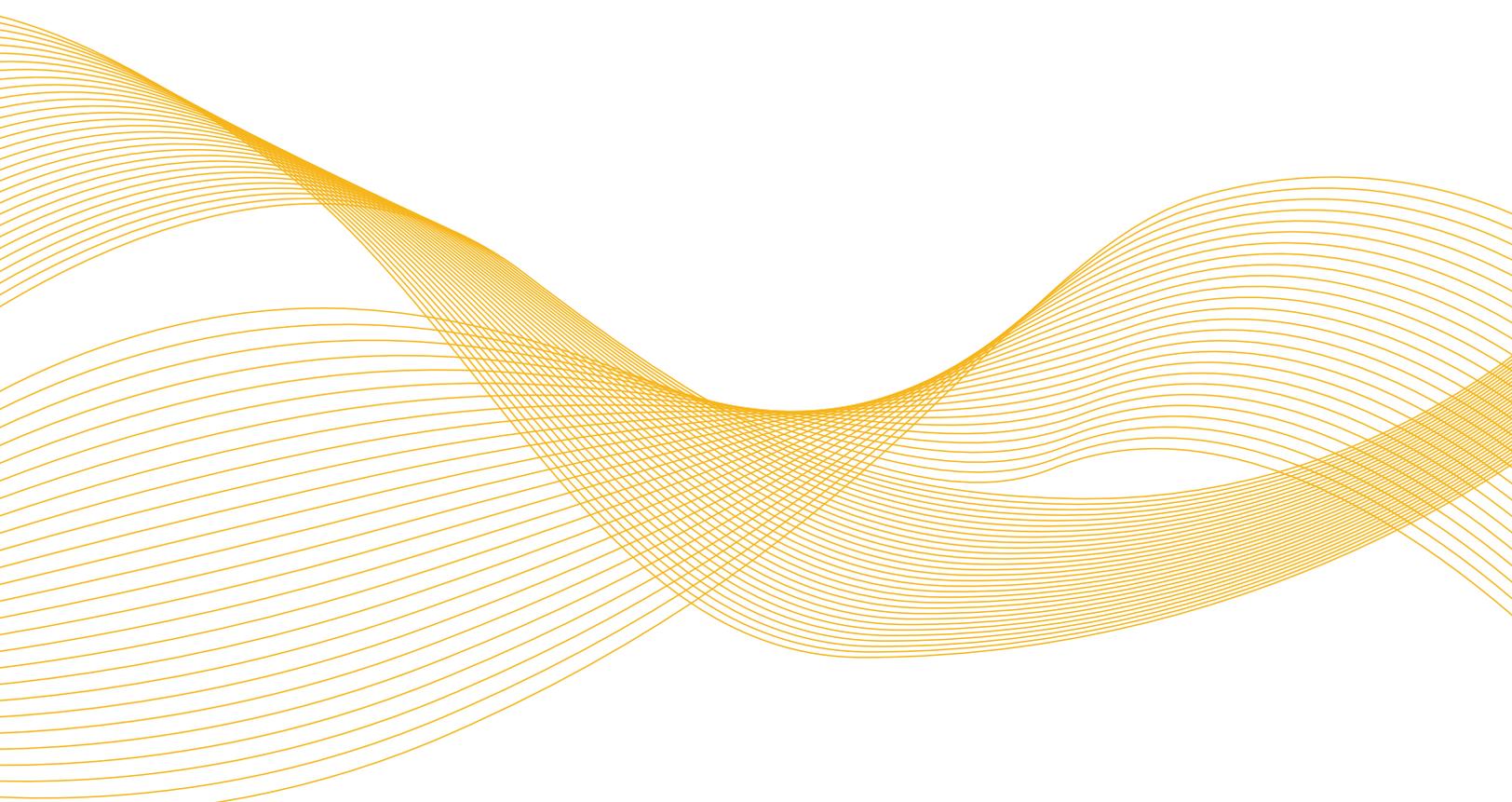




Imagining an Open
Future for Payments

Cross-border payments for Central Bank Digital Currencies via Universal Payment Channels*

Mahdi Zamani, Erin English, Ranjit Kumaresan, Mihai Christodorescu, Wanyun
Catherine Gu, Chad Harper, Cuy Sheffield, Mohsen Minaei, Srinivasan Raghuraman



Synopsis

Growing interest in digital forms of payments have led central banks around the world to explore the possibility of issuing a new type of central bank money, known as *Central Bank Digital Currency (CBDC)*. While we anticipate many central banks will implement some form of a digital ledger, it is unlikely that they all adopt the same stack of technologies and protocols due to, for example, different governance, market requirements, technology providers, and compliance standards. These differences would limit the interoperability of CBDC networks, which could add friction to future cross-border CBDC payments. Critically, the Bank of International Settlements (BIS) is analyzing these issues as well as evidenced in its recent analysis of a multiple CBDC (mCBDC) arrangement.

In this paper, we will focus on the challenges of cross-border payments in the emerging age of CBDCs. We will also envision and evaluate scenarios of how cryptographic interoperability protocols for CBDCs could allow digital money to be moved between these networks. Specifically, we propose cross-border CBDC payment routes called *Universal Payment Channels (UPC)* that could allow instant transfer of funds across CBDC ledgers. We further discuss the technical trade-offs policymakers will need to consider prior to choosing the right interoperability method. As with all considerations regarding CBDC, these decisions will be based upon the unique objectives of a particular central bank and how it envisions the future CBDC ecosystem. Finally, through the paper, we will analyze some of the broader opportunities and challenges of cross-border CBDC payments going forward.



Cross-border payments for Central Bank Digital Currencies via Universal Payment Channels

October 2021



Visa Economic Empowerment Institute





Acknowledgments

This report is a collaboration between Visa Research, Visa Crypto, and the Visa Economic Empowerment Institute. The authors would like to thank the Committee on Payments and Market Infrastructures and the conference committee for the virtual conference, “Pushing the frontiers of payments: towards faster, cheaper, more transparent and more inclusive cross-border payments,” for which this paper was accepted in March 2021. The CPMI recently published this paper in its volume of conference proceedings.

About the Visa Economic Empowerment Institute

The VEEI is a non-partisan center of excellence for research and public-private dialogue established by Visa.

The VEEI’s overarching mission is to promote public policies that empower individuals, small businesses, and economies. It produces research and insights that inform long-term policy within the global payments ecosystem. Visa established the VEEI as the next step in its ongoing work to remove barriers to economic empowerment and to create more inclusive, equitable economic opportunities for everyone, everywhere.

Visit: visaeconomicempowermentinstitute.org

Index

1. Introduction	7
2. Technical Considerations	10
3. Cross-Border Payments Using Universal Payment Channels	14
4. How to think about the way ahead	18
References	21
Disclaimer	23

1. Introduction

As the Bank for International Settlements (BIS) observed in January 2021, approximately 86 percent of central banks have engaged in some sort of work on central bank digital currencies (CBDC) – a 10 percent increase from the previous year [1]. It is still too early to know whether all of these central banks will follow through and ultimately build a CBDC system, but if they do, this gives rise to a technology and policy challenge: how can multiple CBDC platforms, potentially using different technologies, interoperate and conduct cross-border payments (XBPs)? Understandably, most central banks are principally focused for the moment on the domestic use cases for CBDC. However, as noted in a report on CBDC by the International Monetary Fund (IMF) in 2020, “it would seem prudent for central banks to consider coordinating their CBDC efforts closely and introducing sufficient flexibility into their CBDC designs to facilitate cross-border interoperability and standardization across CBDC implementations. [9]”

In early 2020, the Financial Stability Board (FSB) initiated a study of XBPs in response to a request by the Group of 20 (G20) and identified the challenges of existing XBP arrangements. [2] The FSB Stage 1 report identified seven friction points in the existing cross-border process: fragmented messaging formats, complexity of compliance checks, limited operating hours, legacy technology

platforms, funding costs, long transaction chains, and weak competition.

Anticipating these challenges, the Committee on Payments and Market Infrastructures (CPMI) of the BIS initiated a study to examine ways to improve XBPs [3], which in a CBDC ecosystem, translate to methods for interlinking multiple and likely disparate CBDC systems. Even before the arrival of CBDCs, the private sector has been investing in and testing

new technologies to reduce these frictions and building solutions. This is what the BIS might call “new multilateral platforms” and what Visa would call global open networks², both of which share a common aim to enhance global money movement. Depending on the design, central banks are not immune from these frictions for XBP, and should central banks continue to pursue CBDC solutions, they will inevitably encounter new interoperability risks. Without a mechanism or framework to ensure CBDC interoperability, these risks could have wider implications for global cross-border payments.



Central Banks are not immune from the frictions of cross-border payments

² Visa Direct (for low value payments) and Visa B2B Connect (for larger value business-to-business payments) are examples of these new cross-border capabilities.

In the case of a token-based CBDC, consumers could be given the option of buying foreign currency in advance, before spending it abroad. According to a BIS report in 2020 on the technology of retail CBDC, if a CBDC is based on a token, it will by default be open to foreign residents. In this scenario, digital wallets could be the interface with foreign exchange markets – an important issue on the minds of central banks [11]. To help explain the attributes of this scenario, two of the core features of a token-based CBDC are (1) CBDC funds will likely be able to travel across systems that are not necessarily owned or maintained by its issuer (i.e., the central bank); and (2) like cash, CBDC is a type of bearer instrument, whose ownership is tied to a pair of cryptographic keys and the authenticity of that money can be verified cryptographically. This contrasts with the account-based model traditionally adopted by commercial banks, where instead of tying the holder’s ownership to the money itself, the ownership is tied to a bank account that may not move as freely.

Inevitably, individuals will use CBDCs for retail and XBP, and this activity will almost certainly use – to some extent – the existing network of corresponding banks. According to the International Monetary Fund (IMF), “A correspondent banking arrangement involves one bank (the correspondent) providing a deposit account or other liability accounts, and related services, to another bank (the respondent),

often including its affiliates. The arrangement requires the exchange of messages to settle transactions by crediting and debiting those accounts [14].” This model was adopted primarily because the bank used by the source and destination are the most familiar and specialized in their respective jurisdiction: to make a payment, it is only necessary to find one or a chain of correspondent banks that can connect the source and destination banks via nostro/vostro

(ours/yours) accounts held at each bank. Cross-border payment volumes have grown steadily in recent years, driven by several factors, including global e-commerce, migration trends, and global supply chains, among others. Among these volumes are digital remittances, whose growth has accelerated in recent years [9].

As these payment volumes have grown, there has been a concomitant focus on the complexity of the existing cross-border payments process. This complexity is due to several underlying factors, including higher fraud rates compared to domestic transactions; higher technology requirements for authorization, clearance and settlement; and regulatory compliance requirements. Given the complex nature of international transactions, processing for these transactions is more costly than processing for domestic transactions. Maintaining such an advanced, reliable, and robust network requires ongoing investment in technology, product development, risk mitigation, fraud detection capabilities, and regulatory compliance. While the aforementioned new multilateral platforms resolve many of the challenges introduced by correspondent banking and make XBPs faster, cheaper, and more transparent, innovations will also be needed with regard to moving CBDCs across borders.



Policymakers are focusing on the complexity of cross-border payments

It is critically important for a CBDC ecosystem to support, and not complicate, an already robust cross-border payment system [1] that markets have come to depend upon.² While most CBDCs will likely implement some form of a digital ledger, it is unlikely that they all adopt the same stack of technologies



CBDCs will likely use different technology stacks and different protocols—somehow they will need to interoperate with each other

and protocols due to, for example, different governance, market requirements, technology providers, and levels of monitoring and compliance standards required by central banks. This would, unfortunately, limit the interoperability of CBDC networks which is a crucial requirement for implementing frictionless, cross-border CBDC payments.

Adding a novel technology and type of money, such as a CBDC, could further complicate these challenges for banks that are moving these transactions.

In this paper, we envision and evaluate scenarios of how various CBDC networks could operate around the world, and how cryptographic interoperability protocols could allow digital money to be moved between these networks. Specifically, we propose cross-border CBDC payment routes called *Universal Payment Channels (UPC)* that allow instant transfer of funds across CBDC ledgers. We discuss the technical trade-offs policy designers need to consider in order to choose the right interoperability method based on the requirements of a particular CBDC ecosystem. Finally, we will evaluate the road ahead for policymakers.

² More efficient XBP arrangements could result in higher cross-border capital flows causing issues such as exchange rate volatility in emerging markets and monetary policy dependencies between central banks [5]. Such issues could be curbed by setting certain policies on the volume of funds moved by XBPs while still providing XBP efficiency guarantees.

2. Technical considerations

While CBDCs could bring efficiency to domestic economies partly through unified technologies for minting, distribution, and payment rails, envisioning similar unified models for cross-border payments between independent CBDC networks would be challenging. Existing CBDC initiatives involve different motivations, strategies, legislation, regulations, guidelines, and standards. These unique, but ultimately fragmented, CBDC initiatives could significantly impact their interoperability with other CBDC networks. Many international organizations have already begun working on the technologies behind these concepts and can encourage further industry dialogue. This includes the BIS, the IMF, the Organization for Economic Co-operation and Development (OECD), and standards setting bodies such as the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), and the Internet Engineering Task Force (IETF).

While international standards usually take a long time to form and be adopted, significant progress has been made in the past decade in the research, development, and operation of digital currencies as well as interoperability practices in the last few years, which could pave the way for faster standardization and adoption. Fortunately, many of these practices could also be potentially proposed and adopted as international standards. In this section, we review these practices and discuss their design challenges.

2.1 Ledger technology

Record keeping is a key feature of money transfers. Whereas a payment also provides value to consumers in terms of the confidence that they can exchange money for goods, the speed of authorization and of settlement as well as the certainty of the degree of protection they have if payments go wrong are also critical. In a digital world, all these attributes are highly relevant. At the core of every digital currency system, there is a digital record of all of the transactions that have taken place in the system. Such a digital ledger is used to track the balances of the system's users and is essentially a digital bulletin board, where all transactions in the system are posted [5]. Depending on the resiliency and trust requirements, a digital ledger may be implemented using a centralized database controlled by a trusted third party, a decentralized ledger with no central point of control or something in between such as a permissioned ledger. Regardless of the degree of centralization, a digital ledger, which is a digital record and an assurance of a transfer of value, typically needs to be distributed (i.e., replicated) geographically. This inherent resiliency is unique to DLT and can help mitigate crash failures and malicious corruptions of its nodes. This ledger topology is generally referred to as a *distributed ledger technology (DLT)*.

Under a DLT network, there consists of (1) a set of computers known as nodes that store the ledger data, (2) a communication network for the node(s) to receive transactions and possibly communicate with each other, and (3) a set of protocols that describe precisely how the nodes can process and store the transactions securely. A *consensus protocol* executed by the nodes guarantees that even large subsets of them cannot

collude to maliciously modify the ledger. Furthermore, a stack of network protocols ensures reliable delivery of messages and an identity protocol prescribes how participants can obtain identities in the form of digital signature keys to join the consensus protocol and/or create transactions. Additionally, and perhaps critically, the consensus protocol process improves the overall robustness and security of the network and mitigates the likelihood that a cyber threat actor can compromise, corrupt, or manipulate the network's integrity. In short, DLTs can enhance information assurance – a key cybersecurity attribute.

Two major issues with DLT protocols are scalability and interoperability. For scalability, consensus protocols create redundancy by copying data across multiple machines. This unfortunately creates an inherent overhead

to ensure that all or most of the copies are in sync. Consensus protocols are usually designed in a way to ensure certain guarantees in the system they operate in; these protocols are not recognized by nodes in other blockchain systems. This individuality of networks introduces an inherent challenge in communication between multiple systems.

We note that DLT can be used as a mechanism to provide performance

benefits to the underlying system. Nevertheless, there is a natural tension between decentralization and the performance gains of going distributed and we expect different DLTs to make distinct design choices to find the optimum tradeoff. Regardless of this tradeoff, we believe that scalability and interoperability challenges generally appear in some degree in any DLT system.

In the context of CBDCs, DLTs can provide central banks with a unique degree of control and insight into the monetary system without requiring them to build and implement the technology [5]. DLTs can enable automatic verification of ledger events to external entities, and depending on the ledger design and governance procedures, can even do so to ensure a level of privacy. From a XBP perspective, DLTs, if used properly, could offer the potential for reliable tracking of different stages of trade and financial transactions [5] as the transaction travels across different CBDC networks (see Section 2.3). Relatedly, a DLT may optionally be able to execute computer programs, called smart contracts. A smart contract execution may be initiated by either a transaction submitted to the ledger or another contract. In addition to transactions for transferring assets and for initiating smart contract executions, a ledger that supports smart contracts can further store program data, referred to as contract state, for future executions of the contract. Critically, developers could also architect smart contracts into the system to enforce governance or regulatory requirements.

CBDCs will most likely require mechanisms to hide personal and/or financial information recorded on the DLT from unauthorized parties. This includes both the amounts of transactions as well the identities of the sender and the receiver. We assume that the transaction information is encrypted such that it can still be audited for validity and compliance by auditors while still preserving the privacy of the transaction. While significant progress has been made, it is still an open area that requires further research and development to improve efficiency, accuracy, and security. A summary of such efforts can be found in [5]. It is important to stress that most jurisdictions do not allow for anonymity in electronic payments to the same degree as in the cash world, which is likely to remain the case regardless of whether a CBDC involves an intermediary-based model or not. We appreciate the challenges navigating the privacy concerns of a digital currency but designing around a level of anonymity also poses potential challenges such as the risk of invoking Gresham's Law that "bad money drives out good money."



Scalability and interoperability challenges inherent to DLT do not go away for CBDCs using blockchain technology

2.2 Two-tier CBDC model

To enable compliance, security, and availability of CBDC payments, central banks would naturally need to closely monitor the entire CBDC ecosystem from the issuance and the distribution of the digital token to the payments made with the token. Among other actions, central banks will have to require careful implementation of a sophisticated technology infrastructure, which would likely be delegated by the central banks to a federation of highly vetted technology firms. This federation would include technology providers working with the central bank to build the CBDC and financial institutions providing AML/CFT and other compliance functions. In this CBDC ecosystem, such a delegation of trust can be helped by using the principles of public-key cryptography. Namely, the money in transit can carry a digital signature that can only be generated directly by the central bank or indirectly by one of the central bank's certified delegates. Any recipient of the money can then simply authenticate it by verifying the signature against the public key of the central bank and/or the certificate of its trusted delegate.

We anticipate most central banks would adopt a two-tier infrastructure delivered through certified delegation which allows the central bank to outsource the complexity of managing digital certificates

for CBDC tokens to a set of potentially regulated, permissioned entities that derive their authority from the central bank, through digital certificates originated from the central bank at the root [6]. This model decouples the certificate infrastructure (Tier 1) from the critical latency path of CBDC payments (Tier 2), allowing wallet providers such as banks and other financial institutions to securely process

CBDC payments at a high scale without imposing extra overhead on the highly protected PKI nodes.



Most central banks will adopt a two-tier CBDC with a payment layer and an infrastructure layer

This certificate infrastructure (i.e., Tier 1) closely resembles the hierarchy of certificate authorities (CAs) in a *Public-Key Infrastructure (PKI)* that plays a vital role in enabling the secure transfer of information over the Internet. A PKI model for CBDC can significantly facilitate the secure issuance and transfer of CBDC funds with the central bank serving as the root CA and supervised financial institutions (FIs) serving as intermediate CAs under regulatory oversight. These intermediate CAs could play two roles: (1) vetting wallet providers based on regulatory compliance; (2) issuing digital certificates to vetted wallet providers to facilitate CBDC payments securely [6].

2.3 Cross-border CBDC payments

In the context of CBDCs, cross-border payments would require sending payments across CBDC networks. For example, consider a user with funds recorded on a CBDC ledger who wants to send a payment to another user on another CBDC ledger. We assume that the two CBDC ledgers are maintained by separate networks, use different ledger protocols, and reside in different jurisdictions. We further assume that both ledgers are implemented as DLTs, i.e., each ledger is replicated across multiple geographically distributed nodes for resiliency. We finally assume both DLTs support basic, generic smart contract execution that supports digital signature verification (e.g., ECDSA verification)¹ and hash functions (e.g., SHA-3)².

Benefits of DLT for crossborder payments. A central bank could tailor a DLT to accommodate various types of data and could enhance efficiency, streamline cumbersome or fragmented business processes, and develop trust between counterparties based on the integrity of the technology [10]. Furthermore, most enterprises can deploy DLT irrespective of the underlying hardware empowering the system and of the software environment running the ledger protocol. We refer to this characteristic as *vendor*

independence. More importantly, while DLTs could differ significantly from each other on their high-level designs, they typically rely on standard cryptographic primitives (e.g., digital signatures, hash functions, etc.), and commodity hardware on other DLTs can automatically parse and process the DLT's internal messages. *With respect to cross-border payments, vendor independence and reliance on standard cryptographic primitives in DLTs are*

two unique features missing in traditional ledgers that lead to inefficient cross-border arrangements due to relying heavily on manual validity and compliance checks. In addition, DLTs that support smart contracts can bring even more interoperability opportunities through their programmability capabilities as they allow automatic verification of more complex validity and compliance requirements.

On-ledger vs. off-ledger payments. Depending on the scalability requirements of cross-border payments, a cross-ledger protocol may authorize payments in two ways: *on-ledger* or *off-ledger*. An on-ledger payment entails writing the transaction directly on the ledger at the time of payment, while an off-ledger payment relies on a collateralized payment channel to authorize payments securely without writing on the DLT at the time of payment. In practice, an on-ledger payment could take significantly longer to confirm due to the latency of consensus protocols and the potentially massive load on CBDC networks. In contrast, off-ledger payments are confirmed instantly and can scale to a virtually unbounded load. In the next section, we propose cross-border CBDC payment routes referred to as *Universal Payment Channels (UPC)* that allow amortization of the ledger overhead by making one-time deposits into a smart contract and then paying recipients several times without writing on the ledger for each payment. We will discuss UPC in more detail in Section 3.



CBDCs that support smart contracts are better-positioned to enable programmable money

¹ An elliptic curve digital signature algorithm is a digital signature algorithm (DSA) that is an analog of DSA using elliptic curve mathematics [21].

² SHA-3 is a cryptographic hash algorithm that is designed to provide a random mapping from a string of binary data to a fixed-size "message digest" and achieve certain security properties. Hash algorithms can be used for digital signatures, message authentication codes, key derivation functions, pseudo random functions, and many other security applications [22].

3. Cross-border payments using universal payment channels

Figure 1 shows the cross-border CBDC infrastructure using UPC in the context of the two-tier CBDC model described in Section 2.2. As shown in the figure, each CBDC system allows the central bank to delegate the task of key provisioning to one or more intermediate certificate authorities (CAs) who provision keys on behalf of the central bank as *wallet providers*. A wallet provider is an entity that can access the CBDC's DLT and provide wallet services, and optionally, custody services to end users. Here, we purposefully skip how a DLT is setup and CBDCs are minted on the DLT in order to focus on the XBP process.

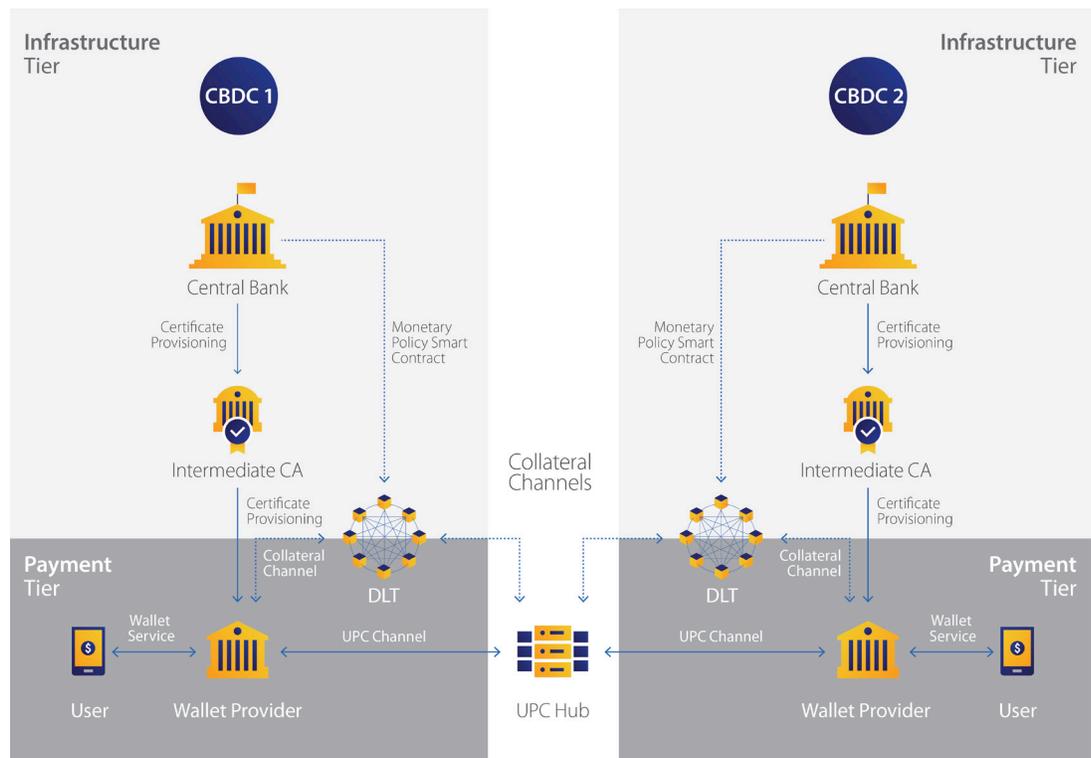


Figure 1: The Two-Tier CBDC Model and Cross-Border CBDC Payments Using UPC

We frame UPC in the context of a common cross-border payments scenario such as the sending of international remittances, where both the sender and the receiver rely on their respective banks (in this case, wallet providers) to send and receive funds on their behalf. In addition, the sender may self-custody their funds by storing secret keys locally and authorizing their wallet provider via a digital signature to initiate a cross-border payment. The wallet provider then submits the transaction to the UPC protocol. Depending on the frequency of XBP requests submitted to the wallet provider and the XBP service provided to the users, the wallet provider may submit a wholesale XBP through the UPC hub to tradeoff between the latency and the cost of XBPs.

The UPC hub. The UPC protocol facilitates payments through an Internet web service called the UPC hub that acts as a gateway [7] to receive XBPs from wallet providers and route them to destination wallet providers. While the UPC hub is trusted to be always available and process payment requests, its operation within each CBDC system is fully transparent by design to any entity (e.g., the central bank and wallet providers) that can read the state of the CBDC's DLT. Meanwhile, our protocol requires the UPC hub to

authorize every payment that happens between the wallet providers off the ledger.

This allows the UPC hub to check the validity and the regulatory compliance of every XBP as it crosses jurisdictions. Such checks could be automatically performed by the hub, for example, using AML models on transaction graphs trained according to the local regulations of each jurisdiction and blocking non-compliant transactions. Nevertheless, progress on the CPMI's roadmap building blocks – which expressly aim to streamline regulation and remove frictions – would be welcome

and could be incorporated into this technical model. The hub may charge each XBP a small fee for the services it renders. We finally note that the hub's access to the DLT to open and close a channel could be made hidden from the public while still visible to the three parties involved. Moreover, the parties' access to the DLT does not imply that they can read other financial information recorded on the DLT. The motivation behind the UPC hub recognizes that each central bank will have different motivations for moving forward with a CBDC, and those motivations will inevitably manifest in different designs.

UPC registration. Before a wallet provider can send or receive XBPs to/from the UPC hub, it needs to register its identity (i.e., the public key obtained from the intermediate CA) with the UPC hub and open a *collateral channel* on the corresponding DLT jointly with the hub, as shown in Figure 1. Through the collateral channel, both parties deposit an agreed-upon amount of CBDCs, that they own on the DLT, into a smart contract (referred to as the *UPC contract*). The UPC contract is deployed on the DLT by the hub during the registration of the wallet provider.

The UPC contract consists of a common set of instructions to open, close (aka, settle), and dispute UPC transactions, and must be written in the specific smart contract language supported by the DLT. This is a one-time task that is done by the UPC hub admin when onboarding a new type of DLT/CBDC. The smart contract guarantees the interest of all parties if they act honestly. Otherwise, a dispute initiated by one of the parties could result in forfeiture of some or all of the collateral deposited by the party. The validity of the UPC contract execution and the security of the collaterals held by the contract are all guaranteed by the security of the underlying DLT.



The DLT UPC Hub maintains confidentiality between the two parties of a transaction

UPC authorization & payment. Once both wallet providers register and open collateral channels with the UPC hub, they are ready to send/receive XBPs via only off-ledger communication with the hub. Every transaction consists of two steps: authorization and payment. In the former step, the receiver issues a payment proposal (akin to a bill of sale) and sends it to both the hub and the sender who show their agreement to the proposal by signing it and sending it to the other two parties.

As part of the proposal, the recipient includes a hash of a secret that it generates uniquely at random for this transaction. The hash serves as a commitment by the recipient pledging that it will eventually (by a time set in the payment proposal, referred to as expiry) reveal the secret upon receiving a valid promise from the sender. Otherwise, the promise does not incur any liability for the sender (i.e., no money will be deducted from the sender's initial deposit in the settlement phase). After receiving the payment proposal, the sender creates a promise and sends it to the hub which verifies the promise and creates a corresponding promise for the receiver. Similarly, the receiver verifies the hub's promise and proceeds to the Pay step.

The receiver begins the latter payment step by sending the secret to the hub which verifies the secret and acknowledges it by sending back a receipt that includes the updated credit value (increased by the amount in the promise) of the receiver. Next, the hub forwards the secret to the sender who verifies and acknowledges the receipt similarly.

UPC settlement. All parties always maintain the latest signatures that they received off-ledger from the other parties during the Authorization & Payment phase, so that they can go to the UPC contract on the DLT and resolve disputes on the UPC channel if they suspect deviation from the protocol. Using the signatures submitted by the disputing party, the UPC contract can automatically calculate the final balance of each party and settle the channel. This closes the UPC channel, and the two parties must open a new channel if they wish to transact again. Note that the maximum amount of funds each party can spend in a unidirectional UPC channel is equal to the amount of collateral each party deposits during the registration phase. If the UPC channel is used as a bidirectional payment medium, then the amount of funds each party owes at any time is always less than or equal to their collateral deposit.



Even for DLT transactions, the UPC Hub performs a critical settlement and dispute resolution function

3.1 Minimum ledger requirements for UPC

Many central banks remain undecided whether their CBDC will be based on a DLT architecture or building a non-DLT, centrally controlled infrastructure. These design choices do not necessarily exclude the adoption of the UPC protocol. In fact, to be supported by the UPC protocol, a ledger protocol only has to provide, at minimum, basic smart contract execution capabilities to support what is usually known as *Hash Time Locked Contracts (HTLCs)* [12]. Indeed, the Monetary Authority of Singapore and the Bank of Canada used a HTLC to link their respective experimental wholesale CBDC projects. Fortunately, such contracts can be provided by both DLT and non-DLT ledgers. Therefore, UPC can support any type of ledger protocol if they support HTLCs [17].

To be interoperable with other ledgers, a ledger protocol may provide, at minimum, basic smart contract execution capabilities to support HTLCs. Fortunately, such contracts can be provided by both blockchain and non-blockchain-based ledgers. An HTLC provides the following functionalities:

1. Locking collateral funds on both ledgers to create a UPC channel, and;
2. Releasing the collateral funds as part of a final settlement of the channel, which could be initiated either automatically at the channel's expiry time or manually by any of the participants (e.g., in case of a dispute or manual channel termination).

More specifically, UPC requires two primitives of HTLCs: *timelocks* and *hashlocks*. A timelock is a primitive that allows a smart contract to restrict spending of some funds until a specified time in the future while a hashlock is a primitive that restricts spending of funds until a secret is revealed to the contract. Given a cryptographic hash function H , the secret is usually represented in the form of a hash preimage x , where $H(x)$ is provided to the contract as a commitment to x .

The commitment allows the contract to ensure that the secret revealed by the committer later (e.g., settlement time) is mathematically bound to some promise the committer made to another party at an earlier time (e.g., transaction time). This is the core property of HTLCs that can be used to reduce counterparty risk in two-party transactions. The UPC protocol takes this one step further and uses timelocks and hashlocks in a special way to minimize counterparty risks in a three-party model (payer-hub-payee), under a hub-and-spoke design. The immediate benefit of such protocol is that it imposes minimal liability on the hub making it possible to scale UPC hub to support millions or even billions of users and/or transactions while reducing fees and complexities of cross-border payments.

When used to route transactions between two different ledgers, the UPC protocol requires both ledgers to support the same hash function. This requirement is in place so that the corresponding smart contracts on the two ledgers can lock funds with the same hash value on both ledgers and unlock them with the secret tokens associated with the hash value. On the other hand, UPC does not demand the ledgers support the same digital signature scheme while any client-hub pair are required to agree on the same signature scheme so that they can authenticate each other's messages.

4. How to think about the way ahead

The design choices that central banks make on CBDC should be based upon the unique policy and regulatory objectives of that central bank. As previously discussed, the use of CBDC for cross-border payments will encounter preexisting financial regulations spread across the globe, but the CBDC design choices of central banks should not act as a barrier or complicate cross-



A UPC hub can provide assurance for financial institutions that will facilitate cross-border CBDC payments

border payments. As central banks build a CBDC they will likely encounter a variety of challenges, not least of which is how to ensure that this new technology is enhancing, and not undermining, compliance regimes among countries. Encouragingly, the BIS has continued its analysis of this challenge when it detailed the attributes of a multiple CBDC

(mCBDC) arrangement that seeks to coordinate, “design frameworks including technological, market structure and legal aspects, aiming to facilitate cross-border interoperability of multiple CBDCs from different jurisdictions [16].” In this spirit of analyzing future CBDC frameworks for cross border payments, a UPC model could help ensure a more technically sound and resilient model for cross-border CBDC payments.

The ability to implement the complex logic of smart contracts into an existing payments architecture at scale is an issue that needs careful testing and analysis. In an August 2020 analysis by the US Federal Reserve, programmability would be possible for a token, account, or hybrid based CBDC, with varying degrees of functionality [18]. Currently, many payment systems do not have the ability to create programmable payments [19]. These innovations are still relatively new, and central banks should thoroughly explore the implications and potential use cases for businesses, users and merchants, so that while new innovation can be allowed to develop, continuation and integration with the existing systems can also be ensured.

By authorizing transactions between wallet providers, a UPC hub could perform as a type of universal correspondent bank. This is helped by the fact that UPC registration requires a strict identity management verification process. This process can also help financial institutions manage the identification challenges that come from managing hundreds of corresponding banking relationships. In effect, UPC has the potential to provide a level of assurance for financial institutions that could facilitate CBDC XBPs. As discussed earlier, this innovation has the potential to mitigate some of the frictions identified in the FSB report [2] while preserving the essential controls inherent in facilitating safe and secure financial intermediation.

Finally, another area of analysis is the need for common standards. International standards form the backbone of the payments industry, enabling ubiquity by maximizing global interoperability and acceptance across all payment systems, creating a common approach at the physical and technical level, yet providing enough flexibility in implementation that preserves vigorous competition and the ability for differentiation across the various payment systems. This paper hopes to contribute to the current standards debate and discussion on CBDC, and cross-border payments generally.



References

- [1] *Ready, steady, go? – Results of the third BIS survey on central bank digital currency. (January 2021).* <https://www.bis.org/publ/bppdf/bispap114.pdf>
- [2] *Enhancing Cross-border Payments, Stage 1 report to the G20: Technical background report (April 2020). The Financial Stability Board.* <https://www.fsb.org/wp-content/uploads/P090420-2.pdf>
- [3] *Enhancing Cross-border Payments, Stage 2 report to the G20. Committee on Payments and Market Infrastructures (July 2020). Bank for International Settlements.* <https://www.bis.org/cpmi/publ/d193.pdf>
- [4] *Cross-Border Retail Payments. Committee on Payments and Market Infrastructures (February 2018). Bank for International Settlements.* <https://www.bis.org/cpmi/publ/d173.pdf>
- [5] Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan Ford, James Grimmelmann, Ari Juels, Kari Kostianen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, and Fan Zhang. *Design choices for central bank digital currency – policy and technical considerations (July 2020). The Brookings Institution.* https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf
- [6] Mihai Christodorescu, Wanyun Catherine Gu, Ranjit Kumaresan, Mohsen Minaei, Mustafa Ozdayi, Benjamin Price, Srinivasan Raghuraman, Muhammad Saad, Cuy Sheffield, Minghua Xu, and Mahdi Zamani. *Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies (December 2020). Visa Inc.* <https://arxiv.org/abs/2012.08003>
- [7] Thomas Hardjono, Martin Hargreaves, Ned Smith. *An Interoperability Architecture for Blockchain Gateways (October 2020). Internet Engineering Task Force.* <https://datatracker.ietf.org/doc/draft-hardjono-blockchain-interop-arch/>
- [8] Martin Hargreaves, Thomas Hardjono. *Open Digital Asset Protocol (November 2020). Internet Engineering Task Force.* <https://datatracker.ietf.org/doc/draft-hargreaves-odap/>
- [9] *The rise of digital remittances: How innovation is improving global money movement (March 2021). Visa Economic Empowerment Institute.* <https://usa.visa.com/content/dam/VCOM/global/ms/documents/veei-the-rise-of-digital-remittances.pdf>
- [10] Erin English, Amy Davine Kim, Michael Nonaka, *Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry (March 2018). Microsoft Corporation.* <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1TH5G>

- [11] Raphael Auer, Rainer Böhme, *The technology of retail central bank digital currency. Quarterly Review (March 2020). Bank for International Settlements.* https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf
- [12] *Hash Time Locked Contracts - Bitcoin Wiki (accessed Feb. 18, 2021). Bitcoin.it.* https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts
- [13] *Correspondent Banking Services FATF Guidance (October 2016). Financial Action Task Force.* <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf>
- [14] Erbenová, M., Liu, Y., Kyriakos-Saad, N., López-Mejía, A., Gasha, G., Mathias, E., Norat, M., Fernando, F. and Almeida, Y. *The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action (June 2016). International Monetary Fund.* <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf>
- [15] *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System -- IMF Occasional Paper No. 222 (March 2021) International Monetary Fund.* <https://www.imf.org/external/pubs/nft/op/222/>
- [16] *Central bank digital currencies for cross-border payments (July 2021). The Bank of International Settlements.* <https://www.bis.org/publ/othp38.pdf>
- [17] *Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies (2019). Monetary Authority of Singapore, the Bank of Canada, Accenture.* <https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf>
- [18] Alexander Lee. *What is programmable money (June 2021)? Board of Governors of the Federal Reserve System.* <https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.htm>
- [19] Paul Wong and Jesse Leigh Maniff. *Comparing Means of Payment: What Role for a Central Bank Digital Currency (August 2020)? Board of Governors of the Federal Reserve System.* <https://www.federalreserve.gov/econres/notes/feds-notes/comparing-means-of-payment-what-role-for-a-central-bank-digital-currency-20200813.htm>
- [20] *NIST SPECIAL PUBLICATION 1800-16. Securing Web Transactions TLS Server Certificate Management (June 2020). National Institute of Standards and Technology.* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf>
- [21] *NIST Information Technology Laboratory. Computer Security Resource Center. (accessed September 2021). National Institute of Standards and Technology.* <https://csrc.nist.gov/projects/hash-functions/sha-3-project>

Disclaimer

Case studies, comparisons, statistics, research and recommendations are provided “AS IS” and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required. All trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

About Visa Inc.

Visa Inc. (NYSE:V) is the world's leader in digital payments. Our mission is to connect the world through the most innovative, reliable, and secure payment network—enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second. The company's relentless focus on innovation is a catalyst for the rapid growth of digital commerce on any device for everyone, everywhere. As the world moves from analog to digital, Visa is applying our brand, products, people, network, and scale to reshape the future of commerce.

For more information, visit About Visa, visa.com/blog and @VisaNews.



Visa Economic Empowerment Institute

