their customers, including merchants, who can leverage the APIs to simplify payments for their customers.[24]

SAs tend to be more open than traditional payment arrangements, giving any (end) user the ability to create their own products and services that use the stablecoin's clearing and settlement program. USDC was intentionally designed to use only open API standards so that developers could easily build products and services using USDC as a means of payment. For example, it leverages the ERC-20 open standard (described in **Box 1**), which implements an API for tokens within smart contracts (Ethereum 2022a). The key difference between traditional payment arrangements and SAs is that the latter are built on open access, permissionless systems. In permissionless blockchains, any user can build new financial products or services in the form of smart contracts that leverage these open standards.[25] These smart contracts are published on the blockchain without subjective assessment by individual nodes or approval by a single central authority. In this way, control over the blockchain is more democratized and a broad set of actors can innovate without constraints.

In theory, broader access policies and less centralized governance on the blockchain can provide benefits in the form of more rapid innovation. According to Statista (2022), the number of cryptoassets grew exponentially between 2013 and 2022, from 66 to over 10,000. The rate at which these newer cryptoassets improve the utility or efficiency of their predecessors, and therefore the degree of innovation, is difficult to measure. However, the

[22] For more information on APIs, see Bank for International Settlements (2019).

[23] See Mastercard Developers (2022).

[24] See Paytm's documentation for developers (Paytm 2022).

[25] The process begins with one party coding a smart contract to invoke APIs on USDC or other ERC-20-compatible smart contracts. It then issues a transaction to "install" the contract on the blockchain into its own account. If the transaction is picked up by miners in exchange for gas fees, the transaction is written into a block on the Ethereum blockchain as part of the owner's account. Other parties can then execute transactions that invoke the smart contract's APIs.

large number of cryptoassets may facilitate competition and improvement in products or services. **Table 4** compares access levels of the three case studies.

Table 4: Comparison of access across case studies

Bank–Mastercard	Paytm–UPI	BitPay–USDC
• Access to Mastercard is tiered, where only financial institutions and authorized financial service providers can be issuers or acquirers • Mastercard provides open APIs to developers for value-added services	• Access to UPI is tiered, where only full- and limited-purpose banks can be members • UPI provides open APIs for core payments exchange; Paytm provides APIs to developers for value-added services	• Access to Ethereum and USDC smart contract is fully open to the public • USDC is built on widely adopted open API standard ERC-20

Note: API is application programming interface; UPI is Unified Payments Interface; USDC is USD Coin.

Speed: Faster cross-border payments

Speed refers to the time between initiation of a payment and the availability of funds to the final recipient on an irrevocable basis. Among other things, the speed of payments is determined by the cumulative rules and policies (e.g., service levels) of each front- and back-end service provider in the payment chain. The speeds they can commit to are limited by various factors, such as their technology or operations.

Traditional retail payments can attain fairly high speeds for domestic payments, but cross-border payments remain a challenge. [26] Mastercard payment speeds vary by jurisdiction, but on average are the slowest among our case studies. Mastercard clears payments in batches and uses local networks of banks and their back-end payment system providers to complete the settlement process. We estimate the highest speeds Mastercard can provide are same-day funds availability, assuming use of local real-time gross settlement systems. As a fast payment system, UPI clears individual domestic payments within India in real time and requires participants to provide funds to customers almost instantly.[27] It also operates on a 24/7/365 basis, so there are no delays, even if payments are made overnight or on weekends. Speed becomes an issue for cross-border payments because both traditional arrangements need interlinking solutions or chains of intermediaries to move money across borders. These

[26] Cross-border payments are payments where the payor and payee are located in different countries. For more information, see Financial Stability Board (2020a).

[27] Like Mastercard, UPI operates under a deferred net settlement model, but participants submit payments to the system for clearing individually rather than in batches.

chains can be long and complex, with each intermediary adding time. In extreme cases, it could take up to 10 days to process a cross-border payment (Cleland 2021).

SAs share similar characteristics to credit card and fast payments. At its optimal speed, a domestic BitPay–USDC payment could be faster than a domestic Mastercard payment but slower than a domestic Paytm–UPI payment. Like Mastercard, the Ethereum blockchain clears payments in batches or "blocks," but new batches are created and settled at much higher frequencies, on average every 12–14 seconds (Ethereum 2022b). Like UPI, Ethereum operates on a 24/7/365 basis, but wallets are not required to provide funds immediately to end users. In fact, BitPay chooses not to credit accounts for USDC until 50 blocks have been confirmed, which takes approximately 12.5 minutes (BitPay 2022b). This is likely due to concerns about the lack of certainty or irrevocability in settlement because Ethereum provides only probabilistic settlement and, although the probability is very low, payments can be reversed (see section on payment system risk). The likelihood of this occurring decreases as the chain lengthens beyond the block containing the payment.

Speed can be quite variable on blockchain-based systems when supply and demand are imbalanced. The supply side can face scalability challenges, because blocks have a fixed size and can fit only a certain number of transactions. Transactions can be queued to wait for the next block if the number of transaction requests on the network is high. On the demand side, the computational resources that are required grow as the number and complexity of transactions increase. Efforts to improve network capacity and throughput on Ethereum are underway. In September 2022, Ethereum upgraded from the computationally intensive proof-of-work consensus algorithm to the more efficient proof-of-stake mechanism. It also plans to use "layer 2" systems to which some transactions are offloaded, where balances are netted and only periodically settled on the main blockchain. Ethereum estimates these changes could increase throughput from 15–45 transactions per second to 100,000 transactions per second.[28]

The main advantage of SAs is that they are built on blockchains that reach a broad universe of entities. They can therefore facilitate shorter transaction chains for cross-border payments. Further data are needed to validate the extent to which the theoretical advantages of blockchain technology translate into improvements in cross-border payment speeds. Complicating this analysis are concurrent developments in both traditional payment systems and blockchains that could further narrow or widen the gap. The G20 made the enhancement of cross-border payments a priority in 2019, and more cross-border payment initiatives are being planned (Bech, Faruqui and Shirakami 2020). In September 2021, for example, the

[28] Following migration to proof of stake, Ethereum plans to add 64 shard chains, which will be new chains used to store data horizontally but not process transactions. Combined with "rollups" that allow a group of transactions to be processed off-chain (analogous to netting transactions) and submitted as a single transaction on-chain, Ethereum estimates it can increase throughput to 100,000 transactions per second (Ethereum 2022c, 2022d).

Reserve Bank of India announced a project with the Monetary Authority of Singapore to link UPI with Singapore's fast payment system PayNow, which could improve payment speeds between these two countries (Monetary Authority of Singapore 2021; Reserve Bank of India 2021). Mastercard is also seeking to facilitate cross-border payments with the introduction of its new Mastercard Cross-Border Services (Mastercard 2022a).

Table 5 summarizes the speed of payments in our three case studies.

Table 5: Comparison of payment speeds across case studies

Bank–Mastercard	Paytm–UPI	BitPay–USDC
• Same-day availability of funds to end users for domestic payments • Speed of cross-border payments may be slower and depends on chain of intermediaries	• Near–real time availability of funds to end users for domestic payments • Speed of cross-border payments may be slower and depends on chain of intermediaries	• BitPay does not provide funds to end users until approximately 12.5 minutes after technical settlement; time to settle depends on fees offered by user • Cross-border payments technically do not require a chain of intermediaries because end users can directly access Ethereum

Note: UPI is Unified Payments Interface; USDC is USD Coin.

Risks and costs of stablecoins as a means of payment

This section identifies attributes for which the BitPay–USDC arrangement may have higher risks or costs compared with the bank–Mastercard and Paytm–UPI arrangements.

Fraud: Weaker consumer protections for fraud losses

Fraud refers to an act of deception for financial or personal gain that can lead to losses for the rightful owners of funds.[29] End users in a payment arrangement are protected against fraud by the preventive controls in place (e.g., security features) and by access to compensation for financial loss if fraud does occur (e.g., liability policies). The latter makes up consumer protection policies for fraud. Although both security controls and access to compensation serve to protect end users, we lack data to rank the adequacy and

[29] Fraud can take various forms. Unauthorized fraud occurs when a payment is initiated by someone other than the legitimate account holder or authorized party (e.g., an account takeover). Authorized fraud occurs when a payment is initiated by the legitimate account holder or authorized party but as a result of deception by the payee (e.g., a scam).

effectiveness of security measures across our case studies. Arguably, a more conservative approach is to consider only consumer protection policies, which can shield users from fraud losses despite weak or non-existent security controls. Hence, we focus on comparing consumer protection policies across our case studies.

Traditional payment arrangements and SAs differ in their provision of controls to compensate consumers for losses if fraud occurs. In traditional payment arrangements, liability for fraud is shared across intermediaries and end users in accordance with their roles and responsibilities. Consumers typically bear minimal liability, given that they outsource the custody and transfer of funds to their payment service providers. Mastercard's terms and conditions protect end users with a strong zero-liability policy for unauthorized transactions, which means virtually no losses in these cases (Mastercard 2022b).[30] However, the merchant can be found liable by the acquirer and thereby charged a chargeback fee depending on the identified reason for an unauthorized transaction.[31] Similarly, UPI's regulator limits users' liability for unauthorized electronic banking transactions, including for UPI payments (Reserve Bank of India 2017). End users bear zero liability in the case of negligence on the part of their bank or a third party. Should their own negligence lead to an unauthorized transaction and subsequent losses, the end user's liability is limited to the losses they incur before notifying their bank.[32]

In contrast to traditional payment arrangements, end users in SAs forgo the intermediaries that take custody of their funds and provide payment services. Consequently, stablecoin users also relinquish access to the consumer protections that underpin traditional payment arrangements and the instruments used within them. Because users assume full custody of and responsibility for their funds, BitPay does not provide access to recourse or redress if unauthorized use of their funds occurs. Stablecoin users assume the burden of full liability should they find themselves victims of fraud. From the end-user perspective, holding stablecoins is therefore analogous to holding cash.

In the absence of consumer protection policies in SAs, it is useful to consider the security of stablecoin platforms. We summarize a study on Ethereum security in **Box 3**, noting the lack of information about the security of SAs.

[30] Users still must exercise reasonable care in safeguarding their card and personal identification number and must report card loss or theft in a timely manner.

[31] For instance, Canadian merchants are liable for domestic card-present fraudulent transactions that could have been avoided by adopting chip technology.

[32] UPI end users who find themselves victims of fraud also benefit from access to UPI's online Dispute Redressal Mechanism and an escalation process for complaints on its website. For more information, see National Payments Corporation of India (2022b).

Box 3: Ethereum security

From a survey of literature on known exploits on the Ethereum platform, 23 vulnerabilities were catalogued across three categories:

- language used in the Solidity smart contract (17 vulnerabilities)
- Ethereum virtual machine (EVM) (2 vulnerabilities)
- blockchain design (4 vulnerabilities)[33]

The survey suggests that the bulk of vulnerabilities arise from weaknesses in the coding language. It found that exploits to date have largely targeted programming language vulnerabilities rather than any weakness in the blockchain or the EVM. Over time, these risks could be minimized through better coding practices and using the many tools available to analyze smart contract code prior to deployment. Regarding USDC, it is unclear if the smart contract code (where most vulnerabilities typically arise) for the USDC instrument has been subject to audits.[34]

These results do not imply that Ethereum is fully secure. It is not known which security certifications, if any, the Ethereum platform codebase has attained and if it is subject to security audits of the type that traditional systems generally undergo. Further, the open-source model of voluntary developers may predispose the platform in the long run to utility features such as convenience at the expense of security features.

In our judgment, given that the security of blockchain technology has yet to be proven and consumer protections are unavailable in cases of stolen funds, fraud risk is currently relatively higher for stablecoin arrangements (**Table 6**).

[33] See IEEE Xplore (2022).

[34] Circle's website suggests that the company follows leading industry standards and practices regarding security, but we cannot confirm this. It is unclear if any security audits conducted by Circle would cover the smart contract code used to execute transfers of USDC (Circle 2022).

Table 6: Comparison of fraud across case studies

Bank–Mastercard	Paytm–UPI	BitPay–USDC
• Consumers have zero liability for unauthorized transactions • Merchants may be found liable for unauthorized transactions and subject to chargeback fee	• End users have limited liability for unauthorized transactions, zero liability in the case of negligence by bank or third party	• End users have full liability for unauthorized transactions

Note: UPI is Unified Payments Interface; USDC is USD Coin.

Payment system and financial crime risks: A nascent regulatory framework for controlling risks and crime

Critical payment infrastructure can be at risk of disruption or failure, which in turn can adversely affect economic activity. This payment system risk can be caused by or composed of other types of risks. We discuss payment system risk in terms of the legal, financial, operational and settlement risks associated with clearing or settling payments.[35] This includes consideration of the stability of the settlement asset (the asset used to discharge obligations). We also review financial crime risks, such as those of money laundering and terrorist financing activity—the basic risks that payment service providers must guard against to support public safety.

Traditional payment arrangements are underpinned by a strong regulatory framework to ensure their safety. In our case studies, the settlement assets are very stable because they are fiat currency held in accounts issued by a regulated commercial bank (e.g., as with Mastercard) or by a central bank (e.g., as with UPI). While less safe than a central bank, commercial settlement banks are subject to liquidity, capital and deposit insurance as well as other requirements to help mitigate the risk of loss of settled funds. Historically, the payment systems in our case studies—Mastercard and UPI—were not regulated because payment system regulation focused on systemically important wholesale systems. This has changed over the past two decades, with multiple central banks designating Mastercard for regulation—and some even considering it systemically important—and with the Reserve Bank of India recently expanding its oversight framework to include UPI.[36] These regulations tend to follow the Committee on Payments and Market Infrastructures (CPMI)-International

[35] The management of financial risks can also affect the safeguarding of end-user funds. In tiered payment systems where an intermediary holds end-user funds, inadequate management of settlement risks on the payment system can lead to losses for the intermediary, who could subsequently impose losses on end-user clients.

[36] In May 2020, the European Central Bank (2020) identified Mastercard as a systemically important payment system. That same year, the Reserve Bank of India (2020) implemented a framework for System Wide Important Payment Systems that included the National Payments Corporation of India (NPCI), the operator of UPI.

Organization of Securities Commissions (IOSCO) *Principles for financial market infrastructures* (PFMIs), a comprehensive set of international risk management standards covering legal, financial, operational and settlement risks.

In contrast, the regulatory framework for SAs is still under development in several jurisdictions. In July 2022, the CPMI published guidance on how the PFMIs apply to SAs and identified several unique features that present additional risks (Bank for International Settlements 2022). This includes the following:

- Stablecoins, as the settlement asset, are relatively less stable because they are not issued by a central bank or an entity subject to regulations that control for redemption risk.[37] USDC is issued solely by Circle, which is not subject to any liquidity, capital or deposit insurance requirements, although it has applied for a banking license in the United States (Circle 2021). Although Circle is not subject to the regulatory requirements discussed above, it voluntarily holds all reserve assets in cash or cash equivalents to minimize redemption risk.[38]

- Certain SAs rely on probabilistic settlement, which assumes a non-zero probability that transactions can be revoked and therefore are not final. This can arise due to certain consensus algorithms or hard forks (see **Box 4**). Ethereum upgrades could help accelerate transaction speeds and enable the creation of new blocks. Since the probability of revocation decreases as the blockchain lengthens beyond the block with the transaction, this could help reduce the time to settlement finality. Still, the CPMI recommends that an SA ensure a clear legal basis exists to support the finality of a transfer. The legal basis for USDC transfers is unclear.

- Control over these SAs is often partially or fully decentralized. For example, while USDC is centrally governed by Centre, Ethereum governance is decentralized and not owned or controlled by Centre. One risk from this is that any user can build new payment products and services in the form of smart contracts on top of the blockchain (see the section on access), even though these contracts may be malicious or vulnerable to attacks. A well-known example is the decentralized autonomous organization (DAO) exploit in 2016 (see **Box 5**). Although a traditional payment system operator may not be responsible for the code integrity of all the products it clears, it could mitigate this risk to some extent by preventing access by unsafe service providers. Stablecoin operators, however, usually do

[37] Redemption risk arises because the stablecoin can be redeemed on demand but there may not be sufficient liquid reserves to meet that demand. This makes it susceptible to a self-reinforcing "run" that reduces the value of the stablecoin and the value of the assets in the reserve as they are sold to meet redemption requests.

[38] In August 2021, Centre announced it would revise the investment policy for USDC such that all reserve assets must be held in cash or cash equivalents. According to third-party attestations, this was achieved the following October (Grant Thornton LLP 2021).

not control access to the underlying blockchain and therefore have more limited control over the full set of risks in its payment ecosystem.

Box 4: Hard forks

A settlement risk that is unique to blockchains is a *hard fork*. The Financial Stability Board describes a hard fork as a bifurcation in a distributed ledger whereby separate and irreconcilable ledgers are created, usually due to an unresolved disagreement among developers or other actors such as miners associated with a distributed ledger. However, forks can also result more generally from changes of the code in the underlying protocol that are incompatible with the previous version. [39] Forking a chain typically requires agreement between a large subset of node operators and, although disruptive, is usually undertaken when the operators believe it is necessary to preserve system integrity.

A transaction reversal due to a hard fork, for example on Ethereum, causes a loss if an off-chain asset was involved (e.g., a payment in ETH to buy bitcoin or a car). If instead two *on*-chain assets are involved (e.g., an ETH payment to buy the ERC-20 token USDC), then a rollback simply restores the assets each party held before the transaction and no loss occurs. Because the use of stablecoins for payments involves off-chain assets, hard forks can pose risks.

Box 5: The DAO exploit

The decentralized autonomous organization (DAO) was a crowdfunding platform launched in 2016. It raised US$150 million worth of ETH and was considered one of the most successful decentralized finance projects at the time. However, an attacker was able to exploit a vulnerability in its code and drain approximately 40% of those funds. To prevent loss of confidence in Ethereum, Ethereum developers proposed a hard fork to roll back Ethereum's network history to before the attack and give investors the opportunity to withdraw their funds. The proposal was largely accepted by miners, exchanges and node operators, leading to a split between Ethereum and Ethereum Classic (the blockchain that did not roll back).[1] Hard forks, outlined briefly in **Box 4**, can create additional risks.

This incident could have involved a payment application and a stablecoin instead of a crowdfunding application and ETH. It demonstrates that blockchains may not have adequate controls to detect or prevent malicious code or applications from being published to the network.

[39] See Financial Stability Board (2019) and International Organization of Securities Commissions (2020).

Payment system risk remains a concern because neither the USDC payment arrangement nor the underlying blockchains are regulated. Should a disruption occur in the ability to transfer USDC, and should USDC be adopted broadly as a means of payment, this could disrupt the smooth functioning of the economy and, in the extreme, pose systemic risk.[40]

Risk of financial crimes, including money laundering and terrorist financing, is also a concern for SAs and for crypto more generally. We expect it will take some time for regulators and law enforcement authorities to adapt to the various ways new ways that blockchain technologies can obfuscate funds. In 2018, the Financial Action Task Force (2021) clarified that anti–money laundering and counter-terrorist financing (AML/CTF) regulations should apply to virtual asset service providers. Since then, many—but not all—jurisdictions have implemented changes to their AML/CTF frameworks, requiring exchanges and crypto wallet providers to collect identities of their users when exchanging between fiat and cryptocurrency. This can help trace and detect criminals. However, even in jurisdictions where regulations apply, it may take time for those wallet providers to be in full compliance. For example, as a non-custodial wallet, BitPay is subject to AML/CTF regulations in the United States. Recently, US regulators found it had violated sanctions regulations and settled for $507,375 (U.S. Department of the Treasury 2021b).

Moreover, criminals can circumvent these regulations and are continuously developing new ways of doing so (see **Box 6**).

[40] The potential for SAs to pose systemic risk has been acknowledged by various regulatory bodies. See U.S. Department of the Treasury (2021a).

Box 6: Money laundering methods using blockchains

Below are some examples in which criminals can circumvent anti–money laundering and counter-terrorist financing regulations on the blockchain:

- "Mixer services" break the linkages between transactions, preventing authorities from tracing transactions on the blockchain.
- Cryptocurrencies built on networks that, like mixers, obscure the endpoint addresses, amounts and transaction graphs make it impossible to link one payment to another. One such coin is Monero, which is becoming the instrument of choice of ransomware attackers (Sigalos 2021).
- Multiple atomic swaps[41] allow users to effectively "hop" funds from one chain to another and back, making them difficult to trace.[42]

Authorities face quite a challenge to understand these new methods, at least in the short to medium term. In contrast, money laundering and terrorist financing methods using traditional payment systems have existed for a longer time and are better understood by authorities.

Table 7 summarizes the payment system and financial crime risks in each of our case studies.

[41] Atomic swaps occur when two parties exchange cryptocurrencies that are on separate blockchains without a third party. For more information, see Haqshanas (2021).

[42] For example, a criminal could accept a ransomware payment in a popular cryptocurrency like bitcoin, then use an atomic swap to exchange it for Monero and another to swap it back for bitcoin. At this point, the new bitcoin cannot be traced back to the original payment and can be cashed out for fiat.

Table 7: Comparing risks across case studies

Bank–Mastercard	Paytm–UPI	BitPay–USDC
• Mastercard is subject to regulatory framework that manages payment system risk; settlement asset is commercial bank money • Regulatory framework for AML/CTF is well established; both providers and authorities are experienced in addressing AML/CTF risks	• UPI is subject to regulatory framework that manages payment system risk; settlement asset is central bank money • Regulatory framework for AML/CTF is well established; both providers and authorities are experienced in addressing AML/CTF risks	• USDC is not subject to regulatory framework that manages payment system risk; settlement asset is a private digital currency • Regulatory framework for AML/CTF is newly implemented; both providers and authorities are less experienced in addressing AML/CTF risks on blockchain

Note: AML/CTF is anti–money laundering and counter-terrorist financing; UPI is Unified Payments Interface; USDC is USD Coin.

Cost: Higher transaction fees for consumers

To compare the cost efficiency of our case studies from a social perspective, one should assess their total costs in terms of overall resources used by society (Kosse et al. 2017). However, due to data limitations, we compare only the explicit costs charged or rewards provided by payment intermediaries to consumers and merchants in a P2B payment (**Table 8**). We note that merchants can pass their costs on to consumers through higher prices (merchant cost pass-through) (Felt et al. 2021).[43]

Table 8: Costs and rewards considered for person-to-business payments

Case study	Consumer (sender of funds)	Merchant (receiver of funds)
Bank–Mastercard	Annual credit card fee to financial institution (–) Rewards (depending on card type) (+)	Acquirer fee plus network fee plus interchange fee (–)
Paytm–UPI	Cashback points (+)	Rewards (+)
BitPay–USDC (Ethereum)	Blockchain transaction fee (gas fee) (–)	Network fee (–)

Note: UPI is Unified Payments Interface; USDC is USD Coin; (–) represents a cost or outflow; (+) represents a reward or inflow.

[43] Theoretical and empirical literature suggests that various factors affect the merchant pass-through rate. Felt et al. (2021) calculated that the median pass-through rate on retail prices due to industry-wide cost changes estimated by previous empirical case studies was 90%.

Traditional payment arrangements have various business and pricing models, but transaction fees for consumers are either non-existent or relatively much lower as a proportion of the transaction value, whereas merchants tend to pay more. Depending on the card type (e.g., basic or premium), Mastercard credit cards have zero fees for consumers, or an annual fee and varying rates of rewards. Conversely, merchants need to pay an acquirer fee, network fee and interchange fee, which vary by jurisdiction. Interchange fees make up the largest portion of merchant fees and have come under intense regulatory scrutiny in recent years. The average interchange fee in Canada is still relatively high at 1.52% (Mastercard 2021) but can be as low as 0.2%–0.3% for basic cards in more regulated countries.[44] In some jurisdictions, merchants can explicitly pass these fees on to customers.[45] The regulator for UPI prohibits UPI participants from charging any transaction fees; in fact, Paytm provides both consumers and merchants rewards for using UPI.[46] However, the viability of such a model is unclear, as Paytm has yet to demonstrate long-term profitability.[47]

Transaction fees associated with stablecoins can be more expensive compared with those of traditional payment methods. Although the consortium for USDC does not charge any fees, front-end service providers and the underlying blockchain create fees for USDC users. BitPay charges its merchants a 1% processing fee, which is potentially even higher than Mastercard interchange fees in some jurisdictions. Consumers also need to pay Ethereum-related transaction fees, called *gas fees*, for USDC payments. Unlike traditional transaction fees that are based on volumes or values, the transaction fee on the Ethereum blockchain is a function of network traffic. More specifically, transaction fees are calculated as follows:

(Base fee + tip) x amount of computational effort required to process transaction

The base fee varies from block to block according to network traffic and is the minimum fee per unit of gas that must be paid for the transaction to be accepted. Changes in the base fee for each subsequent block are capped at 12.5% to give the user some predictability over the maximum base fee they will need to pay (Ethereum 2022e). The amount of computational

[44] For details about rates in Europe and Australia, see Mastercard UK (2021) and Mastercard Australia (2022), respectively.

[45] This can be in the form of a surcharge—a separate fee added when customers choose to pay by credit card. Surcharges have been permitted in the United States since 2013 but are prohibited by some state laws (GSA 2019). As of October 6, 2022, surcharges are permitted in Canada (Evans 2022). We are unable to assess how widely merchants choose to implement the surcharge and the impacts on consumers.

[46] An exception is subscription or recurring payments on UPI, where Paytm charges merchants 5 to 65 rupees for each mandate or annual subscription plan they set up (Paytm Business 2022).

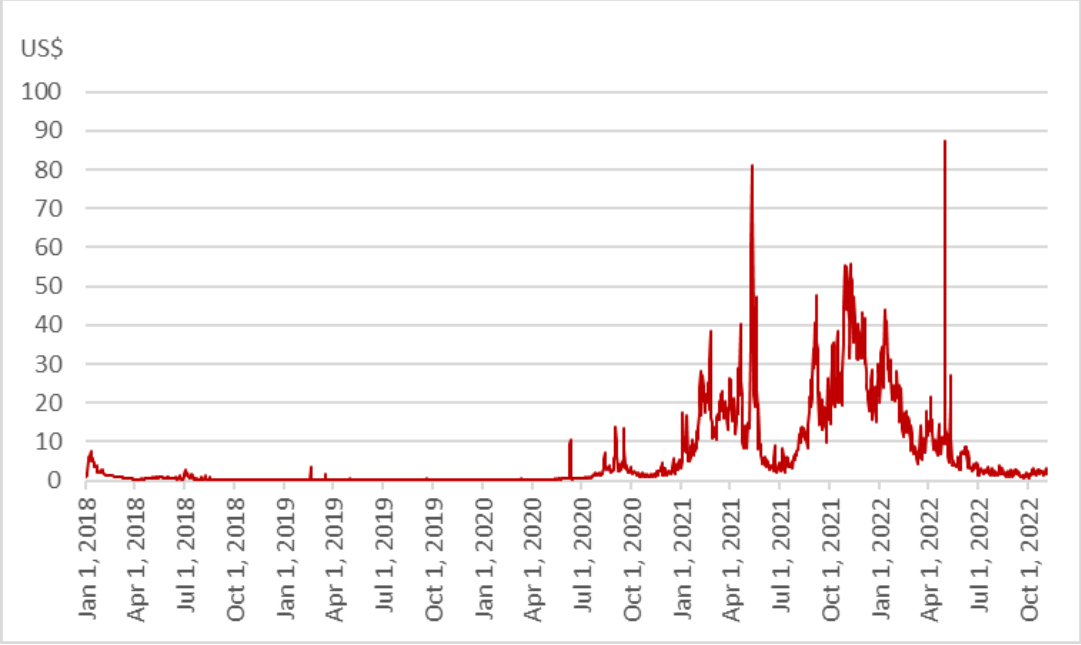
[47] Paytm has lost market share to other third-party application providers like Google and Flipkart (Parkin and Lockett 2021).

effort, measured in gas units, tends to be fixed and is estimated to be 65,000 units for a USDC transfer (Etherscan 2022).

Ethereum's fee structure is designed so that users pay more when traffic or demand for computational resources on the network is high. Given the increasing adoption of Ethereum, particularly to run more computationally intensive DeFi applications, we expect base fees to remain elevated, all else equal.[48] Compounding this issue is the fact that users have the option to pay any amount for "tips" above the base fee to out-compete other transactions for priority processing.

Chart 1 shows our estimated average daily transaction fee for an ERC-20 token transfer.[49] As crypto adoption began to accelerate in 2020, the average transaction fee, which had remained at $0.31 from mid-2015 to the end of 2019, rose to about $9.78 from 2020 to 2022. Fees spiked in May 2021 and May 2022, reaching over $80. Transaction fees have since dropped and recently declined even further, which is likely due to the collapse in cryptoasset valuations rather than technological improvements. Future improvements to Ethereum that resolve network congestion could help lower gas fees.

Chart 1: Average transaction fee for ERC-20 token transfer



Sources: Etherscan and Bank of Canada calculations Last observation: November 5, 2022

[48] Ethereum is currently the predominant blockchain on which DeFi protocols and applications function (U.S. Department of the Treasury 2021).

[49] This is calculated using the average daily gas fee obtained from Etherscan and assuming 65,000 gas units are required for the USDC transaction.

Table 9 summarizes the transaction costs for consumers and merchants for each case study.

Table 9: Comparison of transaction costs and rewards across case studies

Bank–Mastercard	Paytm–UPI	BitPay–USDC
• Consumer pays annual credit card fee and receives rewards, depending on card type • Merchant pays fee to acquirer and network and interchange fee to Mastercard; all fees are fixed percentage of transaction value	• No transaction fees for consumers or merchants • Paytm provides rewards to consumers and merchants	• Consumers pay blockchain transaction fee to Ethereum; minimum fee is variable and depends on network traffic • Merchants pay processing fee to BitPay; fee is fixed percentage of transaction value

Note: UPI is Unified Payments Interface; USDC is USD Coin.

Limitations

The findings in this paper are specific to the case studies selected and should not be interpreted as general statements about these types of payment arrangements. In particular, while the bank–Mastercard and Paytm–UPI examples could be representative of credit card and fast payment arrangements, respectively, the BitPay–USDC arrangement is more specific to fiat-backed stablecoins and non-custodial wallets and does not represent the wide variety of SAs that exist. The BitPay–USDC arrangement was chosen deliberately so that we could focus on more payments-like stablecoins and draw out contrasts with traditional payment arrangements.

Due to data limitations, we are unable to assess the total costs or overall use of resources by society for each payment method. Our findings are limited to a comparison of the private costs to end users, considering both consumer and merchant costs in the case of P2B payments. For example, we are unable to compare a payment intermediary's net liquidity costs of using a traditional payment arrangement with the costs of using an SA for a cross-border payment.

Given the sensitivity of information on a payment arrangement's cyber security controls, we also lack the data needed to assess cyber security or cyber resilience as its own attribute. Cyber security controls can influence fraud and payment system risk. Our quantitative assessment for fraud and payment system risk does not include cyber security. Instead, we take a conservative approach to fraud assessment and evaluate consumer protection policies assuming that fraud occurs, ignoring cyber security controls that could reduce the likelihood of fraud. To assess payment system risk, we look at regulatory controls rather than the system

operator's controls. It is possible that a payment arrangement has high cyber resilience even though the regulatory regime is weak.

Given the rapid evolution of technology and the accelerated pace of regulations, it remains to be seen whether the extent of benefits and risks of SAs relative to traditional payment arrangements will persist over the longer term. Our findings represent a point-in-time assessment and should not be interpreted as steady-state results.

Conclusion

Built on blockchain technology, SAs provide certain benefits but also carry particular risks and costs. We find that some attributes of SAs may make them suitable for specific payment niches in which traditional payment methods do not currently meet end users' needs. Stablecoins may appeal to users who desire more control over their privacy, are frustrated with the speed of cross-border payments or seek to develop or use more innovative products or services through the open blockchain. At the same time, SAs are more lightly regulated, offer lower consumer protections and are, at times, very expensive to use.

The stablecoin sector is rapidly changing and our findings may not hold over the long term. According to one industry report, total stablecoin supply grew from US$29 billion in 2021 to over US$140 billion in 2022, venture capital in crypto increased more than sevenfold to US$25 billion over the course of 2021, and competition among blockchains continues to intensify as they try to lower fees and attract users (The Block 2022). Similarly, regulation and the traditional payments sector continue to evolve. Will regulation erode some of the privacy or access benefits of SAs but make them safer overall? Can traditional payment intermediaries improve privacy protection and speed while keeping costs low? A wider set of case studies and other research techniques will be needed to answer these questions.

Lastly, central banks exploring the development of a retail CBDC will need to continually assess developments in the stablecoin and traditional payment markets to ensure the role and design of any planned CBDC remain relevant. Monitoring the attributes of private SAs and traditional payment arrangements should give central banks insights into where the private sector falls short and where a public digital currency could bring the most benefit to retail end users and the payment ecosystem.

Glossary

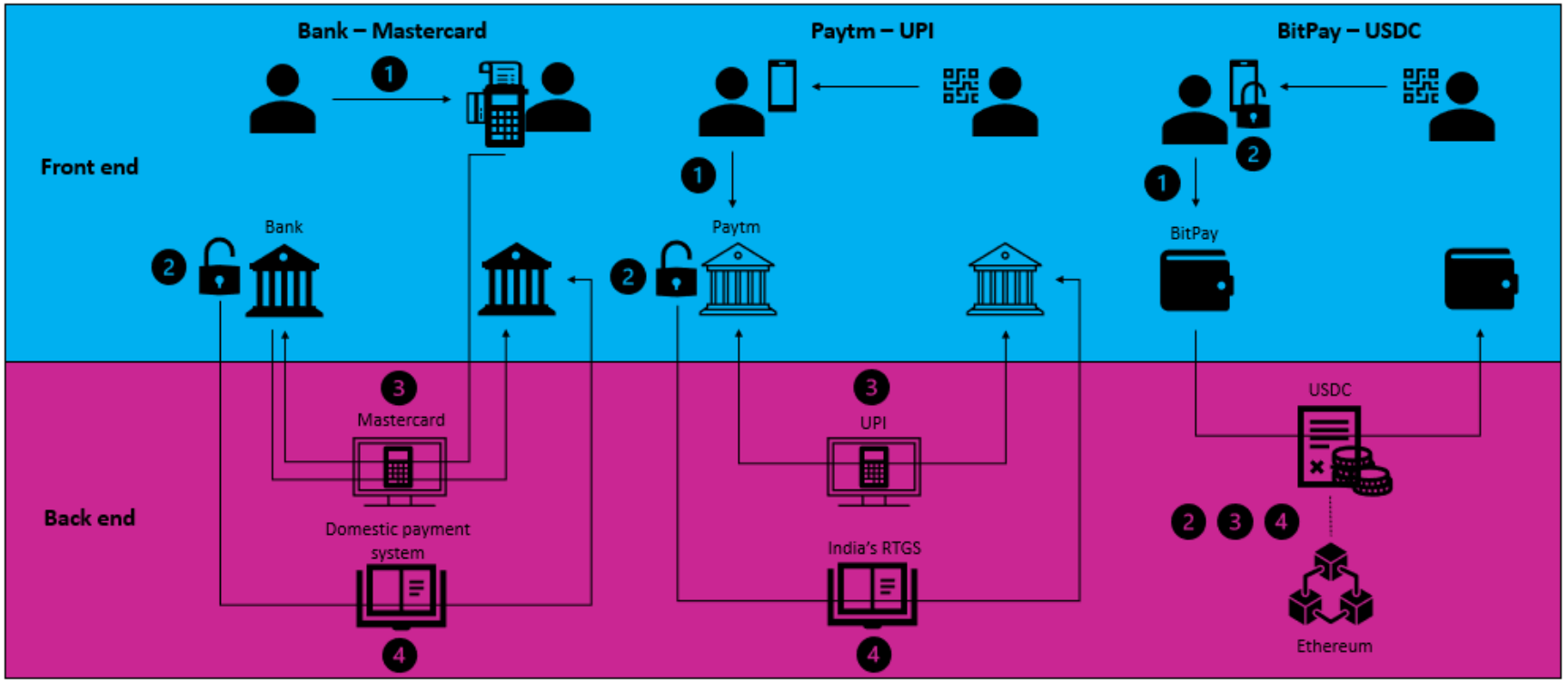
consensus algorithm	A consensus algorithm is a process or mechanism by which a set of agents in a distributed system arrive at an agreement on a single value. In distributed ledger systems, it is a process by which participants arrive at an agreement on which transactions are valid and to be committed to the ledger in the next update (Yaga et al. 2018).
DeFi	DeFi—or decentralized finance—is a general term for decentralized applications providing financial services on a blockchain settlement layer, including payments, lending, trading, investments, insurance and asset management (The Wharton School 2021).
permissionless blockchain	Permissionless blockchains, also known as trustless or public blockchains, are open networks available to everyone to participate in the consensus process (Groopman 2021). Bitcoin and Ethereum are examples of permissionless blockchain networks.
private key	Public-key or asymmetric cryptography is a cryptographic system that uses pairs of public and private keys (Yaga et al. 2018). A private key is one-half of that key pair. It is like a password, known only to its owner, while its corresponding public key is known to others. A message encrypted by one key in a pair can be decrypted by the other. Asymmetric cryptography is useful for many applications, such as encryption and digital signatures.
proof of work (PoW)	Proof of work (PoW) is a consensus algorithm popularized by Bitcoin, where one party (the prover) gains the right to publish the next block by providing verifiable proof to other parties (the verifiers) that a computational problem has been solved by the prover (Yaga et al. 2018). A key feature of PoW is that the computational problem (the "work") is difficult to solve, but its verification is easy. In Bitcoin, the purpose of the "work" is not to solve a useful problem, but rather to deter manipulation of data by establishing a large energy requirement to do so.
proof of stake (PoS)	Proof of stake (PoS) is a class of consensus protocols that operate by selecting validators in proportion to the quantity of holdings they have invested (their "stake") in the associated cryptocurrency (Yaga et al. 2018). Once invested, the stake can generally no longer be spent. PoS algorithms have been proposed as alternatives to PoW to avoid the large computational cost of the latter. While PoW schemes require parties to "invest" their computational power by doing "work," PoS schemes require them to "stake" some quantity of their holdings.
stablecoin	A stablecoin is a cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets (Financial Stability Board 2020b). Different types of stablecoin designs and stabilisation mechanisms exist.

Appendix

Case study details

Figure A-1 and **Table A-1** compare the four key steps and the actors involved in sending a payment for each of the three case studies.[50] Note that additional steps and other intermediaries (e.g., technology solution providers) may be involved that are not depicted for the purposes of this paper. **Table A-2** summarizes the key features of each case study.

Figure A-1: Processing flows of case studies



Note: UPI is Unified Payments Interface; USDC is USD Coin; RTGS is real-time gross settlement.

[50] Figure A-1 and Table A-1 cover sent payments only, not request-to-pay transactions.

Table A-1: Steps involved in sending a payment

Step	Bank–Mastercard	Paytm–UPI	BitPay–USDC
1. Initiation: A payment instruction with required credentials and transaction details is created.	Interface is provided by the payee (merchant) and its service providers. Initiation can be in person, online or mobile. After receiving the payment instruction, the payee uses service providers to route a payment message through the Mastercard network to the payor's bank (issuer). Typically, the payor's account/credit card number can be collected by the merchant.	Same as bank–Mastercard except: • The interface is provided by UPI and hosted by Paytm. • The payor initiates the instruction to its payment service provider, Paytm, which routes the message to the UPI system. • The payor and payee use aliases for routing so that account numbers do not need to be exchanged between end users.	Same as bank–Mastercard and Paytm–UPI except: • The interface is provided by BitPay. • The payor initiates the instruction by calling the USDC smart contract to execute a transfer. The instruction is broadcast to all nodes in the Ethereum network. • The payee's blockchain address is used for routing purposes.
2. Authorization: The release of funds is approved.	The payor's bank approves the release of funds after it (1) authenticates the identity of the payor using credentials entered, and (2) confirms the payor's account has sufficient funds. The pay/no-pay decision is communicated to remaining parties.	Same as bank–Mastercard.	Different from bank–Mastercard and Paytm–UPI in that: • The payor approves the release of the funds themselves by signing the transaction with their private key. • The Ethereum network checks that (1) the private keys are correct (USDCs were encrypted using the payor's public key), and (2) the payor has sufficient USDCs. • Once the two checks are passed, the transaction is added to a pool of pending transactions.
3. Clearing: Transaction is transmitted for confirmation	The payee creates a record of authorization and submits this record to its bank (acquirer) in batches at certain intervals throughout the day.	Same as bank–Mastercard except: • Individual payments are cleared in real time such that	Different from bank–Mastercard and Paytm–UPI in that transactions are continually batched but no netting occurs.

and/or final obligations for settlement are established.	The payee's bank, in turn, enters records into network clearing at certain intervals. Mastercard nets and calculates obligations arising from these submissions and reports this to direct participants.	authorization and clearing are completed in one dispatch. • UPI has 8 (net) settlement cycles throughout the day.	
4. Settlement: Funds are transferred and positions are updated on designated ledger(s) or book(s) of record.	Mastercard uses commercial banks as its settlement banks. Its rules stipulate to which settlement banks and by when participants need to send payments for settlement. Participants use other payment systems to send (receive) funds to (from) the settlement bank. Given the size of transactions, participants typically need to use the domestic large-value payment systems. Funds are typically made available to the payee after settlement, depending on the contract between the payee and the payee's bank.	Same as Bank–Mastercard except: • The Reserve Bank of India is the settlement bank. • Funds are made available to the payee immediately after the payment is authorized/cleared, not after settlement occurs.	Different from bank–Mastercard and Paytm–UPI. Validator nodes batch transactions from the pending pool to create a "candidate block" that can be added to the blockchain. The nodes are incentivized to include transactions that provide higher fees. When a new block needs to be proposed, the Ethereum protocol will randomly select a validator with probability proportional to the amount of ETH held by the validator (its "stake"). A committee of validators is also randomly chosen to determine and vote on the validity of the block proposed. Once consensus is achieved by these validators, all nodes and their record of the Ethereum blockchain are subsequently updated. After technical settlement, the USDC coins transferred are encrypted using the payee's public key and can be unlocked or transferred only by using the payee's private key.

Note: UPI is Unified Payments Interface; USDC is USD Coin.

Table A-2: Key features of case studies

a. Back-end payment arrangements

	Mastercard	UPI	USDC
Type	Credit card	Fast payment system	Stablecoin
Use cases	P2B	P2P, P2B, B2P, B2B	P2P, P2B
Access	Canada: 18 issuers,[51] 10 merchant service providers[52]	• 237 bank issuers • 45 payment service providers • 22 third-party applications	• 1 non-bank issuer (Circle) • 19 non-bank wallet providers • 21 third-party applications
Settlement mechanism	Settlement accounts held at private commercial banks	Settlement accounts held at India's central bank, the Reserve Bank of India	Ethereum uses RTGS, as do most others
Settlement frequency	DNS; number of settlement cycles per day may vary by country	DNS with 8 settlement cycles per day	Batch RTGS with a batch (block) settled every 15 seconds
Jurisdictions	Headquartered in the United States and operates in jurisdictions across North America, Latin America/Caribbean, Europe, Asia/Pacific and Middle East/Africa[53]	India UPI will be interlinked with Singapore's PayNow fast payment system in the second half of 2022	No technical limits to where public networks like Ethereum can operate, needs a single node
Regulators	Regulation varies by jurisdiction Canada: Unregulated Europe: Regulated by the European Central Bank in accordance with the *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements*	Reserve Bank of India	Networks such as Ethereum are unregulated by most governments, but this may change in the future[54]

Note: UPI is Unified Payments Infrastructure; USDC is USD Coin; P2B is person-to-business; P2P is person-to-person; B2P is business-to-person; B2B is business-to-business; DNS is deferred net settlement; RTGS is real-time gross settlement.

[51] See Mastercard (2022c).

[52] See Mastercard (2022d).

[53] See Mastercard (2022e).

[54] See Browne (2021).

b. Front-end service providers

	Traditional bank	Paytm	BitPay
Type	FI	Non-traditional bank that is a PSP	Cryptocurrency wallet
Registration or set-up process	Canada: FI customers apply online or at a branch. A credit card is granted based on an assessment of creditworthiness. The process may be more complex for applicants who are not FI customers.	1. Download app 2. Register as customer (select SIM card) 3. Add bank account 4. Generate UPI PIN	Self-set-up via app download[55]
Funding process	No pre-funding. Credit is accumulated up to the permitted limit and must be repaid within the period stipulated in the terms and conditions, otherwise interest is incurred.	No pre-funding. App allows end users to directly access funds in their Paytm Payments Bank account	Buy with credit card[56] or buy in exchange and transfer to wallet[57]
Jurisdictions	Any jurisdiction with a banking sector subject to the regulations described below	India[58]	Headquartered in the United States and operates in other jurisdictions except those in lists of sanctioned and prohibited jurisdictions[59]
Regulators	Applicable banking supervisory authorities under standards prescribed by the Basel Committee on Bank Supervision	Licensed to operate as a payments bank by the Reserve Bank of India	A registered Money Services Business with the Financial Crimes Enforcement Network of the U.S. Department of the Treasury and a licensed money transmitter in US states where applicable law requires it to be licensed[60]

Note: FI is financial institution; PSP is payment service provider; SIM is subscriber identify module; UPI is Unified Payments Interface; PIN is personal identification number.

Assessment framework

Table A-3: Attribute assessment framework

a. Description of attributes

Attribute	Description
Fraud	The degree to which the end user is compensated for financial loss due to unauthorized and/or authorized fraud.
Payment system and financial crime risk	Payment system risk refers to the legal, financial, operational (including security) and settlement risks that can arise from settlement of obligations between participants in the payment system and that can subsequently disrupt the payment system. Financial crime risk refers to money laundering and terrorist financing risk.
Speed	The time between initiation of a payment and when funds can be made available to the final recipient on an irrevocable basis. The funds availability and irrevocability rules of both the front- and back-end service provider are considered.
Convenience	The ease of initiating transactions in the payment arrangement and the ability of the payment arrangement to accommodate a range of payment activities (e.g., for a variety of merchants or use cases, within or outside regular business hours).
Cost	The explicit costs (e.g., per-transaction and non–per transaction fees) incurred by end users when using a payment arrangement.
Access	The ease with which an entity can participate directly or indirectly in the payment arrangement.

[55] See BitPay (2022c).

[56] See BitPay (2022d).

[57] See BitPay (2022e).

[58] Paytm Payments Bank Ltd. is largely controlled by One97 Communications Ltd., which has other subsidiaries that may operate in the payments business. These include operations in Canada, the United States, Singapore, Dubai, Saudi Arabia, China and other countries in Africa. See One97 Communications (2021).

[59] See BitPay (2022f).

[60] This is applicable to BitPay Inc. For more information, see BitPay (2022g).

Financial inclusion	The extent to which the payment arrangement can be used by a broad set of end users who may or may not have access to the formal banking system. Designs that are intended to address barriers such as geographic remoteness, digital literacy and access to information technology are also considered.
Privacy	The extent to which personal information is collected and stored by the front- or back-end service providers and disclosed to parties other than the service providers, as well as the regulation of these processes in the payment arrangement.

b. Quantitative scoring methodology

	Scoring Criteria
Fraud	
End-user redress for fraud	1 = end user is always liable, 2 = end user may have zero liability for unauthorized fraud, 3 = end user has zero liability for unauthorized fraud
Payment system and financial crime risk	
Stability of settlement asset	1 = claim on non-bank, 2 = claim on private bank, 3 = claim on central bank
Regulation of payment system	1 = no, 2 = yes but inconsistent with PFMIs, 3 = yes but consistent with PFMIs
Regulation of AML/CTF risks	1 = no, 2 = yes—developing framework, 3 = yes—mature regulatory framework
Speed	
Funds availability to payee	1 = > 1 day, 2 = same day, 3 = near-immediate
Convenience	
Ease of initiation	1 = poor, 2 = good, 3 = excellent
Use cases	1 = narrow set of use cases, 2 = moderate set of use cases, 3 = broad set of use cases
24/7/365 availability	1 = no—normal business hours in one time zone, 2 = no—normal business hours in multiple time zones, 3 = yes

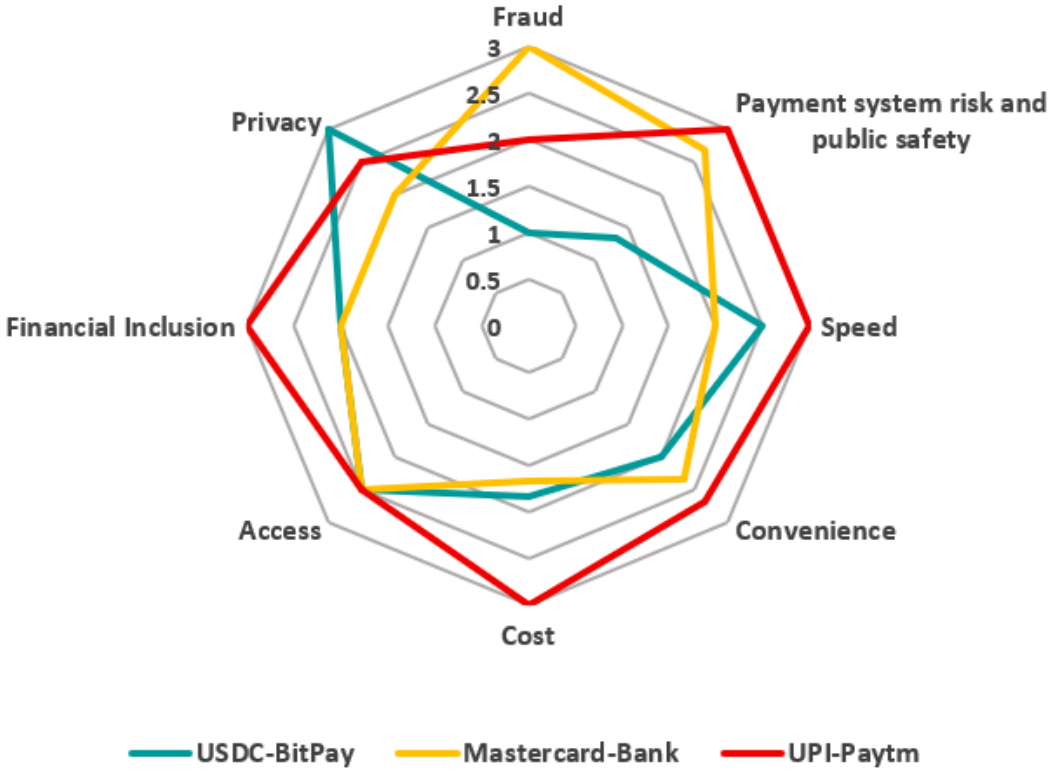
Cost	
Per-transaction fee	1 = yes, 2 = depends, 3 = no
Non–per transaction fee	1 = yes (e.g., annual membership or subscription fees), 2 = depends, 3 = no
Ability to receive rewards	1 = no, 2 = depends, 3 = yes (e.g., loyalty points, cash back rewards)
Access	
Eligibility requirements for participation	1 = banks, 2 = banks plus licensed financial institutions and payment service providers, 3 = none
Availability of API standards	1 = no, 2 = yes—for less advanced payment functions, 3 = yes—for advanced payment functions
Financial inclusion	
Technological barriers	1 = advanced or specialized technology required, 2 = modern technology required (e.g., high-speed internet, mobile phones), 3 = basic technology required (e.g., card, low-speed or dial-up internet)
Non-technological barriers	1 = none, 2 = features address one accessibility barrier, 3 = features address multiple accessibility barriers
Privacy	
Personal information collected	1 = disproportionate for purposes of processing payments (e.g., payment purpose, social network profile, location), 2 = proportionate to purposes of processing payments (e.g., card/account number, participants, amount), 3 = less than typically required for processing payments (e.g., no identity)
Disclosure of personal information	1 = disclosed to other third parties (e.g., advertisers, affiliates of operator), 2 = disclosed to merchant, 3 = disclosed only to payments system/payor's agent or authorities

Note: PFMIs are the Principles for financial market infrastructures; AML is anti–money laundering; CTF is counter-terrorist financing; API is application programming interface.

Results of quantitative assessments

For illustrative purposes, **Figure A-2** shows the simple average of the individual feature scores underlying each attribute. Varying weights could be assigned to each feature but would depend on the perspective taken. Scores range from 1 to 3, with 1 (3) being least (most) attractive for that attribute. The quantitative assessments are complemented by a qualitative analysis that is not reflected in the figure below.

Figure A-2: Attributes of retail payment arrangements



Note: UPI is Unified Payments Interface; USDC is USD Coin.

Are stablecoins more beneficial for financial inclusion?

Financial inclusion refers to access to useful and affordable financial services (World Bank 2022). It is often measured by calculating the proportion of adults with access to a transactional (e.g., chequing) account. According to the World Bank, 31% of the global adult population still does not have access to an account at a financial institution or mobile money service provider, which is a substantial gap (Demirgüç-Kunt et al. 2022).

Proponents of digital currencies believe that these innovations can help close this gap. Recall Facebook's Diem stablecoin project that was heralded as a solution for the unbanked.[61] This is because blockchain participation is open to all and theoretically does not require real-world identifications, which the unbanked may lack.

It is not clear whether stablecoins naturally address more barriers to financial inclusion than some traditional payment systems purposely designed to be more inclusive. In India, the government has made a concerted effort to improve financial inclusion by, among other things, improving accessibility of UPI payments. We compare USDC and UPI in terms of their ability to address technology, geographical reach, cost and identification barriers to financial inclusion.

- **Technology**: A USDC user must have access to a smartphone and high-speed internet, which can be lacking in remote regions where the financially excluded are often located. In contrast, UPI can process transactions carried out through non-smart "feature" phones, a process akin to telephone banking, in addition to online transactions initiated in the same way as those for USDC.
- **Geographical reach**: To address segments of the population excluded due to their reliance on cash and their remote locations, a payment service should provide a combination of physical and electronic access points with broad geographical reach to be considered financially inclusive. This would be a challenge for USDC, which does not have a network of cash acceptance terminals (e.g., Bitcoin automated teller machines) that allow exchange of cash for USDC or another cryptocurrency exchangeable for USDC. However, it is still possible for the unbanked to fund their crypto wallets through international electronic remittances from family and friends, which avoids geographical barriers. In contrast, UPI is supported by a vast network of physical and electronic access points.
- **Cost**: The transaction costs for USDC transactions—at least those carried on-chain—can be very high, depending on the blockchain used (see section on risks and costs). For Ethereum-based USDC transactions, we estimate peak costs of $81.20 per transaction. In contrast, UPI transactions are free for end users—a regulatory requirement. For cross-border payments, however, USDC payments could be cheaper than using a chain of traditional payment systems and intermediaries because nodes other than UPI may add costs.

[61] The Diem payment system is intended to facilitate a more accessible and connected global financial system. For more information, see Diem Association (2022).

- **Identification**: Combined with wallets that do not require identification checks, USDC can be more financially inclusive than UPI payments in this respect. However, alternative solutions do exist to make traditional payment systems accessible to individuals without access to typical identifications. In India, the government created a digital identification system known as Aadhaar to help improve financial inclusion (Unique Identification Authority of India 2022). An Aadhaar number can be issued to any resident of India, and UPI's Aadhaar Enabled Payment System enables customers to initiate payments with only their Aadhaar number and fingerprint (National Payments Corporation of India 2022c).

References

Banco Central do Brasil. 2020. Pix: Powered by Banco Central.

Bank for International Settlements. 2016. "Fast Payments – Enhancing the Speed and Availability of Retail Payments." Committee on Payments and Market Infrastructures (November).

Bank for International Settlements. 2019. "Report on Open Banking and Application Programming Interfaces." Basel Committee on Banking Supervision (November).

Bank for International Settlements. 2020. *Central Bank Digital Currencies: Foundational Principles and Core Features*.

Bank for International Settlements. 2022. "Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements." Committee on Payments and Market Infrastructures Papers, July 13.

Bech, M. L., U. Faruqui and T. Shirakami. 2020. "Payments Without Borders." *BIS Quarterly Review* (March 1).

BitPay. 2019. How to Use Ethereum and Stablecoins.

BitPay. 2022a. How Do I Complete the BitPay ID Process?

BitPay. 2022b. When Will my Payment Confirm?

BitPay. 2022c. How to Create a Wallet in the BitPay Wallet App.

BitPay. 2022d. How Do I Buy Crypto through Simplex?

BitPay. 2022e. How Do I Load My BitPay Wallet?

BitPay. 2022f. Why Can't I Use BitPay's Services in My Country?

BitPay. 2022g. Terms of Use.

Brito, J. and P. Van Valkenburgh. 2022. "U.S. Treasury Sanction of Privacy Tools Places Sweeping Restrictions on All Americans." Coin Center, August 8.

Browne, R. 2021. "China's Central Bank Says All Cryptocurrency-Related Activities are Illegal, Vows Harsh Crackdown." CNBC, September 24.

Carrière-Swallow, Y., V. Haksar and M. Patnam. 2021. "India's Approach to Open Banking: Some Implications for Financial Inclusion." International Monetary Fund Working Paper No. 21/52.

Centre. 2022. Introducing USD Coin: A Stablecoin Brought to You by Circle and Coinbase.

Chapman, J., J. Chiu, S. Jafri and H. P. Saiz. 2015. "Public Policy Objectives and the Next Generation of CPA Systems: An Analytical Framework." Bank of Canada Staff Discussion Paper No. 2015-6.

Circle. 2021. "Our Journey to Become a National Digital Currency Bank." Circle Blog, August 9.

Circle. 2022. Enterprise Ready Custody & Security of Digital Currency.

Cleland, V. 2021. "Working Together to Enhance Cross-Border Payments." Speech at the Central Bank Payments Conference (delivered virtually), November 22.

Diem Association. 2022. Welcome to the Diem Project.

Demirgüç-Kunt, A., L. Klapper, D. Singer and S. Ansar. 2022. The Global Findex Database 2021 – Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. World Bank report.

Ethereum. 2022a. ERC-20 Token Standard.

Ethereum. 2022b. Blocks.

Ethereum. 2022c. The Ethereum Vision: A Digital Future on a Global Scale.

Ethereum. 2022d. Sharding.

Ethereum. 2022e. What is Gas?

Etherscan. 2022. Ethereum Gas Tracker.

European Central Bank. 2020. Decision of the European Central Bank of 4 May 2020 on the Identification of Mastercard Clearing Management System as a Systemically Important Payment System Pursuant to Regulation (EU) No 795/2014 on Oversight Requirements for Systemically Important Payment Systems (ECB/2020/26).

European Data Protection Supervisor. 2019. "International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights." 41st International Conference of Data Protection and Privacy Commissioners, October 21–24, Tirana, Albania.

Evans, P. 2022. "Paying with a Credit Card? Expect to See a Fee when You Shop Under New Rules that Start Now." CBC News, October 6.

Felt, M.-H., F. Hayashi, J. Stavins and A. Welte. 2021. "Distributional Effects of Payment Card Pricing and Merchant Cost Pass-through in Canada and the United States." Bank of Canada Staff Working Paper No. 2021-8.

Financial Action Task Force. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

Financial Stability Board. 2019. Decentralised Financial Technologies – Report on Financial Stability, Regulatory and Governance Implications. June 6.

Financial Stability Board. 2020a. Enhancing Cross-Border Payments—Stage 1 Report to the G20: Technical Report Background. April 9.

Financial Stability Board. 2020b. Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. Oct 13.

Garratt, R. and M. van Oordt. 2019. "Privacy as a Public Good: A Case for Electronic Cash." Bank of Canada Staff Working Paper No. 2019-24.

Gemini. 2022. What Was the DAO? Cryptopedia, March 16.

Grant Thornton LLP. 2021. Independent Accountant's Report. September 30.

Groopman, J. 2021. "Permissioned vs. Permissionless Blockchains: Key Differences." TechTarget, June 1.

GSA SmartPay. 2019. Surcharges: Common Questions about Surcharges and Convenience Fees.

Haqshanas, R. 2021. "First Monero and Ethereum Atomic Swap Completed on Arbitrum." Cryptonews. November 30.

Hyman, V. 2021. "Swiping Left on Magnetic Stripes." Mastercard Newsroom, August 12.

IEEE Xplore. 2022. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract.

International Organization of Securities Commissions. 2020. "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms – Final Report." Board of the International Organization of Securities Commissions, February 2020.

Kosse, A., H. Chen, M.-H. Felt, V. Dongmo Jiongo, K. Nield and A. Welke. 2017. "The Costs of Point-of-Sale Payments in Canada." Bank of Canada Staff Working Paper No. 2017-4.

Kosse, A., Z. Lu and G. Xerri. 2020. "An Economic Perspective on Payments Migration." Bank of Canada Staff Working Paper No. 2020-24.

Mastercard Developers. 2022. Mastercard Developers.

Mastercard. 2021. Mastercard Canada Interchange Programs.

Mastercard. 2022a. Cross-Border Services.

Mastercard. 2022b. Zero Liability Protection

Mastercard. 2022c. Mastercard Credit Cards.

Mastercard. 2022d. Find an Acquirer and Get Started Accepting Payments.

Mastercard. 2022e. Global Locations.

Mastercard Australia. 2022. Understanding Interchange.

Mastercard UK. 2021. Intra-EEA – Intercountry Interchange Fees.

Monetary Authority of Singapore. 2021. "Singapore's PayNow and India's UPI to Link in 2022." Media release, September 14.

MoneyGram International Inc. 2021. "MoneyGram Announces Innovative Partnership with the Stellar Development Foundation to Utilize Blockchain Technology." Press release, October 6.

National Payments Corporation of India. 2022a. UPI Live Members.

National Payments Corporation of India. 2022b. UPI Dispute Redressal Mechanism.

National Payments Corporation of India. 2022c. AePS Product Overview.

Office of the Privacy Commissioner of Canada. 2018. "Summary of Privacy Laws in Canada." January.

One97 Communications. 2021. Prospectus.

Parkin, B. and H. Lockett. 2021. "Paytm Shares Fall 27% on Trading Debut after India's Biggest IPO." *Financial Times*. November 18.

Paytm. 2022. Secure Payments with Paytm. Developer documentation.

Paytm for Business. 2022. Pricing.

Reserve Bank of India. 2017. Index to RBI Circulars: Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. July 6.

Reserve Bank of India. 2020. "Reserve Bank of India publishes the Oversight Framework for Financial Market Infrastructures and Retail Payment Systems." Press release, June 13.

Reserve Bank of India. 2021. "India and Singapore to Link Their Fast Payment Systems – Unified Payments Interface and PayNow." Press release, September 14.

Sigalos, M. 2021. "Why Some Cyber Criminals are Ditching Bitcoin for a Cryptocurrency Called Monero." CNBC, Crypto Decoded. June 14.

Statista. 2022. Number of Cryptocurrencies Worldwide from 2013 to February 2022. March 22.

The Block. 2022. Stablecoins.

The Wharton School. 2021. "DeFi Beyond the Hype – The Emerging World of Decentralized Finance." Wharton Blockchain and Digital Asset Project, University of Pennsylvania.

The World Bank. 2022. Financial Inclusion: Overview.

U.S. Department of the Treasury. 2021a. "Report on STABLECOINS." President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. November.

U.S. Department of the Treasury. 2021b. "Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitPay, Inc." Press release, February 18.

U.S. Department of the Treasury. 2022a. "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats." Press release, May 6.

U.S. Department of the Treasury. 2022b. "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash." Press release, August 8.

Unique Identification Authority of India. 2022. About Your Aadhaar.

Visa. 2021. "Digital Currency Comes to Visa's Settlement Platform." The Visa Blog. March 29.

Yaga, D., P. Mell, N. Roby and K. Scarfone. 2018. "Blockchain Technology Overview." National Institute of Standards and Technology Internal Report 8202 (October).

Zcash. 2021. How it Works.