INTERNATIONAL MONETARY FUND

A Multi-Currency Exchange and Contracting Platform

Prepared by Tobias Adrian, Federico Grinberg, Tommaso Mancini-Griffoli, Robert M. Townsend, and Nicolas Zhang

WP/22/217

2022
NOV

WORKING PAPER

 WP/22/217

IMF Working Paper
Monetary and Capital Markets Department

A Multi-Currency Exchange and Contracting Platform

Prepared by Tobias Adrian, Federico Grinberg, Tommaso Mancini-Griffoli, Robert M. Townsend, and Nicolas Zhang

Authorized for distribution by Tobias Adrian
November 2022

ABSTRACT: Cross-border payments can be slow, expensive, and risky. They are intermediated by counterparties in different jurisdictions which rely on costly trusted relationships to offset the lack of a common settlement asset as well as common rules and governance. In this paper, we present a vision for a multilateral platform that could improve cross-border payments, as well as related foreign exchange transactions, risk sharing, and more generally, financial contracting. The approach is to leverage technological innovations for public policy objectives. A common ledger, smart contracts, and encryption offer significant gains to market efficiency, completeness, and access, as well as to transparency, transaction and compliance costs, and safety. This paper is a first step aiming to stimulate further work in this space.

JEL Classification Numbers:	E5; E41; G15; F30
Keywords:	Cross-border payments, multilateral platforms, digital money, CBDC, programmability, encryption
Authors' email addresses:	tadrian@IMF.org fgrinberg@IMF.org tmancinigriffoli@IMF.org rmtownsen@mit.edu nxyzhang@mit.edu

WORKING PAPERS

A Multi-Currency Exchange and Contracting Platform

Prepared by Tobias Adrian, Federico Grinberg, Tommaso Mancini-Griffoli, Robert M. Townsend, and Nicolas Zhang [1]

[1] The authors would like to thank Majid Bazarbash, Pamela Cardozo, Martin Cihak, Max-Sebastian Dovi, Kelly Eckhold, Dong He, Annamaria Kokenye, Kieran Murphy, Julia Otten, Adina Popescu, Asad Qureshi, Herve Tourpe, as well as seminar participants at the Bank of England, BIS, ECB, MIT, University of Minnesota, and Stanford University for discussions and for their comments and suggestions. Remaining errors are ours. The views presented here do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Contents

BOXES

FIGURES

TABLES

1. Introduction

Cross-border payments are oftentimes slow, expensive, and risky as they are exposed to fundamental obstacles to trade. Domestically, there are infrastructures and governance structures that allow the private sector to better provide payment and financial services. At the international level, however, lack of coordination creates insufficient provision of these public goods and results in inefficient arrangements for cross-border transactions. These issues are compounded by disruption in cross-border payments emerging with new technologies that may allow for transactions that circumvent borders and regulations and by fears of fragmentation that have risen given ongoing geopolitical conflicts.

The need for better cross-border payments has been long recognized by the international community. In October 2020, G20 Finance Ministers and Central Bank Governors endorsed a Roadmap for Enhancing Cross-Border Payments. This comprises 19 Building Blocks that aim to achieve faster, cheaper, more transparent, and more inclusive cross-border payment services. These should be safe and secure, and can facilitate economic growth, international trade, global development, and financial inclusion.

The objectives of this paper are twofold: to encourage further discussion on how multilateral platforms could enhance cross-border payments, and to eventually stimulate the provision of key international public goods and infrastructures.[2]

With these objectives in mind, we present in this paper a specific vision for a multilateral exchange and contracting platform (X-C platform). The design of the platform improves cross-border transactions in two dimensions. First, it has a design that centralizes payments and settlement and integrates functionality needed for cross-border transactions, namely, to streamline compliance, to reduce cost of foreign exchange (FX) conversion, and to better manage financial risks. Second, it leverages new technologies to better organize payments and associated financial markets. These new technologies are common ledgers with unique states, programmability that allows for automated financial contracts (“smart contracts”), and encryption which ensures privacy, can alleviate the underlying obstacles to trade. These tools allow the design of a multilateral exchange and contracting system where participants can truthfully share information with smart contracts but retain privacy relative to other parties.[3]

Exchange systems must deal with fundamental problems which create the need for contractual arrangements to deal with risks, credit, and insurance. At the level of individual agents, payment flows are asynchronous: inflows and outflows over intervals of time rarely match and flows may not balance. Thus, agents accumulate liquidity buffers, borrow to ensure they have enough liquidity to meet their obligations, or enter insurance

[2] This paper builds upon Building Block 17 on “New multilateral platforms and arrangements in cross-border payments” (see CPMI, IMF, and WB 2022) and Building Block 19 on “Options for access to and interoperability of CBDCs for cross-border payments” (see CPMI, BISIH, IMF and WB 2022).

[3] In this paper, we refer to “contracts” from different (and related) perspectives. From the point of view of economics, a “contract” refers to arrangements among economic agents, generally in the presence of information asymmetry. From a legal point of view, a “contract” refers to an institutional arrangement for the way in which resources flow, which defines the various relationships between the parties to a transaction or limits the rights and obligations of the parties. From a computer science perspective, a “smart contract” is a computer program or a transaction protocol that is intended to automatically execute, control or document legally-relevant events and actions according to the terms of a contract or an agreement.

schemes to withstand net outflows. Agents that wish to share their financial position to facilitate these contracts may find that their messages may not be trusted[4] or that doing so may put them at disadvantage by revealing private information.

Trade and settlement are typically separated in time creating limited commitment. As underlying circumstances may change, this gives parties in a contract the opportunity to renege on pre-entered trades. This, in turn, creates costs as counterparties need to take actions against this risk through escrow, collateral, or through monitoring and audits. Bilateral reneging can create contagion, and, without a common reconciled ledger, it is difficult to monitor how systemic these risks may be.

These problems in payments and financial markets exist within jurisdictions but have been alleviated by public goods. Examples include payments and financial market infrastructures, and central bank money. Regulation delineates rules and responsibilities to create trust in financial intermediaries so these intermediaries can play a key role in absorbing the counterparty risk and offer resolution.[5] This includes frameworks for due diligence on their clients and complying with customer standards. Payment system infrastructures (like RTGS) allow aggregating and clearing of requests for payments. The central bank offers a common settlement asset (central bank reserves) that allows participating institutions to extinguish their obligations with finality. Further, central banks can backstop liquidity shortfalls with policy actions. Financial markets support the payments infrastructure by allowing futures and derivative contracts to manage risks. These are regulated and have their respective infrastructures for contracts, execution, and settlement.[6,7]

This landscape is continuously updated by private and public sector innovation. Fast (retail) payment systems are emerging from private bank clearing associations, and from central banks. Fintechs serving households and small businesses start from digital payment functions but build credit and insurance products on top, with synergies in the data and financial products.[8] At the wholesale level, large intermediaries like JP Morgan have been developing blockchain-based solutions for instantaneous digital transfers of Treasury and collateral (US money market funds).

The responsibility for tracking transfers and changes in ownership in this landscape rests on multiple brokers and intermediaries that modify their clients' accounts to reflect those transactions. As infrastructures and legacy systems were created to facilitate intermediation, the information from transactions is recorded in several ledgers, for each intermediary and each of the clients that enter a transaction. These ledgers do not guarantee a unique common underlying state. Limited communication makes reconciliation time consuming and costly.

For cross-border payments, many of these infrastructures are insufficient or do not exist. Establishing "trust" and coping with market failures is more difficult and expensive when transactions must be carried out across

[4] Agents lack the ability to share the information. In the language of contract theory, agents suffer from "limited communication".

[5] As a result, these institutions have market power over their clients, as they typically cannot share the state of their balance sheets without them. Initiatives as Open Banking and Open Finance aim to mitigate this.

[6] ISDA's framework provides guidance on how to regulate derivative contracts. https://www.isda.org/

[7] These public goods solutions are sometimes a result of direct public sector intervention, a true public good. Public good solutions can also arise indirectly as a result of having common enforced rules, laws, and regulations, following an industry standard.

[8] Alipay (China), Mercado Pago (Latinamerica), and GoPay (Indonesia) have become large players in payments and offer different financial services. See IMF GFSR April 2022.

borders. At the international level, the lack of common governance across borders makes these public goods scarce or non-existent and leads to high risks, high costs, and high concentration.

First, internationally there is no common and widely available settlement asset. Domestically, the combination of regulation and supervision, access to a safe settlement asset, and potential central bank backstops make financial institutions' liabilities highly liquid and, in most circumstances, acceptable for settlement. In contrast, the lack of common settlement assets in cross-border payments results in networks of bilateral claims or closed-loop solutions with intra-firm claims. Internationally, banks must rely on foreign banks to access foreign central bank money through nostro/vostro accounts or must set up branches and be regulated in the countries for which they want to have access to central bank reserves.

Second, across borders there are different currencies and thus agents need to make foreign exchange (FX) transactions. While in most domestic transactions there is a single currency involved, cross-border transactions usually require that an agent in the payment chain make the conversion across currencies. In many cases, this implies risks and high costs. These costs have been documented as one of the main drivers of cross-border transaction costs.[9]

The importance of FX costs is especially true for countries that have "illiquid" FX markets where spreads charged by intermediaries are typically high. These intermediaries need to hold inventory of multiple currencies which exposes them to FX risk. The more illiquid the market is, the more expensive it is to manage this risk. Contracts and markets for forward swaps and FX derivatives may be nonexistent. High costs and economies of scale in self-insurance reinforces large players' market power in cross-border payments. Only large financial institutions can in-house FX conversion, internally buffering risks thanks to the scale given by their large balance sheets. In sum, lack of market depth in FX derivative markets can hamper spot market liquidity and increase cross-border transaction costs (Mehrling 2013).

Third, compliance with rules for cross-border transactions is expensive. These include preserving financial integrity (know-your-customer or KYC and anti-money laundering and countering the financing of terrorism or AML/CFT) and complying with existing capital flow management measures (CFMs). At the domestic level, financial institutions incur costs associated with KYC and AML/CFT and want to preserve the data they gather by creating client relationships that generate market power. At the international level, this friction is compounded. There is a lack of common governance for these vetting procedures and monitoring: not only is it expensive to gather these data on customers, but it can also be risky to trust financial institutions from other jurisdictions as there can be uncertainty on the soundness of their procedures. Compliance with CFMs slows down transaction processing and makes solutions that build on existing legacy systems harder to implement.

Specialization in overcoming these three frictions gives rise to networks of bilateral correspondent banking relationships, international banking, and closed loop solutions in cross-border payments (e.g., Wise, MoneyGram)[10] which have high fixed costs and economies of scale. This results in concentrated market structures and large intermediaries that play a central role in cross-border payments.

[9] For emerging market and developing economies (EMDEs) especially, FX margins play a large role in cross-border payments overall fees (Feyen et al 2021).
[10] CPMI-IMF-WB (2022).

There have been many public and private sector innovations and initiatives to improve cross-border payments. Standardizing messaging allowed correspondent banking to be faster and safer.[11] Netting and settlement has been improved for some currencies.[12] Regional payment platforms have been developed[13] and experimentation in interlinking domestic payments systems is also ongoing.[14] Payment providers have also been developing new services.[15] Solutions that leverage stablecoins for fast and inexpensive cross-border payments have also grown recently.[16]

There are related ongoing projects and experimentation that also aim to develop solutions for cross-border payments using Distributed Ledger Technologies (DLT). Some of these projects are public and led by a consortium of Central Banks[17] and some are done in collaboration with BIS Innovation Hubs.[18] The private sector also has been active and launched initiatives to make cross-border payments more efficient.[19] What projects share is that they use a DLT with tokens representing different national monies and focus on how to move value from one country to another.[20] Banque de France-MAS (2021) explicitly presents a solution to FX markets using automated market making (AMM).[21,22]

We build on these initiatives and go further. Our proposal for the X-C platform has a centralized multi-currency FX trading environment on the platform. We also allow for the introduction of contracts and policies to manage FX risks.

Our focus with X-C naturally goes beyond purely payments as we include other functions that are needed for competitive and efficient cross-border payments outcomes. Technological improvements in the design of intermediation systems can allow economies to be better connected. The idea is to create markets that are currently missing, establish infrastructures to fill in gaps in financial access, and reduce inefficiencies in cross-border payments. To do so, we are explicit about economic frictions, and we lay out the technological requirements for the solutions we propose. This gives blueprints for the design of the platform, its infrastructures, and its functions.

---

[11] Swift was an innovation that created a common standard for messaging payment requests, relative to the fragmented systems that preceded it. Swift has more recently introduced a basic tracker to let clients know where their request for payment lies in the chain of domestic and international correspondent banks.

[12] CLS is a centralized system for netting and reducing of FX settlement risk operating in only 18 currencies.

[13] Most innovations for cross-border payment have focused on payments narrowly. There are cross-border regional systems as for example with PAPPS and TCIB in Africa and P27 in the Nordics. See CPMI-IMF-WB (2022).

[14] See, for instance, Buna, TIPS, and JoMo. Nexus aims to interlink fast payments across borders.

[15] Visa and Mastercard are global retail cards, and Visa B2B Connect and Mastercard Track Business Payment Services offer business services, with Visa Direct for remittances.

[16] For example, Stellar and Ripple.

[17] Bank of Thailand and HKMA's have been developing the Inthanon-LionRock project. This allows the conversion of depository receipts into wholesale CBDC and uses DLT solutions with smart contracts for multi asset liquidity management. The programming of other contracts is not yet featured, though Ithanon did a pilot of bond lifecycle management and DvP for interbank repo trading.

[18] With m-Bridge under the auspices of the BIS, and with the addition of China and Saudi Arabia, this now includes four countries.

[19] For example, JP Morgan, DBS and Temasek with Partior, Santander with Ripple, and Citibank with M10.

[20] The Regulated Liability Network (RLN) is an industry-driven project that features the tokenization and exchange of private sector regulated liabilities, that is, a broader class of assets beyond tokenized central bank reserves. See https://regulatedliabilitynetwork.org/

[21] See BdF-MAS (2021).

[22] See Neilson (2022) for a discussion.

A first key aspect of the design is that organizing cross-border transactions in a multilateral platform like X-C could improve efficiency by reducing transaction chains, settlement risk, and costs of FX transactions.[23] This aspect of the design hinges on (i) an architecture that would provide key public goods: a common infrastructure with rules and governance that would shorten transaction chains and would give legal certainty to participating agents; (ii) having common settlement assets to reduce settlement risk; and (iii) a trading environment to trade these different settlement assets in the platform.

A second key aspect of the design is combining the separate features of new technologies that X-C would require to address market failures and inadequate contracts. These features of new technologies are: (1) one common ledger (2) programmability, and (3) cryptography.[24] We use the common ledger to build markets and keep track of ownership of transactions offered by participants. The ledger is built to be able to interact with computer code. Smart contracts can read, execute, and modify entries in the ledger and automatize financial contracts. Cryptography allows smart contracts to be executed without revealing information to relevant parties.[25] Each of these three features is used to address different fundamental obstacles to trade that limit contracts. Limited commitment caused by potential reneging of contracts can be addressed with cryptographic commitments as atomic swaps and automatic transfers. Untrusted messages, where agents are suspicious whether the other party complies with rules, can be tackled with domestic certification combined with cryptography to preserve data sovereignty and privacy. Unobserved states that generate financial risks can be taken care of by aggregating information from privacy-preserving messages. Unobserved actions like front-running can be tackled with contracts executed by programmed rules.

We anchor the design on contract theory and market design: how agents should interact to best overcome market failures, what should they trade, and how markets should be organized for best results. Falling short of this engenders limited participation. In the current cross-border payments landscape, large institutions act as dealers and need to cover the cost of holding currency inventories. There are further markups to cover FX and counterparty risk. The market power from concentration also results in even higher markups. Our design aims to increase competition, lower spreads, and reduce risks by providing infrastructure, contracts, and markets for just-in-time liquidity transfers for previous contract commitments, a centralized multi-currency market, and instruments and markets for better hedging of risks.

The paper is structured to start with the barebones design of X-C and then add features that can improve cross-border transactions. In Section 2, we present the architecture of the platform, and we explain the key technological requirements that it should meet. In Section 3, we discuss how the technology can complement governance arrangements and allow for more efficient compliance with customers due diligence and capital management measures. In Section 4, we show how to organize spot and derivative FX markets to improve

[23] In highly related work, CPMI-IMF-WB (2022) discusses the benefits, costs, and potential challenges of setting up multilateral payment platforms.

[24] These technologies are used in Distributed Ledger Technologies (DLT), but we choose to highlight them separately as they can also be implemented in centralized databases. The focus of the paper is not on stressing the differences between these technologies but to highlight how the three features highlighted in the text above can be combined to address frictions in cross-border transactions. Still, there are important differences in terms of cyber-security, resiliency, and governance. We go back to these in section 2. A deeper discussion is very relevant and left for future work.

[25] That is, only parties with the right private keys will be able to see specific messages, smart contracts, and financial positions.

market liquidity and better manage risks. In Section 5, we argue that the same tools can be applied for Central Bank backstops and operations on the platform.

2. X-C Architecture and Design

Highlights

Architecture

- X-C is a common financial infrastructure for exchange and for entering into and executing financial contracts. Having deep currency exchange markets is key for an efficient cross-border payments platform.
- X-C provides an environment for digital monies issued by Central Banks ("Certificates of Escrow" or CEs) for programmable final settlement in participant countries' currencies. This shortens payment chains, reduces balance sheet interconnections, and makes transactions faster, cheaper, and safer than bilateral private claims.
- X-C allows for greater competition to cross-border payment intermediation by opening access to bank and non-bank financial entities. Agents from participating countries would be able to transact using all available CEs in the platform. This aims to increase competition and increase liquidity in currency pairs.
- X-C has technological features that include a single ledger where participants' accounts and contracts are recorded, the ability to program smart contracts, and to encrypt accounts, contracts, and information that flows in the platform.
- Settlement risk is eliminated by immediate guaranteed settlement at a point in time or guaranteed contracted settlement at future designated dates and states. Messaging, settlement, and committing contracts become linked. Thus, cross-border transactions using X-C are final and irrevocable.

Features

- X-C's first key technological feature is the unique state of the common ledger. This mitigates settlement risks. Once a trade contract or transfer is executed, the agreement and ownership are recorded. The common and unique state of the ledger ensures that all participants retrieve the same information from the platform and trust that what others observe is consistent with this information
- X-C's second key technological feature is its programmability. The smart contract code can be executed via a transaction request to its address. The smart contracts execute contractual arrangements without the need for a trusted third party to implement the contractual arrangement. The rules for market exchange, contracts, and mechanisms can thus encode ex ante contingent actions or states and automate execution of these actions.
- X-C's third key technological feature is the use of cryptography. Encryption is the process of encoding information to protect messages' content and authenticity providing additional guarantees on authenticity, commitments, and enforcement of contracts. It can help solve frictions that constrain financial contracts as it allows participants to share private information with the smart contracts without revealing it to other

parties. Settlement risk is eliminated by immediate guaranteed settlement at a point in time or guaranteed contracted settlement at future designated dates and states. Messaging, settlement, and committing contracts become linked. Thus, cross-border transactions using X-C are final and irrevocable.

Applications

- Smart contracts can be used to address limited commitment in exchanges. A solution to the commitment problem is a system in which trades are carried out with pre-programmed code and ensures Payment-versus-Payment (PvP) and/or Delivery-versus-Payment (DvP) without fails.
- Smart contracts can be extended to dynamic future and conditional versions. The platform's ability to check that a contract has an underlying asset allows for rehypothecation and interlinking contracts, thus saving collateral and conserving liquidity. Insurance and risk sharing agreements can be developed using smart contracts that observe outcomes and agents' messages but preserve their privacy.
- Auctions can be implemented without a trusted third party while preserving agents' bids privacy. The role of the auctioneer can be assigned to a smart contract that observes encrypted bids, ranks them, and determines the correct outcome of the auction. Settlement risk is eliminated by immediate guaranteed settlement at a point in time or guaranteed contracted settlement at future designated dates and states. Messaging, settlement, and committing contracts become linked. Thus, cross-border transactions using X-C are final and irrevocable.

Future proofing and upgradability

- The openness and upgradability of this architecture is a desirable model that X-C aims to reproduce (in a safe and compliant fashion), as "future proofing" the infrastructure and contract structure would ensure that the investment to adopt it would pay-off over a longer period of time.

2.1 General Description

This section gives an overview of the architecture for the cross-border platform we propose. It lays out the minimal requirements that allow deployment of the tools we presented in section 1. We specify the architecture of the platform in terms of participation, access, and assets that would be available. We then explain how the platform works for cross-border payments and the related financial infrastructure.

Settlement risk is an important friction in legacy cross-border payments. X-C addresses this friction by providing a form of central bank digital monies as settlement assets available to all participants. X-C also leverages new technologies and mechanism design to minimize risks of reneging on previous trade agreements. The proposed architecture for X-C is based on using digital monies issued by central banks to shorten transaction chains, allowing more direct transactions, and reducing counterparty and settlement risk. The platform provides programmable and final settlement in participant countries' currencies.[26]

[26] Participation and currencies available on the platform would depend on the scope of the platform's implementation and the agreements among participant countries. This paper is not proposing a specific group of countries that should set an agreement nor proposing a specific global implementation.

More generally, the features of X-C's design propose an improved financial infrastructure that enhances contract possibilities. This approach does not rely on networks of bilateral claims as corresponding banking does. Rather, it aims at increasing competition in cross-border payments. It allows smaller intermediaries to provide services directly in an environment where risks are better managed, as there are more opportunities for them to enter hedging and risk-sharing contracts. At the same time, X-C also addresses concerns that central banks may have in terms of non-resident unsupervised financial institutions holding their fiat money.

X-C's architecture and design have the following key specifications. First, the platform is a common financial infrastructure for exchange and for entering financial contracts, where agents from participating countries would be able to transact. Second, the platform allows for greater competition to cross-border payment intermediation by opening access to bank and non-bank financial entities. Third, the platform includes a settlement asset for each currency that can be freely transacted inside the platform but still addresses limits to fiat money that central banks may want to impose on non-resident entities. Fourth, X-C has technological features that include a single ledger where participants' accounts and contracts are recorded, the ability to program smart contracts, and to encrypt accounts, contracts, and information that flows in the platform. In the next subsections, we present X-C's design in detail.

2.2 X-C's Architecture

A multilateral platform for exchange and contracting is a financial market infrastructure set up for transactions between platform participants that maybe in different jurisdictions ("cross-border transactions").[27] As such, it must have common rules, governance, standards, and technology that reduces risks and costs of exchange. While platforms can in principle provide "front-end" services to final users, here we describe the setup of a platform focused on "back-end" services and where financial intermediaries are responsible to provide services to their clients.

X-C has a "centralized" model with multiple currencies. Participants from different jurisdictions that are part of the platform would have accounts in the multilateral platform.[28] As such, X-C does not require modifying domestic systems. In principle, all participating jurisdictions' currencies would be available on the platform. As greater participation of intermediaries helps increase competition, the design envisages access by banks and non-bank financial institutions, including payment service providers (PSPs). Still, under these common principles, each jurisdiction would decide the entities it would give access to X-C.

The platform's design includes a final settlement asset for each participating country issued by its central bank. We call these assets "Certificates of Escrow" (CE). These CEs are issued one-to-one against central bank reserves. As a result, CEs are safe and homogenous and do not carry intermediaries' risk. There are no interoperability issues, as CEs are native to the platform and are only issued and exchanged in it. This shortens chains, reduces balance sheet interconnections, and makes transactions faster, cheaper, and safer than bilateral private claims. The speed, cost, and safety features of CEs also facilitate subsequent contracts based

[27] Note that this is a more general definition than "multilateral platform for payments". See CPMI, IMF, and WB (2022).

[28] This can be contrasted with "hub-and-spoke" models, where participants have accounts in their domestic infrastructures and the hub entity connects these different infrastructures. See CPMI-IMF-WB (2022) for a detailed discussion.

on the same CEs, as is discussed in section 4. CEs can be committed under contracts and, so committed, it is escrowed until released by a specified contingency.

Settlement is done by transferring value on the platform's ledger by moving CEs between agents' accounts. When there is exchange of different CEs, agents with funds in their accounts can enter smart contracts to eliminate risks in the transaction.[29] An example of this are hash-time locked contracts, explained further below.[30]

All participants from all countries who participate in the platform would be able to hold both domestic and foreign CEs in each of their platform accounts. This is intended to allow for more competition in market making for each currency pair.[31] For multi-currency cross-border payments to be feasible, it is necessary that at least one agent must be able to "intermediate". In principle, this can be done by final users (e.g., when tourists pay in cash), by banks (that have multi-currency nostro and vostro accounts or accounts at CLS), or by Central Banks (that hold international reserves).

A distinctive feature is that CEs are always convertible at par for entities that are regulated by the central bank and are allowed to hold reserves.[32] But CEs are not convertible to reserves for non-regulated entities (typically, non-residents that have access to the platform).[33] The reason is that the use of central bank money to settle cross-border transactions is limited. Other than paper currency, central banks have not given non-regulated entities access to their balance sheets. Thus, typically central banks' reserves cannot be held by non-residents, and these cannot be used to pay or be paid across borders.[34]

The parity of each CE with domestic fiat would be pinned down by the competition among regulated entities that have access to central bank reserves and by the commitment of each central bank to always redeem CEs at par. Any difference in market value between reserves and CEs of a given fiat money would be subject to riskless arbitrage by these domestic entities. This also has foreign exchange (FX) implications. For non-residents, the expectation that they will find a counterpart that accepts domestic CEs at the same rate as the value of fiat outside the platform will underpin the equality between the value of FX currency pair and the corresponding CEs value pairs.[35] Thus, having deep markets to exchange CEs is key for an efficient platform and ensure that all can

[29] Smart contracts are self-executing software protocols that reflect the terms of an agreement among multiple parties.

[30] We chose not to use the term "token" or "tokenization" as there are different and sometimes contradictory uses of what these could mean (see AWS 2022). Here, we could use the term "token" to represent a financial instrument that is recorded on the platform. This definition is consistent with CPMI (2019). Thus, X-C's participants have accounts kept on the platform's ledger. When they hold an asset or issue a liability on the platform, these are tokenized financial instruments. In this section, we focus on how tokenized central bank liabilities can be used to transfer value across borders. In section 4, private contracts are tokenized to provide tools for risk management. In section 5, we explore how tokenizing other financial instruments can help implement central banks' policies such as liquidity windows.

[31] Section 4 goes into more details on how FX market liquidity can be enhanced with X-C's functionalities.

[32] As mentioned in the discussion above, this could potentially include non-bank financial institutions and PSPs.

[33] In principle, a central bank could relax this. It would be equivalent to having a cross-border wholesale CBDC accessible to non-residents.

[34] There are several projects that explore allowing non-residents to hold CBCDs, for example Inthanon-Lionrock and mBridge (see BIS 2021, 2022). These projects are related to X-C in its basic architecture, but their scope is typically delimited to transfer value across borders. X-C, in contrast, focuses on delivering a set of potential solutions for frictions in cross-border payments, such as shallow FX markets, lack of risk management contracts, and the implementation of central banks' backstops on the platform.

[35] The same logic can apply to domestic participants without access to central bank reserves. In principle, these could fund their X-C accounts indirectly (e.g., through a bank with access to central bank reserves), but they would also need to rely on such domestic provider to cash-out their CE out of the platform

find counterparts and to avoid concentration.[36] We discuss the challenges and potential solutions of thin FX markets in section 4.

Settlement risk is eliminated by immediate guaranteed settlement at a point in time or guaranteed contracted settlement at future designated dates and states.[37] The platform does this by providing PvP and DvP. In effect, messaging and settlement, or messaging and committed contracts, are linked, no longer separated in time. Thus, cross-border transactions using X-C are final and irrevocable.[38]

Figure 2.1 illustrates how participants' accounts are funded using reserves. In this example, in Step 1 a PSP from country A (PSP_A) funds its account with CEs from its country (CE_A) using reserves, and a commercial bank from country B ($Bank_B$) does the respective operation to fund CE_B. Both central banks reflect the respective changes in their liabilities. In step 2, PSP_A and $Bank_B$ exchange their CEs at an agreed FX rate. In principle, this transaction could be done relying on an outside fixing rate (an "oracle"), by a bilateral agreement as typical in over-the-counter (OTC) trades, or in a centralized trading environment such as dealers' market or multi-currency auctions. In section 4 we discuss this in more depth and highlight the benefits of centralized exchanges to reduce fragmentation, foster market depth, and increase competition.

Figure 2.1. CE issuance and cross-border

	Central $Bank_A$	PSP_A	$Bank_B$	Central $Bank_B$
(1)	- $Reserves_A$	- $Reserves_A$	- $Reserves_B$	- $Reserves_B$
(2)	+ CE_A	+ CE_A	+ CE_B	+ CE_B
(3)		- CE_A + $CE_B/FX_{A,B}$	+ $CE_A/FX_{A,B}$ - CE_B	

Note: This figure illustrates the issuance of CEs in country a and b against reserves. The dotted boxes denote assets and liabilities that are recorded in the platform's ledger. In country a, step 1 shows a PSP exchanging reserves for CE, and in country B a commercial bank exchanging reserves for CEs. In step 2, country a's PSP exchanges CE_A for CE_B with country b's commercial bank. In general, both intermediaries (PSP_A and $Bank_B$) can hold CE_A and CE_B. In this example, however, only PSP_A can hold $Reserve_A$ and only $Bank_B$ can hold $Reserves_B$.

Figure 2.2 shows how a resident of country A ("Alice") could make a payment to a resident of country B ("Bob") to cancel a debt she may have with him that is denominated in B's currency. In step 1, Alice sends an order to her PSP to pay Bob and thus, the bank reduces Alice's deposits by the equivalent in B's currency. For instance, this could be done using a "best execution" protocol or an FX reference rate provided by the platform.[39] In step 2, PSP_A sends CE_B for the specified amount. $Bank_B$ receives it and, in step 3 it increases Bob's deposits for that amount. In step 4, Bob confirms receiving the deposit and cancels the IOU_B. For comparison, Figure 2.3 shows how a similar transaction would be done using correspondent banking and messaging.

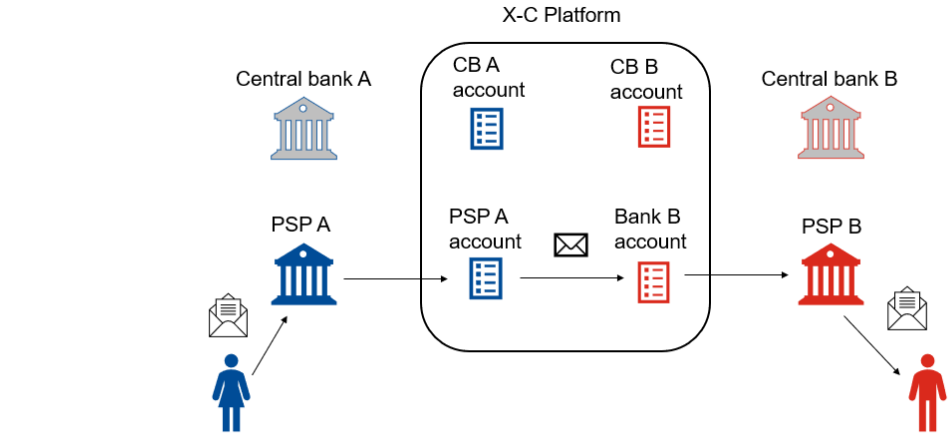
[36] Markets in which individual trades are small relative to average daily volume, and hence impact prices, are known as deep markets. When individual trades are large relative to market volume and thus can impact prices, markets are known as "thin". https://academic.oup.com/rfs/article/28/10/2946/1580141

[37] Settlement risk that emanates from the limited commitment problem, willful failure to pay or inability to pay

[38] CPSS-IOSCO (2012), Principle 8 defines final settlement "as the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the FMI or its participants in accordance with the terms of the underlying contract."

[39] See, for example, Zetsche et al (2021).

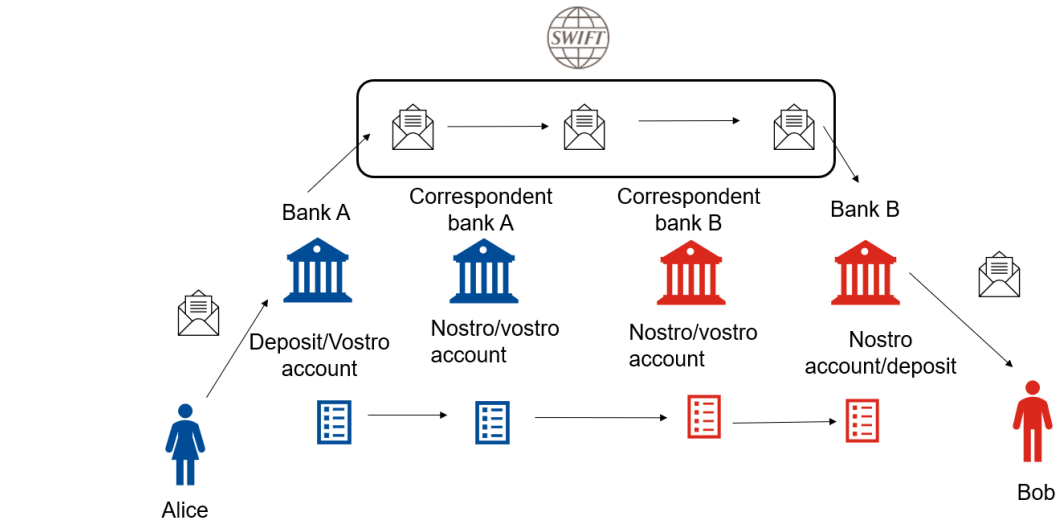
Figure 2.2. Cross-border payment using X-C.

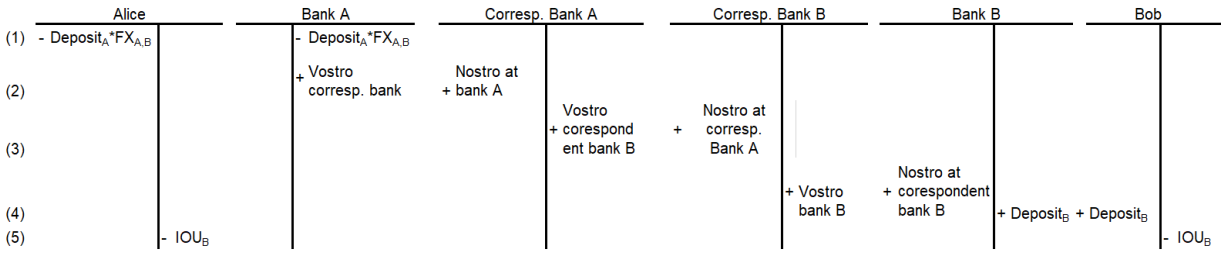


	Alice		PSP_A		$Bank_B$		Bob	
(1)	- $Deposit_A$*$FX_{A,B}$		- $Deposit_A$*$FX_{A,B}$					
(2)		- CE_B		+ CE_B				
(3)					+ $Deposit_B$		+ $Deposit_B$	
(4)		- IOU_B					- IOU_B	

Note: The figure below shows how intermediaries can use the X-C platform to send encrypted transactions on behalf of their clients. Central banks are depicted as they are participants in X-C and needed for initial funding (see figure 2.1 for that) but they are not needed for this specific transaction (see figure 2.2). Balance sheets would adjust so that a resident of country A ("Alice") can use X-C to cancel a debt she may have with a resident of country B ("Bob"). Transactions are shown sequentially for clarity. First, Alice sends an order to her PSP to use funds in their deposit account to make a transfer to Bob. These are converted to currency B by her PSP at a rate $FX_{A,B}$. Using X-C, the PSP then sends CE_B to Bob's bank. $Bank_B$ credits deposits to Bob, and Bob cancels Alice's IOU_B.

Figure 2.3 Cross-border payments using correspondent banking





Note: The figure illustrates how a cross-border payment is done using correspondent banking. Each bank must adjust bilateral assets and liabilities while sending payment instructions using Swift messages. Balance sheets show how they use vostro and nostro accounts to create bilateral exposures and move value across borders. For simplicity, in this example, bank A is assumed to make the FX conversion to currency B using its balance sheet.

X-C is a dedicated infrastructure for cross-border transactions that would complement existing domestic payment systems and would not require harmonization of existing infrastructures (other than the connection to the platform). As described above, central banks would provide the on-off ramp for domestic currency funding and redemption of funds. Participants would retrieve information and send instructions to the platform (including contracts) using APIs.[40] The only important feature would be the 24x7 availability of a wholesale RTGS and access to central bank reserves to CE conversion as this acts as the bridge between traditional rails and the platform.[41]

The modularity of X-C would also have the benefit that central banks could develop new solutions (including CBDCs) for domestic use without being constrained by potential interoperability requirements. Having CEs as a dedicated digital liability for cross-border transactions would allow central banks to pursue the design of their CBDCs to achieve their domestic policy goals, rather than having to coordinate it.[42] Box 2.1 compares CEs to other types of money.

[40] Banca d'Italia (2022) explores models for interoperability between an instant payment system (TIPS) and DLT-based solutions. Two specific experiments allow for the synchronization of the asset-leg and the cash-leg of a DvP (delivery versus payment) transaction. Both use the Target Instant Payment Settlement (TIPS) platform to provide the settlement services of the cash leg. The first, named "TIPS Hash-Link", is a lightweight, API-based and DLT agnostic protocol which enables a loosely coupled integration of the market infrastructure with the majority of DLT platforms. Inspired by the Hash-Time Locked Contracts (HTLC) protocol, TIPS Hash-Link has been specifically tailored to overcome some failure scenarios commonly experienced with HTLC, leveraging TIPS as a trusted escrow for funds and a smart contract to coordinate the DvP operations on the DLT in a safe and consistent manner. The second one, named "TIPS-Algorand Just in Time Locking", takes advantage of the features offered by a specific DLT platform, Algorand. In particular, it leverages a native feature of the chosen DLT that simplifies DvP transactions guaranteeing atomicity; as such, this approach needs the two systems to be directly connected to interact with each other.

[41] Limited RTGS operating hours availability could be a challenge. In that case, the platform would be operating after-hours, while the domestic infrastructure is not available. See CPMI (2022a).

[42] See Soderberg (2022) for a discussion on policy goals and design considerations for six advanced CBDC projects. See BIS (2022) for a survey on EMEs' potential policy goals for a CBDC.

Box 2.1 How do CEs compare with other payment instruments?

CEs allow more agents access to central bank reserves. It opens access to non-bank financial institutions, NBFIs, and payment-system providers, PSPs, and to non-residents. While non-residents may have access to paper currency, in practice this is not useful for high value cross-border transactions or wholesale payments in general

Compared with commercial bank deposits and stablecoins, each country's CE provides settlement finality and, as it is a central bank liability, the same as are paper currency, reserves, and CBDC, it is homogeneous and has no counterparty risk. CEs share an important dimension with stablecoins as both are programmable (see section 1.2). A key comparison is with CBDCs. While access to those may vary depending on the country and could potentially be used by non-residents (and thus be useful for cross-border payments), CBDCs may be designed for specific country circumstances and are not expected to be coordinated internationally to be on the same ledger. Thus, while CBDCs may be indeed programmable for their users, cross-border transfers are sometimes an afterthought. With CEs we directly address the need for a multi-currency platform.[43]

Table 2.1. Alternative types of monies as payment instruments

		Public				Private	
		Cash	CB reserves	CBDC	CE	Bank deposits	Stablecoins
Access	Retail	Y	N	?	N	Y	Y
	Banks	Y	Y	Y	Y	Y	Y
	NBFI+PSPs	Y	N	Y	Y	Y	Y
	Non-residents	Y	N	?	Y	Y	Y
Settlement finality		Y	Y	Y	Y	N	N
Cross-border transactions		N	N	?	Y	Y	Y
Common ledger		N	N	N	Y	N	?
Programmable		N	N	?	Y	N	Y

[43] The concepts behind CEs have precedents in the Inthanon-LionRock project and its "Depository Receipts" and in CITI's Regulated Liability Network https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf

Platforms must have common rules, governance, and standards, and a technology to reduce risks and costs of exchange (see CPMI-IMF-WB 20222). All these can be holistically called part of the “infrastructure” as it implies the provision of public goods that all participants benefit from. This common infrastructure can also contribute to increasing transparency in cross-border payments: procedures are clearly specified, must be followed, and are enforceable.[44]

The operation of the platform can benefit from the automation that its technological features enable. The different “actions” in the platform can be executed by computer code (smart contracts) and would not have to rely on a supranational entity to perform them. Put differently, the solutions we propose in the following sections are done by code that can read and act on the platform and can protect and manage data to ensure trust while allowing new business models to form. Financial transactions like simple cross-border payments, FX conversion, or more complex hedging or risk sharing agreements (e.g., see section 4.3) are written and enforced as “smart contracts” (computer code). This is achieved thanks to such code stored and executed in the platform’s ledger.

Transactions and changes in accounts’ holding can be validated by a central authority (“single node”) or by more than one (“multiple nodes”). This decision will vary depending on the agreed governance, the trust participants may have on a central authority, and the required need of resilience in the ledger.[45] Thus, the choice of the underlying technologies and whether validation should be done with DLT or centralized databases should be weighed against differences in terms of cyber-security, resiliency, and governance.

For example, a centralized ledger architecture can entail efficiency gains, but it also concentrates risks (if this ledger were to be attacked or corrupted). Distributed computing can also make the physical infrastructure more resilient.[46] A centralized ledger, however, can also concentrates the control mechanisms and tools to detect misbehavior. Concentrating transaction and operations provide the data for algorithms implementing automatic detection of suspicious activities to function (for instance the "siphoning" of funds, either from abnormally few numbers of accounts, or to abnormally few numbers of accounts). All these issues must be considered together with governance models. A cost-benefit analysis on technology choices is beyond the scope of this paper and is left for further work.

New multilateral platforms such as X-C could be operated under different structures and with different roles for the public and private sector (CPMI-IMF-WB 2022). Fair participation requirements, pricing, open access and governance arrangements which uphold the policy objectives of competition and interoperability should be priorities.[47] As challenges may arise from large stakeholders, ensuring broad representation in decision making would be important.[48] The existence of different commercial interests, and divergent views on the cost-benefit analysis, may require public intervention from an early stage to allow the development of a platform to

[44] For example, to perform as a safe asset, CEs will require a sound legal underpinning. Legal soundness of the platform and its functionality may require arrangements involving multiple legal jurisdictions (see CPMI 2019).

[45] For example, Project Hamilton deploys 4 nodes. See Federal Reserve of Boston (2022)

[46] For example, Project Hamilton’s phase 1 used DLT and focused on continuing to provide system access and preventing data loss even in the presence of multiple data center failures.

[47] In the case that a platform’s uptake is high, the public sector should ensure that the platform does not use its market power to extract excessive rents from participants. See CPMI, IMF, WB (2022).

[48] Existing global governance structures like the one supporting Legal Entity Identifier (LEI) could be used as a guide. See FSB (2022).

progress. Costs associated to establishing and sustaining a multilateral platform should also be considered and its fees, prices, and business model should also include cost-recovery considerations.

Risk management must be incorporated in design from early stages. Risks arise from financial integrity, operational and cybersecurity risks, but also financial stability, sustainability of the ecosystem needed around the platforms, and implementation risks (for instance, in failing at developing sufficient overall adoption or adoption in targeted participants).[49] We go back to financial integrity issues and data management in section 3. We discuss financial stability risks in section 4.

To the extent possible, design should consider how to minimize the needs to harmonize legislation relative to data, digital ID, commercial and financial transactions, insolvency, and central banking and payments. For instance, if inconsistency between national insolvency regimes is not addressed, the finality and irrevocability of payments may not be achieved. Moreover, the governance of the platform and the design of contractual agreements between the participating countries might require legal reform.[50] Also, smart contracts still suffer in many jurisdictions from legal uncertainties (and therefore from legal risks) especially in terms of the application of commercial and financial law.[51]

The specific design of such arrangements could be tailored to the scope that a platform may have. For instance, a platform in a region may have a different governance design relative to another one in a different region. Sufficient compatibility across potential X-C regional platforms, however, would be desirable to allow for interoperability among them.[52]

2.3 X-C as a Dynamic Ledger for Contracting

There are three key technological features in X-C. These play different roles in the different use cases. These are (1) a common and unique ledger with participants' accounts, (2) programmability, and (3) encryption techniques.[53] We outline different ways in which these components can be recombined or unbundled depending on the use case, and how several of these combinations can satisfy our technological requirements.

---

[49] International organizations that may want to be part of a multilateral platform like X-C at a regional or global levels should carefully consider the operational and legal risks that this may create. For example, if an international organization were to be in the operation of the platform, assessment should be made to identify the new legal obligations and risks that may result from this. For example, the organization may become subject to strict national data protection laws (e.g., GDPR) if the data processed as a result of this operation is qualified as protected data under such laws; the organization's legal and/or reputational risk related to AML/CFT compliance (see section 3 for a general discussion of these risks); the organization incurring risk of litigation and legal liability for indemnification for malfunctioning or hacking that could result in damages to third parties. Note that in all of those areas, even if the international organization chooses to outsource, it would legally remain the ultimate responsible entity.

[50] For example, some national laws prohibit creating liens over sovereign assets which could be an obstacle for closing out a default position in the platform, or reform might be needed to give central banks the power to participate or to issue CEs if the latter are considered under the law as a new type of central bank liability.

[51] This applies especially in areas such as contract formation, authentication, and performance. For example, how can general legal principles of good faith or fair dealing be applied in terms of the performance of contract executed by smart contract. For further details see Garrido et al (2022).

[52] The required features for such interoperability across different platforms are beyond the scope of this paper, but certainly should be carefully investigated.

[53] These features are bundled in blockchain ledgers. These blockchains also have validation procedures that are embedded (proof of work, proof of stake, or permissioned blockchains). Here we discuss these features separately as they serve different purposes. As stated above, we are agnostic about the validation procedures. An innovation underpinning blockchain is that of distributed computing, which aims at building up resilience: in case of hardware failure as in the case of an attack, or in the case of software

X-C's first key technological feature is the unique state of the common ledger. This ensures that all participants interact with the same dataset on who has or owns what. Put differently, participants' accounts must be always mutually consistent. In computer science terms, X-C needs to ensure a unique state of shared information. When a transaction or contract is signed or executed, this must cause a state change in the database and an update in the information that agents may retrieve from it.

With the introduction of a unique state of shared information, settlement risks are mitigated. Once a trade contract or transfer is operated on this ledger, then the agreement and ownership are definitely recorded, not only validated by direct parties but also verifiable by all in the encrypted ledgers. This allows for "trustless" exchanges or transactions, but also allows participants to pledge assets that they do not have yet but have committed to buy (for instance through rehypothecation of smart contracts—more on this later).[54]

Our proposal generalizes schemes being developed for domestic[55] or cross-border uses[56] by creating the appropriate escrow accounts on a multilateral contracting platform, instead of staying within platforms centered around one private balance sheet or a limited function or use case. X-C's objective is to provide different complementary functions under the same umbrella, as this would result in greater efficiency, interoperability, and competition.

X-C's second key technological feature is its programmability. Put simply, this means that smart contracts can be written to read and potentially modify the data recorded in the platform's ledger. A smart contract is then a reusable snippet of code (a program) that is published into the shared unique ledger of the platform. The smart contract code can be executed via a transaction request to its address, and developers can write executable applications into the shared unique ledger by publishing smart contracts.[57,58] Because the ledger is common to

bugs and failure, or against both. These resilience protocols are what directly lead to the consensus protocols at the core of a blockchain (which in addition integrates cryptographic signatures to allow for identities and transactions between them, and a storage feature to keep track of funds and prevent double spend). This has received the bulk of attention in popular press on bitcoin and academic circles critical of the actual proof-of-work validation algorithm used. However, the blockchain includes more tools than validation, as it integrates cryptographic signatures to allow for identities and transactions between them; a storage feature using hashes to keep track of the history of funds in a data archive, with Merkle trees, to prevent double spending; and cryptographic puzzles with controllable difficulty to randomly select what is most likely an honest node. What is misleading about the 'blockchain' and 'distributed ledger' terminology is that these confusingly bundle all these tools together under one roof, so to speak, whereas in fact a subset of tools can be used separately in any particular application, as dictated by that application.

[54] Encryption can also help to make data sharing on the platform compatible with domestic and regional data frameworks and avoiding the need of a complete overhaul of such regulations.

[55] Therefore, it is not a surprise that many private actors are now racing to issue a platform that would allow easier, cheaper and faster pledging of collateral (BNYM and Blackrock on money market fund shares as collateral, JP Morgan with repo markets, DTCC for securities in general) among parties that do not rely on the same intermediaries (broker dealers or custodians). All these are great prototypes and application-specific projects, sometimes already used commercially, but emanating from the private sector and serving customers' needs rather than holistic policy goals.

[56] This is also a trend underway in cross-border payments, with private banks creating omnibus accounts where they receive fiat collateral from corporate clients, who receive in exchange tokens recorded on a unique shared ledger, which they can transfer to recipients in another country and currency, who can then redeem this token directly for fiat denominated in their currency. They can of course also reuse this token for further cross-border transactions and save liquidity as well as time and fees.

[57] This definition is consistent with the one presented in Ethereum's White Paper.

[58] This, of course, would be supervised by a specific body that the platform's governance would designate.

all participants and a unique state would be ensured, commitment of assets in one of these programs have to be non-conflicting with commitment of the same assets in another one of these programs.[59]

X-C's third key technological feature is the use of cryptography. Encryption is the process of encoding information to protect messages' content and authenticity, controlled revelation to maintain market depth, while securing senders and receivers' identities and privacy, providing additional guarantees on authenticity, commitments, and enforcement of contracts can help solve frictions that constrain financial contracts.

Encryption uses a key pair that consists of a public key, which can encrypt messages, and a private key in that space which is used for decryption of messages. The public key can be seen and used by anyone wishing to send something in an encrypted fashion to the holder(s) of the private key, which is the only one who can read the content of this encrypted message. Properties of the encrypted space make it virtually impossible to decipher an encrypted message without the private key that was used as part of generating it. Symmetrically, for an outgoing message, the private key can be used to generate a digital signature which can be verified by those knowing the sender's public key. Moreover, they can also verify the origin of the message and that the message has not been modified since it was signed. Likewise, the sender cannot repudiate the message after signing. For more details on this and other aspects of encryption see Townsend, Zhang, and Zhao (2022).

Encryption can solve communication and commitment problems. It further allows for a larger set of outcomes by making information flows a decision variable in the design of the contracts.[60] With modern privacy-preserving cryptography, a designer can also rely on an intermediate state of information, that can now be not only either fully public or alternatively fully private, but rather in-between these extremes. For example, pieces of information can be inputs to aggregation and computation, while remaining fully private for all the participants. That is, code and mathematical operations can be performed on a group of encrypted messages, and the result can still be revealed, without revealing the initial inputs.[61] Just as the ability to choose different production technologies may expand the "possibilities frontier," expanding the information flow technologies will typically result in an outcome closer to one without information frictions.

We use these three technological features to offer new designs tailored to the economic and policy problem of cross-border exchange. The rules for market exchange, contracts, and mechanisms can thus encode ex ante contingent actions or states and automate execution of these actions, so that one party cannot renege on a contract they had agreed on. The common and unique state of the ledger ensures that all agents retrieve the same information from the platform and trust that what others observe is consistent with this information. The smart contracts execute contractual arrangements that maximize participants' outcomes without the need for a trusted third party to implement or verify the contractual arrangement.[62] And encryption allows participants to share private information with the smart contracts without revealing it to other parties.

[59] The consistency of the deployed smart contracts is fundamental for the safety of smart contracts where agents commit to deliver an asset that they themselves should receive from another agent (that is, when pledges are rehypothecated). We revisit this important point in section 4.

[60] In the mechanism design literature tends to focus on whether information is revealed truthfully. When encryption is introduced, the mechanism can also incorporate a decision on which, how, and with whom information is shared.

[61] As in a series of studies such as SCRAM; see quotes of studies and nuances between them here https://scram.mit.edu/

[62] In the language of contract theory, smart contracts can be guided by mechanism design to ensure finding a constrained optimal arrangement, one that maximizes participants' welfare subject to incentive, resource, and limited commitment constraints. The

A first application of these tools is the use of smart contracts to address limited commitment in exchanges. Limited commitment is an important obstacle in legacy cross-border payments and gives rise to trade failures. Trade and settlement take place at distinct times. Thus, a holder of an asset may renege at the time of settlement on a previous trade agreement, to pass the asset back to the issuer, or to a third party as per a multilateral trade agreement. This can be a function of a change in circumstances between the time of trade and the time of targeted settlement.

Bilateral agreements may reflect the best intentions of both parties at the time of trade, but with limited commitment, the seller of the asset, or the purchaser as provider of liquidity, may not relinquish the relevant object at time of settlement, or at least, not at the agreed upon price. This hold-up problem is aggravated by the evolution of private unobserved underlying states which makes a party want to choose the most advantageous time of settlement or renege entirely. In short, there is counterparty risk when trade and settlement are separated. With that risk, trade is limited or may even collapse so no transactions are carried out.

A solution to the commitment problem is a system in which trades are carried out with code and ensures PvP and/or DvP. Under bilateral or multilateral smart contracts there can be no reneging, even if circumstances change. This means that if the delivery of an asset is promised, this asset will be taken automatically by the smart contract. This eliminates settlement uncertainty from counterparty risk. As Lee et al. (2022a, 2022b) show this is closely linked to the idea of "instant settlement."[63] Implementing this with escrow accounts (with either the assets locked in, or a commitment to deliver the assets from another rehypothecated smart contract), or with atomic swaps type PvP, can address the limited commitment and trade fails problem.

Atomic swaps use a smart contract to commit agents to an agreed simultaneous exchange of a smart contract, like a committed "handshake." Figure 2.4 illustrates how atomic swaps work with a simple example. Two agents (Alice and Bob) agree to exchange their domestic CEs (A and B, respectively) for future use on the platform. They enter a standard contract to exchange at a given FX rate.[64] Alice and Bob lock their respective CE funds in escrow accounts that are managed by the smart contract. The contract executes the exchange and unlocks the escrow only when both participants provide their temporary key (s) and "shake hands".[65] This protocol avoids reneging on the exchange, even if done sequentially: Bob observes that Alice entered her temporary key to get the CEs she wanted (and that were in escrow), and then can copy and enter it to get the

literature on mechanism design assumes the existence of a "social planner" that can implement the contracts. In practice, a third party that is trusted and that behaves non-strategically, or equivalent code, is needed for the mechanism design to work as intended.

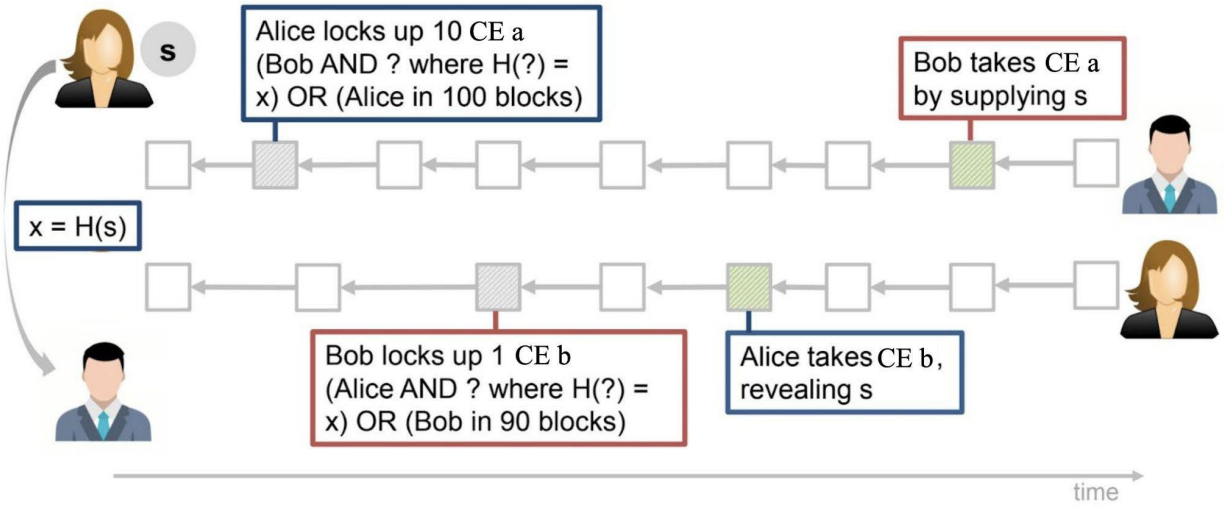
[63] The latter is an explicit goal of SIX, Finality, and HQLA of Deutsche Borse, R3, DTCC as expressed in their white paper (https://www.dtcc.com/-/media/Files/PDFs/White-Paper/Digital-Securities-Management-Industry-Update-White-Paper.pdf).

[64] In Section 4 we discuss FX rate determination.

[65] The contract uses a "hash function" H that is standardized and known to both participants. A key property of hash functions guarantees that for a given outcome X, one has to know the secret key s to produce H(s) = x and will not be able to find that private key s by chance. In the example, the smart contract contains the condition "unlock Bob's escrow to Alice if she sends an s to the contract such that it produces H(s) = x. Now that Alice sent her s to unlock Bob's escrow account, Bob can just copy this s and also send it to the smart contract, which has the similar condition "unlock Alice's escrow account to Bob if he can send an s that produces H(s)=x". The idea is that the contract relies on a participant's secret that unlocks both escrow accounts, and that the unlocking requires the participant to share this secret - in the process enabling the other party to copy it and also unlocking the funds he is due.

CEs he wanted (and that were in escrow). In practice, the figure below should be made symmetric so that Bob also has a temporary key and is also able to initiate the sequence, ensuring that no agents can block it once committed. There can be a short time window to enter these temporary keys, and were the contract not to receive the keys, original funds would be returned to agents.

Figure 2.4. Hash Time Lock and Commitment, guaranteed instantaneous trade and settlement



Source: Adapted from Narula (2018).

Note: the smart contract contains the condition "unlock Bob's escrow to Alice if she sends an *s* to the contract such that it produces H(s) = x". Now that Alice sent her s to unlock Bob's escrow account, Bob can just copy this s and also send it to the smart contract, which has the similar condition "unlock Alice's escrow account to Bob if he can send an *s* that produces H(s)=x".

These ideas can be expanded to dynamic future and conditional versions of atomic swaps. For example, these can require the seller to have contractual evidence that she will be in possession of the asset at the specified time. Buyers can then use the platform's ability to check that a contract has an underlying asset, thus allowing for rehypothecation of the contract (of the asset to be delivered). In borrowing and lending agreements, the contracts can also have a conditional provision which include the option of default and collateral forfeit. But full collateralization is not needed in all contracts, as penalties can be incorporated into the design.[66] Thus, as a general principle, not all trades on the digital contracting platform need to be fully collateralized with seizable assets that are escrowed. The platform's ability to check that a contract has an underlying asset allows for rehypothecation and interlinking contracts, thus saving collateral and conserving liquidity.

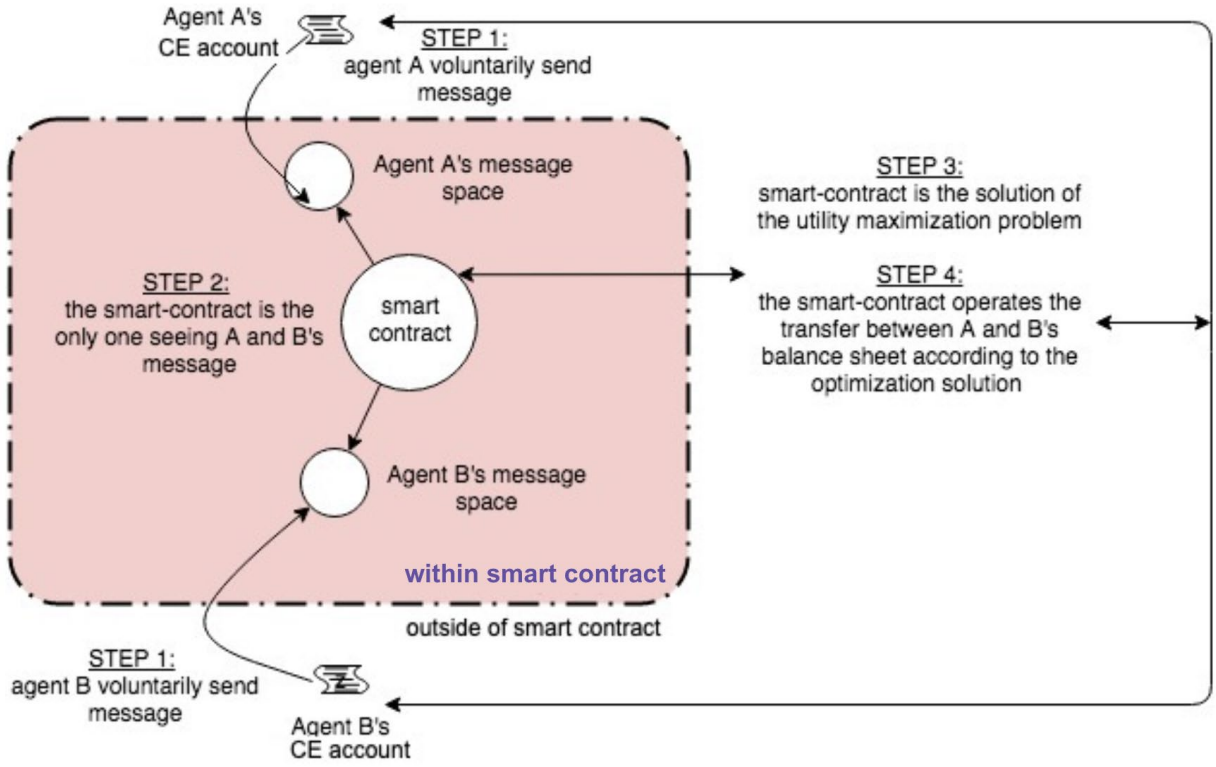
A second example of how the technological features can be exploited is the design of insurance agreements. Figure 2.5 illustrates how smart contracts and cryptography can be used in a bilateral risk sharing contract. Here, Alice and Bob agree on a smart contract where they commit to exchange goods at a given price, and in a guaranteed, PvP fashion. The maximum possible premium is put in escrow, in advance of the shocks. Both agents experience shocks to their balance sheets (for example, due to other trades or to market revaluations), but these are private. Under the contract, they are given an incentive to announce these shocks honestly, that

[66] Contracts without escrow and loans without collateral, if they are to be sustained, require a penalty, such as being kicked-out of future trades which would otherwise have been beneficial. Though history of past trades is likely encrypted, the code can nevertheless allow a contingency, that is, a trigger of exclusion is pulled when a condition is met, namely, not honoring the pre-agreement.

is, to send messages which are truthful. But the messages, encrypted, go into the code and are not revealed to others. The code then generates transfers, which can be positive or negative, on the two parties' balance sheets. In this insurance example, the risk across balance shocks is pooled, and one party is paying a premium and the other receiving an indemnity. See Townsend and Zhang (2020) for a specific example.

A third example is the implementation of auctions. In an auction, multiple parties bid over an object. The incentives for participants to bid honestly their valuation of the object are part of the design of the auction.[67] Observing the different bids and allocating the object to the winner would require a trusted auctioneer that should act non-strategically. The role of the auctioneer can be assigned to a smart contract that observes encrypted bids, ranks them, and determines the correct outcome of the auction (that is, who the "winner" is and what price she must pay). Buyers can audit the code and be assured it works properly and accomplishes the objective of the auction. Thus, the smart contract replaces the third party and creates trust in the mechanism. See Townsend and Zhang (2020) for a specific example. In section 4 we discuss how this can be applied to FX price determination in a multi-currency environment as X-C's.

Figure 2.5. Smart contracts, cryptography, and mechanism design.



Note: this figure portrays the balance of each of the two agents, A and B, which is subject to shocks. These shocks are announced as encrypted messages, going into the smart contract code. That pre-programmed code solves the optimal design problem, so that as a function of encrypted messages a transfer among the two parties is executed, giving a new state for the balance sheets.

[67] For example, the auction mechanism proposed by Vickrey (1961) makes the winner of the auction pay the second highest bid. This creates incentives to bid according the true valuation that each auction participant has on the auctioned object.

2.5. Contracts' Governance: "Supervised Open Contracting"

A fundamental aspect of X-C is how smart contracts could be deployed, for which use cases, and by whom.

The explosion of innovation triggered by the Internet and its open and layered architecture provides guidance. A key for this were Internet's common protocols, especially open ones—as emphasized by the Digital Currency Initiative at MIT in their design of a CBDC prototype. More broadly, engineers from the IT industry often refer to the Open Systems Interconnection model (OSI model) to abstract in different layers the communications happening in a computing system. Within an OSI layer, communications are organized via "protocols," which are agreed ways for all participants to interact. These are executed by components of an OSI layer speaking a common language (for the Internet, browsers are the components executing the common language of HTTP).

For the Internet, for instance, these shared standards allowed users to post messages and host them, create content, and post them at a website address that directs other users to the hosted content. From an OSI point of view, at the base level of Internet protocols lies Ethernet, which is how two computers can be connected to each other. On top of that lies TCP/IP, which specifies how to route messages in a network. Then the World Wide Web, and other layers come next. At each layer different successful companies provided unforeseen improvements to the overall architecture by developing their new layer, stacked on top of existing protocols. And even while they do so, these companies do not "own" the protocols on which they were based, nor do they control them. Each layer has a different stewarding body that oversees its deployment and potential changes over time.

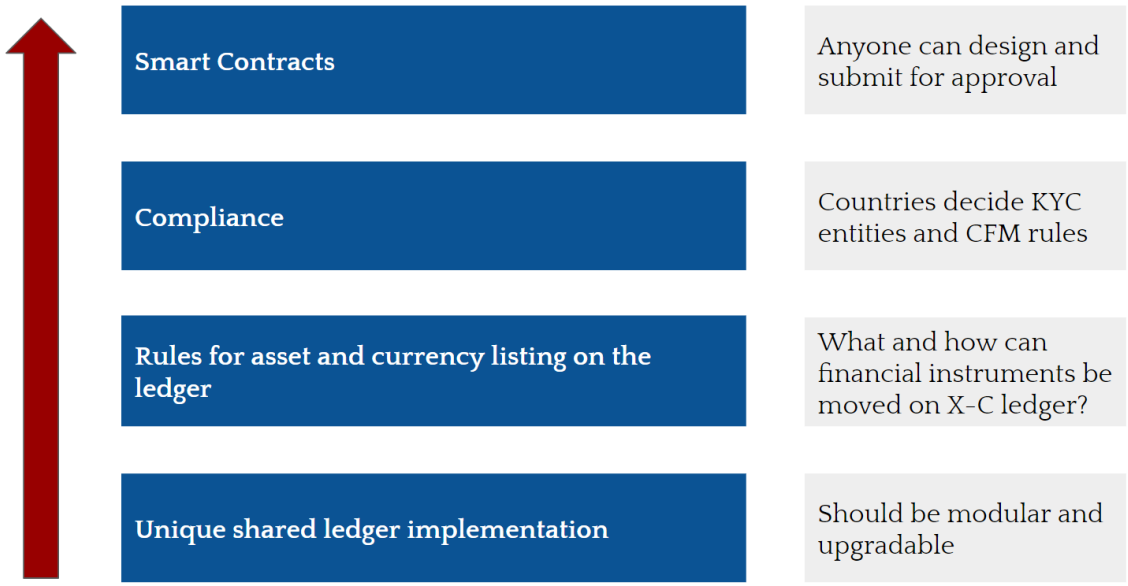
The openness and upgradability of this architecture is a desirable model that X-C aims to reproduce (in an economically safe and regulatory compliant fashion), as "future proofing" the infrastructure and contract structure would ensure that the investment to adopt it would pay off over a longer period of time. Figure 2.6 illustrates this analogy between OSI and digital payment technology stacks.

There are trade-offs between how open versus standardized protocols can be. For instance, open-source smart contracts are easy to standardize, but open standards like ISO20022 for payment information require more coordination and governance. Hence a layered architecture and open protocols can take a long time to develop, which is an argument to take into account existing successes in open protocols while designing a new system, so that the resulting platform builds on these existing protocols instead of replacing them.

In X-C (potentially pre-selected) participants could propose a smart contract to be deployed, and if it is validated by the platform operator or its oversight/governance bodies, then it can be integrated within the platform and used by any participant. X-C would start with "templates" that could be adopted. For example, smart contract templates for exchange via centralized multi-currency auctions, forward and risk sharing contracts could be proposed in follow-up papers and prototypes. The open access ensures competition and pricing on the platform, again, provided security and regulatory audits of the proposed contract to be deployed on the platform pass specified criteria.

With a library of smart contracts that can be deployed if approved, and with open contracting for participants of the platform, the objective is to foster competition, in which we can let users come up with contracts and code tailored to their needs and their existing relationships.

Figure 2.6. X-C as a protocol stack



3. Compliance, Data, and Privacy

Highlights

- X-C can deal with data, retain privacy, and comply with domestic and international regulations. X-C leverages cryptography to enable regulators and compliance officers to conduct checks, monitor and audit in a privacy-preserving fashion. Financial integrity checks and capital flow management measures (CFMs) encompass two sets of rules and regulations that can make cross-border payments slower, riskier, and more expensive.
- In the case of financial integrity, a major challenge is the required harmonization of KYC frameworks which requires multilateral coordination to ensure that the information generated in each country is trusted by others. CFMs are unilateral rules imposed by each country on resident or non-resident agents, so there is no need for inter-jurisdictional agreements.
- Strong privacy can be retained while preventing untraceable transactions by leveraging “credential providers” and control agencies together with cryptographic proofs and checks. This allows decoupling controls and user authorization from transaction submission and execution.
- “Credential providers” issue anonymous credentials, which ensure that only authorized persons can use the system while simultaneously protecting their identities. These credentials can be associated with actions that are outside the system (“off-ledger”) such as identity or with actions inside the system (“on-ledger”) such as limits to certain transactions amounts.

- The functionalities of X-C allow it to manage efficiently and in a privacy preserving way the information generated at the local level, to identify and vet individuals or firms that X-C ‘s participants may want to serve. For example, a transaction order can read a list of sanctioned individuals and attach a cryptographic proof that the individuals participating in a transaction were vetted and are compliant with, for example, AML-CFT rules.
- When CFMs are applied to holdings within the platform’s common ledger, the programmability can greatly simplify transactions involving CFMs. In this case, all the information needed for compliance is in the platform’s ledger, so smart contracts can read it and apply the CFM. When CFMs involve information generated outside the platform this requires a “bridge” so smart contracts can read that information. In contrast, CFMs that are applied by administrative decisions would be unlikely to allow for more efficiency.

This section explains how X-C can deal with data, retain privacy, and comply with regulations. X-C leverages cryptography to enable regulators and compliance officers to conduct checks, monitor and audit in a privacy-preserving fashion.[68] Financial integrity checks and capital flow management encompass two sets of rules and regulations that can make cross-border payments slower, riskier, and more expensive.

Information generated outside the platform will be needed to comply with both financial integrity and CFMs (for example, information on customers IDs, and a sanctioned individuals list, or on financial positions on ledgers not connected to X-C). In the case of financial integrity, a major challenge is the required harmonization of KYC frameworks. This will need to include multilateral coordination to ensure that the information generated in each country is trusted by others and that the adequate safeguards are put in place to ensure the quality and reliability of the information.[69] CFMs are unilateral rules imposed by each country on resident or non-resident agents, so there is no need for inter-jurisdictional agreements. In both cases, this section illustrates how X-C can help to reduce the costs and risks by automatizing compliance with these rules while preserving privacy.

The role of data (and the type of data collected or generated by X-C) is wider than what is discussed in this section. Data is not limited to user privacy, as aggregated anonymized data, non-user specific data, or trends may represent significant value for both private sector’s participants and would play an important role in adoption of X-C (see Rizaldy and Sun (2022)). Aggregated data can also play an important role for policy makers—specially to monitor financial stability (see section 4.3 for a discussion). Unpacking the type of non-private data available on the platform could also highlight the possibility of new functionalities, such as descriptive analytics (getting the pulse on what is happening live), diagnostic analytics (identifying emerging issues and their root cause), or even predictive analytics, possibly leveraging artificial intelligence. These issues are beyond the scope of the paper but deserve careful investigation in future work.

[68] Of course, regulators and supervisors would only access to the data of the entities that are in their scope.

[69] CPC’s Building Block 5 discusses different approaches to this. Amplus (2020) proposes a specific governance based on LEI to generate interjurisdictional trust and delegate KYC to specialized domestic entities. Other approaches may be possible. For example, the governance of X-C may recognize the authority of a country’s agency to determine an acceptable KYC scheme, specific to their jurisdiction, which does not need to be the same as another jurisdiction. As long as all participants trust that the approval of a KYC scheme is properly agreed, managed, and controlled, it might not be necessary for all parties to use the same KYC framework.

3.1. Privacy in Digital Payment Systems: Separation of Roles and Dedicated Cryptographic Schemes

Current designs of CBDC that aim to promote strong privacy while preventing large-scale flows of untraceable money do so by decoupling controls and user authorization from transaction submission and execution, leveraging existing controls agencies and using cryptographic proofs and checks.[70]

In general, separating controls from transactions allows for a very high degree of privacy. The intermediaries involved could be made to not see the identities of the sender and the recipient of a transaction flow, nor the amount involved. However, the relevant parties would receive cryptographic proof that the users and their transactions are compliant with rules. Transactions without a valid proof could be automatically rejected.

The approach usually followed to operationalize this is to design systems that integrate two cryptographic components. First, "credential providers" issue anonymous credentials, which ensure that only authorized persons can use the system while simultaneously protecting their identities. These credentials can be associated with actions that are outside the system ("off-ledger") or with actions inside the system ("on-ledger"). Off-ledger validation requires credential providers to attest that something is indeed true. For example, whether the sender or the recipient of a payment is who she says she is. On-ledger validation can be done directly by the system, for example, checking that a certain transaction amount is not above a specified limit.[71,72]

By applying this, details of transactions sent to X-C can be hidden in cryptographic commitments, and transactions themselves are authorized using digital signatures. This is illustrated in Figure 3.1, from one of MIT Digital Currency Initiative's work proposals. In the example, all details of the transaction are encrypted: its amount, sender and recipient's identities, and any metadata. All these would be encrypted on the platform so that no one can see its real value.[73] But the transaction would still carry a proof that a certain condition is true, without revealing anything else about the underlying information backing this proof. These proofs are called "zero-knowledge."[74] This can, for instance, attest that the sender and recipients are cleared off criminal lists, and that the funds being transferred do not exceed limits imposed by CFMs in their respective jurisdictions, even while the exact transfer amount and/or identities are kept secret.[75]

[70] See for instance the Hamilton project design. See Federal Reserve of Boston and MIT (2022).

[71] The possible governance of these credential providers is clearly a very relevant issue. In principles, these providers could be overseen by their country treasury or central banks, which are in turn overseen by a supranational entity. International cooperative oversight arrangements like a CCP college, CLS oversight committee or SWIFT G10 oversight are examples on how this arrangement could be designed.

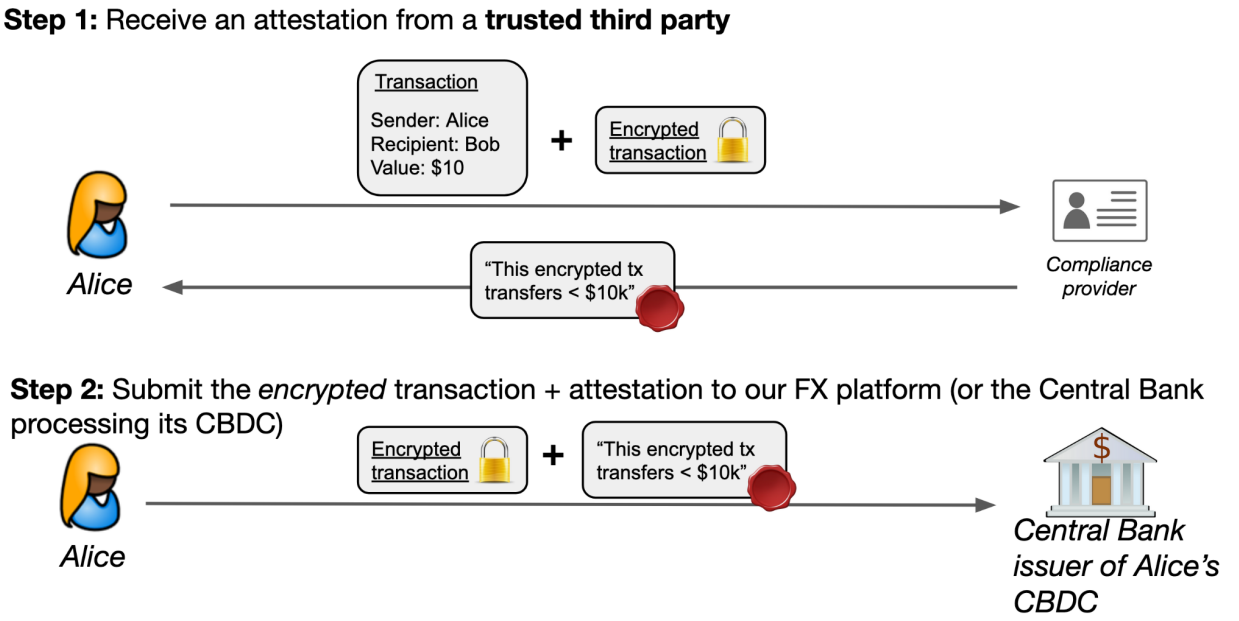
[72] This design can scale to volumes necessary for nation-scale CBDC, as the GNU Taler and the Hamilton project showed This can even be done in a privacy-preserving fashion, if the transaction data is encrypted to protect its privacy, but a certificate associated with the checking in question is provided (for instance "this transaction respects this compliance/capital control measure").

[73] Of course, mechanisms to reveal such information would need to be built in cases where there is an investigation by law enforcement.

[74] The name "zero knowledge" refers to the goal of these techniques, which is to prove that some condition is satisfied (e.g., "this transaction amount is compliant with capital controls") without revealing anything else in the process (i.e., without revealing the exact transaction amount).

[75] These zero-knowledge proofs can be as simple as a Petersen commitment, as in zkLedger. See Narula et al (2018).

Figure 3.1: Delegating verification using zero-knowledge proofs



Note: This figure inspired from MIT DCI's design illustrates the two points above: first in step1 a "compliance provider" checks that a non-encrypted transaction is indeed the one associated with the encrypted version provided, and that this transaction respects compliance rule XYZ. The compliance provider then issues a certificate that validates that this encrypted transaction is compliant with rule XYZ (the certificate is attached to the encrypted transaction, by for instance referring to its hash on the certificate—so that it is only valid for this encrypted transaction). Then at step 2 Alice can just submit this encrypted transaction (therefore protecting her private information, such as sender ID, recipient ID, transaction amount and other data), along with the certificate that this encrypted transaction is compliant, for the platform to process it, without gaining any private information. Different technologies could be used for the computation on top of encrypted transaction on the platform (such as zero knowledge described above), and the permissioned nature of our platform make these privacy preserving technologies much easier to implement than on public blockchains.

The separation of different parts of X-C into a set of trust-minimized components guarantees that the compromise of a single component does not impact the overall privacy of users. Data sovereignty can also be protected this way. Identity and information about users do not leave the country, but the transaction carries cryptographic proof that the transaction is being carried by identified individuals that are allowed to do so or that the transaction is compliant with limits. Thus, participants can be reassured that relevant rules (on who can make transactions and on transactions' characteristics) are being enforced

How privacy protection works can be illustrated by comparing CEs with other forms of central bank money. For example, country A's central bank issuing CEs may be able to directly monitor their supervised entities' X-C accounts (and their CE holdings). From that perspective, CEs would be akin to central bank reserves but on X-C's ledger. But when a CE issued by this central bank is held by a non-resident PSP, it could become more like cash: the central bank would know that it has been issued, but it may not be able to know who is holding it.[76] Of course, and different from cash, transactions using those CEs would need to comply with rules and carry cryptographic proof of that compliance.

[76] In cases where there is insufficient trust in other jurisdictions' supervisors, it is also possible to envisage that the issuer central bank could see which non-resident institution is holding its CEs.

Finally, data being stored and processed in different entities and kept confidential does not preclude privacy-preserving computations to be performed on top of these. As discussed in section 2 smart contracts with the right permission could still interact with encrypted data. This capability is explored in more detail in next sections.

3.2: Sharing Identities and Information Across Jurisdictions

The costs of preserving financial integrity represent an important friction in cross-border payments. At the domestic level, financial institutions must incur costs to comply with KYC/AML-CFT, but they preserve the data they gather by creating client relationships that generate market power. Initiatives like Open Banking aim to make some of this client's information "sharable". At the international level, there is no common governance for these vetting procedures and monitoring: not only is it expensive to gather this data on customers but it can also be risky to trust financial institutions from other jurisdictions as there can be uncertainty on the soundness of their procedures. Lack of common digital ID standards only creates more hurdles.[77,78,79]

The functionalities of X-C allow it to manage efficiently and in a privacy preserving way the information generated at the local level, to identify and vet individuals or firms that X-C 's participants may want to serve. For example, this information management feature can read a list of sanctioned individuals and attach a cryptographic proof that the individuals participating in a transaction were vetted and are compliant with, for example, AML-CFT rules.

Of course, this functionality "on-ledger" needs to rely on the trust-worthiness of the information created outside the platform ("off-ledger"). The provision of identification and vetting services would require additional governance to ensure that platform's participants can trust the information behind the proofs that transactions will carry.

The importance of providing a reliable framework for international identification is reflected in the multiple workstreams of the G20 agenda to enhance cross-border payments.[80] One possibility that creates a flexible

[77] There are other important hurdles to ensure financial integrity across borders. There can be inconsistencies in the legal and regulatory framework across jurisdictions (where national laws and regulations in different jurisdictions contradict each other or have incompatible requirements); rules which exist in some jurisdictions, but not others; rules which exist in all jurisdictions but are interpreted or applied in different ways or to different extents. There can also be inconsistent "supervisory approaches" across jurisdictions; especially if they fall short in complying with the international standard, may challenge the overall efficiency of the X-C platform and oversight over cross-border payment arrangements. There can be lack of standardization in data formats and data elements. There can also be lack of information sharing due to data protection and privacy concerns, lack of interoperability of cross-border and domestic payments systems. There can also be conflicts between AML/CFT laws and data protection regulations which might also affect the free flow of information across jurisdictions, in particular when related to sensitive data on customer due diligence measures. All of these important considerations are outside the scope of the paper but should be explored in follow-up work.

[78] The proposal by the Digital Identity Group, Amplus addressability module, or CPMI's Focus Area D aim to solve these hurdles.

[79] There are other reasons for this difficulty to share payments data across borders beyond KCY and AML/CFT considerations. These include data retention obligations related to domestic or regional regulatory and supervisory requirements, data security and privacy and consumer protection. The challenge to reduce these impediments while ensuring payments are safe and secure and that the data is handled appropriately should be a key part of a platform implementation.

[80] The Financial Action Task Force (FATF) is the chief organization for improving the effectiveness and efficiency of AML/CFT standards and co-leads building block 5 ("Applying AML/CFT rules consistently and comprehensively") of the G20 work on improving cross-border payments. Building blocks 6 to 8 also aim at improving the efficiency of compliance checks. See Bindseil and Pantelopoulos (2022) for a discussion on the relevance of this agenda.

governance framework is presented in Amplus (2020).[81] Their governance module relies on local providers (e.g., financial institutions, mobile operators) to identify and onboard customers. These would be overseen by a local authority, while the local arrangements (providers and local authorities) would be overseen by a supranational entity.[82]

The governance of the off-ledger identification framework could be part of X-C governance or could be a separate scheme, although complementarities and rules' alignment can potentially be easier if this were to fall under the same arrangement.

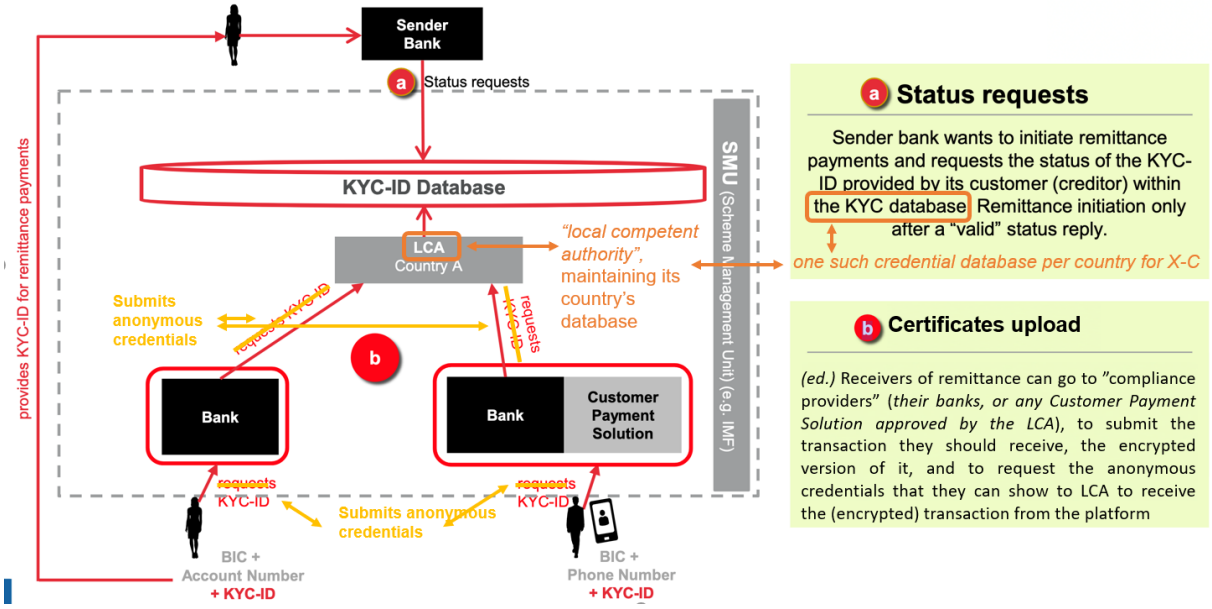
An example of complementarities between X-C's features with a common KYC framework would be the creation of business models specialized in KYC onboarding that can be 'monetized' when used for cross-border transactions. Once a KYC provider has on-boarded a customer and added her to the KYC list, transactions on X-C could carry the (encrypted) information of the provider that validated the identity of a final user. That could help create accountability, but it also could generate incentives to provide these validation services, as fees on that service could be paid with each transaction in which proof of that validation is attached. The implementation in the platform would have (1) KYC checks that do not leave national borders, (2) an instruction that adds a fee to the transaction and that it is sent to the initial KYC provider. Of course, this is only an example of how to leverage X-C to create markets and incentives. Other designs could certainly be feasible too. In all cases, the platform will require close coordination and cooperation to ensure the ongoing due diligence on the business relationships and the scrutiny of transactions thorough the course of the relationship (including KYC, their business, risk profile, and source of funds).[83]

[81] There are of course more general types of decentralized identity schemes like Decentralized Identifiers (DIDs). See https://www.w3.org/TR/did-core/#abstract

[82] Local operating units (LOUs) are responsible for implementing and assigning KYC identifiers. These LOUs are governed and overseen by a local competent authority (LCAs) with a scheme management unit (SMU) at the global level.

[83] Financial integrity risks associated with design choices must be assessed prior to a launch and develop the requisite mitigating measures. AML/CFT frameworks may need to be updated to account for its use in a multilateral platform like X-C and to ensure all relevant actors and activities are subject to AML/CFT regulation and supervision in line with FATF standards, especially if new providers that are not already regulated are part of the scheme. If needed, the implementation of the AML/CFT regime should be improved by addressing existing shortcomings and vulnerabilities and building capacity among competent authorities. In any design and implementation, it will be key to consider KYC as a continuous process and whether adequate resources can be in place to provide a front-end solution for end-users and assure compliance. Also, the required regulatory and supervisory framework should assess whether and how new potential service providers can ensure users financial integrity and provide adequate monitoring.

Figure 3.2: Extending Amplus' Identification Scheme with Encrypted Certificates



Note: This figure extends Amplus (2020) to include anonymous (encrypted) credentials and preserving data sovereignty.

3.3. Capital Flow Management Measures

The use of CFMs is common among countries and especially for EMDEs. This can be an important barrier that could hinder the development of multilateral platforms as improvements on cross-border payments.[84,85]

Depending on the different CFMs designs, the platform's capabilities will be easier or harder to leverage.

- **CFMs on the platform's common ledger:** when CFMs are applied to holdings within the platforms' common ledger, the programmability can greatly simplify transactions involving CFMs. In this case, all the information needed for compliance is recorded on the ledger, so smart contracts can read it and apply the CFM. For example, when non-residents ought to pay a tax or hold CEs for a period of time.
- **CFMs off the platform's common ledger:** when CFMs are applied to holdings that include balances outside the platform ("off-chain"), it is possible that solutions will need to be devised to comply with these CFMs and still have smart contracts in the platform. In this case, there will be a need to bridge this gap and bring information from an outside source (e.g., a commercial bank reporting system) to the platform, so smart contracts can read it and potentially apply CFMs to holdings within the platform. For instance, when CFMs are designed over an entity's total holding of domestic or foreign assets, the value held in the

[84] CFMs can be grouped schematically in three types: (1) quotas or taxes, (2) holding periods (a tax via opportunity costs), and (3) authorization requirements. These CFMs can be applied to non-residents ("inflow" CFMs) or to residents (so called, "outflow" CFMs).

[85] CFMs non-residents rarely distinguish between the type of agent (whether it is a financial institution, a corporate, or retail) that may hold a domestic asset. Non-residents can face limits on the percentage of certain assets they can buy. A typical example is that nonresidents cannot buy more than a percentage of a certain security or are banned outright on a certain security. They may also face holding periods on liquidation, authorization requirements, limits/control on taking out interest (related to investment duration), taxes for transfer of repatriation of investments, reserve requirements on short term inflows to loans, debt securities (on local banks against non-resident inflows).

platform (“on-chain”) will be reconciled with balance sheets held in traditional systems. This can create hurdles to the type of propositions that can be created in the platform. The hurdles can be overcome, for example, Inthanon-LionRock allows for Thailand to enforce their limit on non-residents deposit holdings.

- **Administrative decisions:** when CFMs are applied by “ad-hoc” administrative decisions, automatizing transactions is much harder. Since these permits are not administered and decided automatically, human intervention may impair the platform’s capabilities. For example, when an official needs to manually issue a permit for a transaction to be authorized, it will be more difficult to reap gains from programmability and automation.

4. Markets and Contracts for FX

Highlights

- FX spreads play a large role in the fees for cross-border payments and are usually a result of wholesale market underdevelopment. A better trading infrastructure, better risk management, and a more predictable policy environment can contribute to lower FX trading risks and better-functioning for FX markets.
- Currently, FX trade is mostly done through a set of oligopolistic intermediaries who carry different currency inventories. This requires large balance sheets, resulting in imperfect competition and in price distortions. When markets are decentralized or shallower, market power and distortions are usually larger.
- The centralization of information and exchange of FX trading can contribute to improving markets by increasing transparency and by creating incentives to increase competition. It allows for visibility on prices and quantities that are being actively traded. It also allows elimination of settlement risk from transactions.
- X-C is distinguished from other proposals by organizing FX exchange in a multi-currency environment that utilizes market design theory. Intermediaries act as broker dealers and compete to attract trade from clients. Also, multi-currency auctions are introduced as a robust solution that generates competitive outcomes and can be implemented entirely through smart contracts where no third-party auctioneer is needed.
- X-C is also distinguished by enabling participants to hedge FX risks via forward or contingent contracts, allowing on-platform FX derivative contracts and markets for those. Agents can also enter contracts that mutualize idiosyncratic risks though contingent on aggregate shocks. Smart contracts take as inputs the messages of all the agents with private shocks and implements a cross agent allocation
- X-C’s dynamic ledger can help control and manage financial stability risks from these derivative contracts without requiring full escrow or collateral. The dynamic ledger goes beyond preventing double spending of funds and avoids the double commitment of the rights to future funds that have been contracted with others. As smart contracts are part of the ledger, these can be made to be consistent with each other.
- When there is risk that cannot be diversified, the dynamic ledger can still allow for privacy preserving monitoring of exposures

4.1 Currency Exchange-Market Illiquidity and Hedging Contracts

For EMDEs, FX margins play a large role in the fees for cross-border payments (Feyen et al. 2021). This is usually a result of wholesale market underdevelopment: transactions in shallow and illiquid domestic wholesale FX markets are more expensive, and that pricing spills over to retail FX markets.[86] Where FX markets do not function well, inter-dealer FX market trades are irregular, insignificant, and shallow, and so de facto complementary markets FX hedging instruments do not exist. As a result, FX exchange can be costly for more illiquid currency pairs, and, in certain circumstances, it can reinforce existing players' market power in cross-border payments.

A key for well-functioning for FX markets is to reduce FX trading risks. This can be done by providing a better trading infrastructure, better risk management, and a more predictable policy environment. This can result in lower costs and risks of market making, so that this activity can be profitable at smaller spreads.[87] The centralization of currency trading can contribute to this, as it increases market transparency for participants. Trading rules and mechanisms within centralized structures are also important as these create incentives for a more competitive environment.

The next subsections present solutions for (1) organizing FX exchange in a multi-currency environment that utilizes market design theory, and for (2) designing hedging contracts to manage risks that utilize contract theory. These solutions distinguish X-C from existing proposals that use new forms of digital money for cross-border payments; these typically take market structure as given and do not discuss how programmability can be applied to improve contracts and markets functioning.[88]

4.2 Market Design: A Centralized Multi-Currency Market

In existing cross-border transactions, FX trade is mostly done through a set of oligopolistic intermediaries who carry different currencies inventories. Creating and carrying such inventories requires large balance sheets, resulting in imperfect competition and in price distortions. Where markets are shallower, market power and distortions are usually larger.

These outcomes stem from pairwise trading, which contributes to the inefficiency of legacy systems. Pairwise trading means that one currency trades against another (as if in a bilateral market or a series of bilateral markets) to complete the end transaction. This market structure is sometimes taken as a given in proposals to enhance cross-border payments.[89] Economic theory, in contrast, provides guidance for market organization. For example, theory can guide recommendations on how agents should meet and what should be the rules of engagement in those interactions in order to create desirable outcomes: more competition and higher efficiency can be obtained with a multi-currency centralized marketplace. This can help create market depth for illiquid currency pairs, mitigate market power, and facilitate cross-border transactions.

[86] See Rostek and Weretka (2015) for a theory of thin markets.

[87] For example, CLS reduces settlement risk (DvP) – this is an effective but expensive solution and only 15 currencies participate.

[88] As a result of this, most of the new proposed solutions for cross-border payments rely either on FX prices from legacy markets or intermediaries posting quotes. Bindseil and Pantelopoulos (2022)

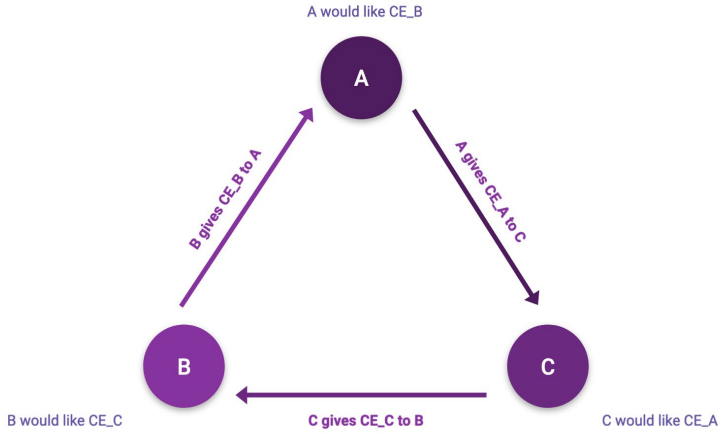
[89] See, for example, Bindseil and Pantelopoulos (2022).

The organization of exchange markets

Market structures that rely on decentralized environments (such as in OTC trading) are less likely to generate competitive and liquid markets.[90] There are three basic conceptual issues which are clarified by market design considerations.

The first issue is the absence of double coincidence of wants that can prevent trade when exchanges of different commodities occur in separated environments (that is, trade is done in bilateral segregated exchanges). If trade in currencies is restricted to be pairwise, then with an absence of double coincidence of wants, the result can be low volumes being exchanged. This is a well-known basic problem of monetary theory, and it applies to currency trade. Figure 4.1 provides an example, drawn from Wicksell (2013). In this static setup, an agent from country A wants to give up currency A to get ahold of the currency of country B, an agent from country B wants to give up currency B but to obtain the currency of country C, and an agent from country C wants currency A. In the absence of a centralized exchange, trades would have to take place pairwise, that is, one exchange market with trades for currencies A, B, one exchange market for B, C, and one for C, A. For the underlying example environment with three traders, there is no mutually beneficial bilateral exchange, and the outcome is autarky. On the other hand, if all three participants meet in a centralized platform, trade is possible. Agents need only respect their own budget constraint, that the value of currency surrendered as a sale be enough to sustain the value of currency acquired as a purchase.

Figure 4.1. Pairwise trade



Note: this figure illustrates a simple case where each of the agents want a specific currency. Absent a centralized exchange or a dealer, there may not be transactions.

The second issue is that coordination in the use of one currency as a unit of account and “vehicle” does not solve the problem of segregated exchange. That is, even with the use of one specific currency as part of each bilateral trade, multiple equilibria and market power still arise in segregated markets.[91] For example, if traders believe there will be no active market in one of the currency markets, then no one will trade there. This type of

[90] See Weill (2020).

[91] Shapley and Shubik (1977) trading post environment is similar to legacy market structure with a dominant currency as means of exchange. One currency is designated as the means of payment, and each of the other currencies has its own market in which that currency can be bought or sold for the dominant one. Multiple equilibria is one problem

self-fulfilling prophecy can be a source of market illiquidity and shallowness. When these arise, two things happen. If there are few participants to buy, the price can move against them when they place orders.[92] But also, it is more likely that some agents will have market power as it becomes easier for large players to be strategic and extract rents. More generally, fears of lack of liquidity and uncompetitive environments can discourage participation and leave thin markets.

The third issue is that lack of information centralization prevents segregated exchanges from achieving competitive outcomes. Agents may not have visibility of which prices are being traded by others, so they may not be able to properly value their positions. Moreover, agents with larger balance sheets will engage in more trades and thus will be able to profit from a better understanding of market conditions. Agents also may not have visibility of the volumes being traded. This can lead to coordination problems, inefficient outcomes, and financial instability.[93]

Possible solutions to these issues create yet other problems. A first possible solution is that all participants are endowed in ample amounts of a common currency, so that each can buy before selling, if need be, given the target efficient sequence of trades. But achieving a first best solution would require very large and costly liquidity buffers.[94] A second solution is a common large trader with sufficient inventory of all currencies, so that this intermediary would be able to sell to whomever arrives without stock outs. This also requires that inventory be large and creates excessive market power. A third solution is to have currency trade run on pre-allocated credit. This creates exposure to credit risk.[95]

Centralizing information and exchange can limit these problems. From an aggregate standpoint, it allows for visibility on prices and quantities that are being actively traded. It also allows elimination of settlement risk from transactions, as traders' financial position can be checked. But even more so, recording the trades serves as a reference for future exchange.[96] This is particularly important for contracts, as discussed in Section 4.3.

Centralized dealers' markets

The X-C platform provides two ways in which a centralized marketplace can be organized. First, intermediaries such as broker dealers can compete on the same platform to try to attract trade from clients. Second, multi-

[92] Shapley and Shubik (1977) use a rule for price formation which is strikingly similar to AMM of crypto, with price as the ratio of demand orders to supply orders.

[93] Suppose traders meet pairwise, with segregated trade in each pairwise market at each moment in time even if there can be multiple pairings at each moment in time. Participants in a given market may not know the history of trades of others with whom they or other current participants have not yet traded. Ostroy and Star (1974) refer to this as information decentralization and they show that in general, it is difficult with information decentralization to coordinate on an efficient outcome. Townsend and Wallace (1987) show a similar problem arises if the issuance of high velocity circulating debt is not coordinated. Spector and Townsend (2020) give an example where lack of coordination can lead to sharp drop in prices and welfare losses.

[94] As an example, real time gross settlement (RTGS) is in practice implemented paired with different liquidity savings mechanisms. Thus, payment systems are typically hybrid. See Bindseil (2004).

[95] An example of this are the risks incurred by central clearing counterparties (CCPs).

[96] More formally, with a multi agent contract among participants, an algorithm would prescribe how agents should behave when they meet, with code taking as input histories of trade on the platform database.

currency auctions can deliver a robust solution that generates competitive outcomes.[97] Thanks to X-C's capabilities, these auctions can be implemented in the platform in a privacy-preserving way and without the need of a trusted auctioneer.

X-C allows for centralized order book exchanges for dealers, but with dealers competing on the common platform. Dealer exchanges sponsored by market makers competing can generate competitive outcomes under two conditions. First, there must be free entry into market making. All participants should be allowed to act as dealers and offer terms of trade on the platform to attract other buyers and sellers, with the exchange of currencies coming from others through the consequent order book or from the dealer's own inventory. Free entry prevents capturing clients and allows for price arbitrage.[98] Second, their posted prices should be hard commitments: orders from clients must be honored, and the dealers are not allowed to stock out or renege from their announced terms of trade. In the jargon of the financial markets, these posted prices should be "hittable".[99] [100]

With multiple active intermediaries proposing trades, the outcome becomes competitive. If there are two or more competing dealers offering different terms of trade, then clients would arbitrage away these differences.[101] In a frictionless environment, terms of trade offered by various dealers over vectors of assets should be identical. With these two results in play, any participant, whether client or dealer, must achieve an allocation of assets which is utility maximizing given the common price vector: this is the definition of a competitive Walrasian equilibrium.[102]

However, in environments where there are shocks and agents must continuously interpret "news", dealers cannot commit to terms of trade for any possible trade size. Thus, in practice, hittable quotes are limited to transactions that can be easily fulfilled.[103] This leaves the door open for market power in allocating large trades.

Centralized multi-currency auctions can provide robust solutions to generate competitive outcomes and limit market power – even for larger lots or when markets are thin. These are set-ups where trades in all the assets are connected to each other via both preferences and budget constraints. As assets are allocated simultaneously, this allows agents to substitute one object for another as dictated by preferences and that

[97] FX auctions have been used to increase FX market depth and visibility and as part of the policies to improve FX market functioning and allow price discovery. See Lafarguette and Veyrune (2022)

[98] Edgeworth's (1881) conjecture for a pure exchange economy was that outcomes would converge to competitive outcomes for a variety of quantity or price setting mechanisms, as more and more participants come to trade. This has a formalization in the more contemporary work of Debreu and Scarf (1963), that noncompetitive outcomes will be blocked by coalitions of traders seeking better outcomes. Such blocking happens when, with free entry, another dealer offers another contract, attracting the coalition. In the formalization, allocations that cannot be blocked in this way, which is denoted a core allocation, shrink to the Walrasian allocation as the number of participant clients gets large.

[99] Bindseil and Pantelopoulos (2022) propose a similar solution for an FX conversion layer for interlinking domestic payment systems.

[100] These posted prices would be available to all participants. The design could also envisage the real-time online publication of relevant summary statistics of these prices.

[101] Also, from the perspective of any one dealer, it would prefer to buy from the others at those price vectors rather than be at the mercy of leftovers after honoring client orders.

[102] See Arrow (1954).

[103] Clearly, the size of these lots is idiosyncratic to each market and its participants.

forces agents to bid in a way consistent with their budget constraint.[104] X-C applies this logic to multiple currency auctions.

There are different potential designs of multi-currency auctions that can generate competitive outcomes.[105] If agents submit net demand schedules for each of the currencies, Dubey and Sonderman (2009) show that this guarantees competitive outcomes. Multi-currency auctions can also be implemented as multi-product limit order auctions. There, each participant submits a vector of orders to buy and sell all the currencies simultaneously.[106] Dubey (1982) shows that this setup also generates competitive outcomes.

Centralized auctions in X-C also avoid the need of a common currency for trading. The unit of account for pricing in the auctions is only used to reconstruct relative prices for each pair. Any currency, whether it is traded on the platform or not, can be the "numeraire". The use of a currency for pricing is thus distinct from a potential role as "vehicle" currency needed to trade and connect other currencies. Under the competitive allocation in the auction, no arbitrage across currency pairs is possible as otherwise entities would not be maximizing profits.[107] More specifically, competitive prices for each of the currencies with an arbitrary (but specified) unit of account can be computed from orders and in such a way as to rule out arbitrage.[108]

Multi-currency auctions and private information

These auctions can be also implemented in contexts where there is private information. Different mechanisms for auctions in the literature can be specified.[109] But mechanisms to implement auctions can be designed to allow for price discovery and select what information is kept private and what is made public.[110]

Mechanism design offers a solution to the information rent extraction problem as a pre-coded set of rules for an auction. Agents in mechanism design problems are given incentives to announce truthfully. The concept of

[104] Klemperer (2010) shows this for what he refers to as multi-product auctions, in his case for securities, in which bids for one or several grouped securities are placed simultaneously by all buyers and sellers. The Bank of England did not engage in auctions for each security separately, one at a time. The intuition for why this works is that, first, agents can easily move away from a given security to another which is a close substitute in preferences. Secondly, an agent's proposed trades for a given security have budget implications, creating tightness or slack for that agent's net demand for other securities, which the bidder takes into account.

[105] Dubey and Sonderman (2009) provide proof of these results. Although their setup relies implicitly on public information on the environment, others have shown that even with imperfect information, market implementation mechanisms converge to Walrasian outcomes if there is a sufficient number of players and information is not "mononopolized". We take this up in the text below.

[106] For a buyer of a fiat currency, a limit order is the maximum price willing to pay and the maximal limit for the quantity demanded, and likewise for a seller, the minimum price willing to receive and the maximal limit for quantity sold.

[107] One can interpret this as a Walrasian outcome that delivers the price of each and every currency pair. If there are n fiat monies, there are n(n-1)/2 such pairs, so the vector of orders can be of high dimension. So, all currency pairs are priced in these auctions.

[108] This insight is applied by Ramseyer et al (2021) who propose a decentralized exchange (DEX) in crypto currencies letting participants securely trade assets without giving any single party undue control over the market. It achieves high speed, can handle numerous offers, and again eliminates internal arbitrage opportunities, so that a direct trade from asset A to B always receives as good a price as trading through some third asset such as using USD as a bridge. Finally, it prevents frontrunning attacks that would otherwise increase the effective bid-ask spread for small traders. SPEEDEX's key design insight is, again, to use an Arrow-Debreu exchange market structure that fixes the valuation of assets in a common unit of account for all trades in a given block of transactions.

[109] In Dubey (1982) for example, the premise is Nash equilibrium, and for that, each trader need only take as given orders of all other traders. That object for each can be aggregated while preserving agents' privacy using multi-party computation (see Section 2).

[110] See Parkes et al (2008).

"private-but-contributing-state-of-information" addresses a core problem in mechanism design: how private information that is revealed by agents is treated by the mechanism. Information held by agents is needed to convince counterparties and allow trade, but information cannot be fully revealed for fear of some counterparties exploiting the information.[111] This reinforces the point about the importance of privacy – if traders are unwilling to reveal their private valuations, they might worry even more about revealing their beliefs about the valuations of other assets and, for X-C, their valuation of different CEs or contracts around them.

X-C allows auctions to be implemented entirely through smart contracts so that no third-party auctioneer or intermediary, nor any other party, can see the bids of others, in contrast to legacy infrastructure. Both these aspects are important as they can shape social gains of trade and mitigate potential rent extraction.[112] They also make the governance and implementation easier in a multi-country set up. The bids are induced to be truthful but are themselves encrypted and hence kept private. Bids can then be rank ordered without revealing any information to different parties (using, for example, FHE methods[113]). This can achieve price discovery and an efficient allocation of auctioned currencies. The code (the smart contract) is designed to operate on these bids and replaces the auctioneer and the potential abuses of bids-wanted-in-competition schemes.

Implementation details

In practice, the frequency of these repeated auctions would need to be decided. For this, a solution can be coordinated commitment on how often these would happen: markets can be organized as swarms, attracting traders with pre-arranged periodic trading dates. Frequent trading (more auctions per unit of time) allows more immediate asset reallocation after new information arrives at the cost of a lower volume of beneficial trades in each double auction. A moderate market slowdown to the level of seconds or minutes per auction can improve allocative efficiency for assets with relatively narrow investor participation and relatively infrequent news.[114] In some contexts, auctions are run continuously. These decisions would be part of the overall design. Likewise, one can coordinate on some specific contracts that would serve as anchors to price others. For example, trade in on-the-run Treasuries is the accepted convention, creating a thick market most dates, even though the bulk of treasuries outstanding, in value, are not traded much. Lastly, business models must be sustainable and there has to be sufficient financial incentives to make participation in the centralized market to be worthwhile.[115]

[111] For example, in a generalized Vickrey auction, when reservations values are correlated, the auction involves asking each bidder to submit valuations contingent on all other bidders' possible valuations. See Varian and MacKie-Mason (1994).

[112] Townsend (1988) provides guidance on the social gains that could be collected by keeping messages secret.

[113] FHE and MPC have been used in practice. The same guiding principles can be applied to FX markets. For example, in an auction for an agricultural good buyers submit demand schedules, and the farmers submit supply schedules. The latter is proprietary information, reflecting farmers' underlying circumstances that they want to keep secret. Pricing in real time electricity markets is another example of the use of FHE and MPC. A decentralized protocol for local electricity trading allows the market to identify the selected bids, calculate the clearance price, and compute the total amount of electricity traded by the users belonging to each individual supplier. These same encryption techniques can be used in the platform to exchange fiat tokens while incorporating the relevant economics, for optimized design. See SCRAM for more details.

[114] See Du and Zhu (2017).

[115] In related work, He et al (2022) propose that the coexistence of traditional FX markets that settle at T+2 with FX markets with immediate settlement as the one proposed for X-C can generate a business case that may entice participation.

Box 4.1. Auctions, smart contracts, and pricing liquidity needs

There are other potential applications of auctions besides spot FX trade. For instance, Garratt (2022) shows that markets can be put in place to manage high frequency liquidity problems. End-of-day settlement which separates trade from settlement runs the risk of default, as noted. Real time gross settlement, RTGS, would require in principle every entity to have sufficiently secured balances to honor all payment requests from others instantly when submitted. In practice, liquidity savings mechanisms, LSMs, are adopted in conjunction with RTGS, with computer algorithms to determine who should pay whom and when, once a batch of payment orders are submitted. Nevertheless, the algorithms used by Central Banks suffer from logjams due to queuing and occasionally fail to find solutions (see Leinonen 2005).

But liquidity provision can be priced, in a market, as originally suggested by Garratt (2022). Sophisticated matching and assignment algorithms can be used to think about the problem of an optimized design, of who is executing payments with whom, potentially varying composition of subclusters over time. In Townsend (2022) linear programs are used to solve for efficient market structure and deliver type specific shadow prices for each potential cluster, where the cluster uses internal clearing for its membership. Conceptually, the cluster can be run by a broker dealer with its order book. There is an entry price into a group if the participant is benefiting, paying for liquidity, or a price received if a participant is helping others by providing liquidity. In the decentralization, traders respond by choosing the groups. Again, these shadow prices are type-specific prices in a price-taking competitive equilibrium, which, by design, achieves an efficient outcome.

4.3 Hedging Risks: Forward and Risk Sharing Contracts and Markets

Efficient FX forward and risk management is fundamental for achieving low FX transaction costs. However, in jurisdictions with shallow financial markets, availability of forward and risk management products can be limited. For instance, banks may not offer regular derivative transactions to clients, The general perception is that the market demand is too scarce to make it attractive for banks to engage regularly in the derivative market, while the regulatory uncertainty, or perception thereof, acts as a further restraint to any form of market engagement in hedging.

The features of X-C enable participants to hedge FX risks via forward or contingent contracts by allowing on-platform FX derivative contracts and markets for those. This contributes to a more competitive market structure for cross-border transactions, as it allows for smaller intermediaries to compete on a more equal footing. Smaller balance sheet size becomes less determinant of participants ability to manage risks.

There is a strong complementarity between the development of derivative and spot markets: agents need both an active, liquid, and well-functioning spot FX market, and to be able to price intertemporal trades in their own currency.[116] While this varies depending on the country, the discussion below proposes the option of an “on-platform” intertemporal market for domestic currency CE as well as a derivative market for exchanging CEs denominated in different currencies (FX).

[116] That is, a liquid term money market in domestic currency is also key for agents to price forward contracts, as it generates a yield curve.

In the rest of this section, we first discuss frictions in a simple intertemporal environment and how to address them with forward contracts implemented on X-C. Second, a richer use case for contingent risk-sharing contracts and their implementation.

Intertemporal and forward contracts

Agents may experience a deficit in a specific currency and would like to borrow it with the promise to repay that same currency at a future date. They need a counter party lender in that currency. Or, to give another example, a group of agents know they will have need of one given currency at a future time, perhaps because entering other contracts which require them to deliver another distinct currency in the future. This future spot trade can be managed by agreeing now on forward contracts in those currencies.

More generally, one can consider dynamic currency swaps. Traders have preferences over holding currency as an asset during various distinct sub-periods. Just as in a repo contract, traders have the asset, they give it up for liquidity, but then reacquire it at a designated time later, designated in the contract. Here in this multi-currency environment, two currencies can be swapped, with the exchange going in one direction when initiated and reversed at a designated future date.

Two obstacles that constrain currency swaps lending are limited commitment and private information.

- Limited commitment is a key obstacle to trade discussed earlier in the context of trade and settlement taking place at different points in time. The risk of the payer reneging, not granting ownership of a designated CE settlement asset to the payee, can be solved in the X-C Platform in which such trades are carried with pre-programmed code that prevents reneging.[117] With the X-C Platform, a promise to deliver is done with a contract which verifies that the party promising to deliver will have the assets in the portfolio or has contracted to get it.

- Private information is also a key obstacle to trade which remains even after the limited commitment problem is solved. Specifically, knowledge of ownership of an asset at the time of trade is a starting point for all the existing atomic swap designs, the ones being used correctly on other platforms. That is, in order to commit in the future to exchange, of one CE for another, at a specified date for example, the supplier of the first settlement asset has to prove that either directly, or indirectly she will be in possession of that asset at that future time. As Lee, Martin and Townsend (2022a) argue, there can be a problem with information revelation at the time of entering into trade.[118] If information is revealed, it can put the revealing part in an adverse bargaining situation. Indeed, this hold-up problem can reduce or even eliminate otherwise beneficial trade.

[117] See Lee, Martin, Townsend (2022a, 2022b).

[118] In a key example, there are three traders. Agent B is the intermediary agent who is paired in the trade period either first with agent A, then with B, or first with C and then with A. B takes on possession of the asset only to act as intermediary for A and C. Thus, if agent C knows that agent B has already entered into a trade agreement with A, agent C has bargaining power, knowing B has an asset he will want to pass onwards in the execution settlement period.

A solution to this information revelation problem is to leverage encryption and the common unique state of the ledger. This can conceal whether a party has entered into a prior agreement with another party or not.[119] In this way, negotiation for trade takes place when agents are uninformed about the histories of their matched partners. The latter data are kept secret at the time of trade and revealed later only when trades are being carried out in the settlement period.

X-C eliminates trade failures and reduces the need for buffers to achieve liquidity management. As in Lee, Martin, and Townsend (2022b), using dynamic atomic swaps allow trade and the movement of an asset to be separated in time, but on the other hand, there is certainty on settlement since the asset is contracted to be available and committed at the specified time. Related, liquidity does not have to be sequestered in advance in order to settle, and there is no need to store ex-ante liquidity (which would be costly), nor employ liquidity savings mechanisms, nor rely exclusively on broker dealers in order to allow execution of contracts. Rather, X-C allows just-in-time contracted liquidity management.

As with spot transactions, price discovery and allocation of forward contracts could also be implemented with multi-currencies-multi-forward auctions. In this case, the dimensionality of the auction would be larger, as it would involve delivery times. Taking into consideration the appropriate frequency of these auctions, these market designs can generate depth and achieve competitive outcomes.

Risk sharing contracts

Besides different financial needs at different points in time, agents that participate in X-C can be exposed to shocks. This may depend on the realization of an entity's own needs or, if it is acting as an intermediary, its clients' needs. For instance, valuation effects from movements in FX rates will affect balances.[120]

The existence of shocks as risk factors calls for insurance contracts. Under full insurance with full information on shocks and no other obstacles, then risk can be mutualized. Agent-specific idiosyncratic shocks can be pooled so that ideally no risk is borne. Common aggregate shocks cannot be avoided and, in that case, the more risk tolerant should bear more. It is important of course that risk sharing contracts be entered into before any information about shocks is realized. For example, if shocks were independent and identically distributed then risk sharing agreements entered in advance of shocks for each period would suffice to achieve an optimal allocation of risk.[121]

In more realistic environments, agents receive shocks to their balance sheet positions that are private information. If these shocks are not communicated, then obviously contracts cannot be made contingent on them. So typically, messages about shocks need to be communicated but there need also to be incentives to communicate honestly. Generally, this involves giving the agent with private information some kind of trade-off for voluntary disclosure. Encryption allows the sharing of this information safely to smart contracts, so others do

[119] In the example above, whether B has entered a contract with A.

[120] One can think as in microeconomics of price movements having income effects but here through balance sheets. Indeed, ignoring substitution effects, price movements change quantities of each of the CE assets (and liabilities if applicable).

[121] Likewise, if there were no shocks, then any remaining intertemporal variation can be handled with simple borrowing and lending arrangements. Converse if there are shocks then simple borrowing and lending is not enough to achieve an optimal allocation of risk.

not see the messages, thus allowing for schemes that result in less individual risk exposures.[122] But revealing shocks over time too quickly can damage the possibility of beneficial trade as it washes out insurer's incentives to enter into the contract. This is akin to a standard insurance, in which ex ante insurance possibilities are lost once an ex-post adverse event has occurred.[123] Box 4.2 illustrates these issues in an environment where agents want to borrow, lend, and insure against risks.

In X-C agents can enter contracts that mutualize idiosyncratic risks but contingent on aggregate shocks.[124] Further, risk pools can also be securitized to cater to different risk profiles of investors despite limited information. In these cases, the smart contracts take as inputs the messages of all the agents with private shocks and come up with a cross agent allocation. Agents do bear some level of risk, of course, to give them skin-in-the-game and make them reveal their shocks truthfully. Information from aggregate shocks can also be incorporated into the risk mutualization contracts. An example would be movements in FX rates. The contract shares outcomes across agents at point in time so this pool of resources can be "indexed" by these observable aggregate shocks.[125]

[122] An example of this could be serving retail clients liquidity needs

[123] Incentives to tell the truth in the second period are easier to muster if the sender in the second period, agent b, does not know what message was sent by agent a in the first period. The information- constrained optimal allocation is such that lying in the second period generates a very bad outcome for the sender with positive probability. Put differently, if there were full revelation of all messages, the outcome would be Pareto inferior.

[124] For example, multilateral coordination problems that could contribute to alleviate Mundell's n-1 redundancy problems.

[125] A second consequence is more subtle. The allocation mechanism also determines resources available over time. To achieve maximal efficiency with high powered incentives, those dynamic decisions need to be under control of the contract. See Townsend (1988).

Box 4.2. A Hybrid Model with borrowing, lending, ex-ante insurance, and private information

Consider a potential borrower with varying stochastic needs realized at the time of borrowing and a lender, who is on the other side of the trade. The lender in turn has varying needs at the time of future repayment. Before any of these shocks are realized, the two agents meet and agree ex-ante in a contract on what amounts will be borrowed depending on the realization of the borrower's shock and what will be returned, depending on the lender's shock.[126] While these random shocks themselves make intertemporal borrowing and lending insufficient, there would not be full ex-ante risk sharing either, due to the private nature of these shocks.

The optimal arrangement under these information constraints is thus a hybrid between borrowing and lending and insurance. Townsend (1982 JPE) shows as an example that the gain to enduring relationships can be captured, formalized in multi-period contracts. There is a borrower with unobserved current states of income, urgency for cash, or balance sheet shocks. There is a lender which, for simplicity, does not experience shocks and has known resources each period. Each can commit resources to the contract, putting maximum payout in escrow in advance. If the borrower's shock is low, inducing the desire to borrow, then that shock is announced under a message sent into the code, and the borrower receives payment from the lender's escrow. The amount is more than what would have been a loan in the simpler borrowing/lending contract without shocks, as it now has an indemnity component to compensate for the bad shock. But what the borrower receives is below the level of full insurance: otherwise, she would always claim the indemnity and there would be no incentive to announce truthfully the shocks she receives, and consequently no trade. Relatedly, if the shock is such that the first party with the shock wants to lend rather than borrow, to receive a net positive loan-plus-interest in the next period, then the party on the other side who receives the funds has put the sufficient income realized into escrow in advance in order to be able to repay. But the interest rate on this contract is lower than the market borrowing/lending rate, reflecting the movement toward more insurance. In sum, hybrid contracts work as flexible risk sharing arrangements for the needs of borrowers and lenders when there is private information.

[126] See Townsend (1988).

Box 4.3. Concealing histories

Privacy can be accomplished with encryption and multi-party computation even among all parties to the contract. One can think of there being three parties, borrower, lender, and the code as in Townsend and Zhang (2022). Again, one can think of agents with CE accounts subject to shocks. To keep privacy as to whether the borrower is in a high or low liquidity need, “a layer” of scrambling in the allocation is added so the lender is not able to infer for sure if the borrower is in the high or the low liquidity situation. Each agent sees the outcome and the allocation of funds that pertains to that agent, but not the messages from others that triggered that outcome. Moreover, the messages are encrypted, but the code is able to randomize when needed “as if " a trusted third party.

This scheme exhibits the power of encryption tools. Here it is harder to conceal agents’ “bids” than in the typical auction case. In an auction, bids are encrypted and in principle only the winner sees the payment of liquidity and receipt of the seller’s object. Here, the outcome of an auction is an allocation for all agents over time, so at least part of the outcome is seen by all at each moment, from which information can be gleaned. That information is carried over to the subsequent period, impacting incentives there. Thus, the allocation mechanism must encrypt messages and make further inference difficult as allocations are realized and messages are sent. One wants as much ex-ante insurance as possible over realizations of dynamic paths while mitigating strategic behavior that comes with announcements of private information. If the allocation is being randomized, then the smart contracts must (i) implement the randomization without knowing underlying states and (ii) ensure no other intertemporal contracts have been entered into which might be in conflict with and undercut this hybrid contract.

Financial stability and smart contracts

Financial market deepening and the development of markets for hedging contracts can increase efficiency. When paired with market structures that foster competition, these can complement X-C’s improvements on settlement and on FX market liquidity.

Left unchecked, financial derivatives can create financial stability risks. In legacy markets, if interconnectedness is high or large players are very exposed, these risks can become systemic.[127] In traditional financial markets, risks arising from large institutions are managed with different combinations of ex-ante prudential regulation.[128] This does not prevent risks arising in unregulated financial markets such as shadow banks, where excessive leverage and risk taking are not addressed and can result in the need of ad-hoc backstops, as when failures threaten to generate contagion effects. In newer financial markets like Decentralized Finance (DeFi) where there are no central institutions providing a balance sheet, risks are managed with high collateral requirements.

X-C’s dynamic ledger can help control and manage these risks without requiring full escrow or collateral. At the most basic level, a single state ledger prevents double spending of available funds. But the dynamic ledger goes beyond that and prevents the double commitment of the rights to future funds that have been contracted

[127] See Yellen (2013), Faruqui et al (2018).
[128] See FSB (2017).

with others. As smart contracts are part of the ledger, these can be made to be consistent with each other.[129] In the simple case of forward contracts, the platform can require proof that the agent that is committing to deliver will have the deliverable at expiration date. Importantly, this does not require the committed agents to have escrow liquidity. Other forward contracts would be valid collateral too. In this case, an original CE put in escrow can be rehypothecated without generating risks.

In more complex contracts such as the hybrid risk sharing schemes described above, the dynamic ledger could also check that payments will be delivered in different contingencies. The limit to this consistency check links back to the structure of the shared, common ledger.[130]

Thus, when a participant is entering a contract and is committing future resources, this commitment (even if in the future) is recorded on the shared unique ledger, and double commitment (analogous to double spend) is prevented. This is the core mechanism through which a smart contract that has received some commitments in the future will be guaranteed to be executed. Therefore, to make all contracts guaranteed to go through and all commitments be final, one only need to check that for instance one CE is escrowed at the start of a chain of contracts (with that chain of contracts potentially extending into the future, being reused/rehypothecated among different parties, and even being adjusted depending on contingencies). That verification can be automated whenever some parties want to enter a contract and check whether any party that is committing anything has in his possession the commitment of a CE escrowed somewhere on the platform already. This commitment of a commitment of a CE in escrow (instead of the current necessity of the commitment of a CE in escrow) reduces the cost in liquidity on the platform, while still guaranteeing settlement.

Furthermore, even when there is risk that cannot be diversified, the dynamic ledger could still allow for privacy preserving monitoring of exposures.[131]

[129] The dynamic ledger can enforce dynamic stochastic budget constraints to hold and to be mutually consistent both at all times and in different states of the World.

[130] Bitcoin and Ethereum are both distributed ledgers, however Ethereum allows smart contracts in addition to payments by providing also “a single, canonical computer (called the Ethereum Virtual Machine, or EVM) whose state everyone on the Ethereum network agrees on. Everyone who participates in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer. Additionally, any participant or any program on the ledger can broadcast a request for this computer to perform arbitrary computation. Whenever such a request is broadcast, other participants on the network verify, validate, and carry out (“execute”) the computation. This causes a state change in the EVM, which is committed and propagated throughout the entire network.

[131] See Abbe et al (2012) and de Castro et al (2020).

5. Policy Design and Implementation in X-C

X-C can be used to implement policies using smart contracts. It also allows the possibility of representing additional assets on the platform's ledger, which can also be useful for policy making. This allows for implementing domestic or multilateral safety nets, for creating FX intervention rules and implementing them on the platform, and for coordinating policies among different central banks.

Central banks are entities with escrow accounts on the platform. Each can trade in spot auctions and the other markets. But central banks also play a special role in X-C. Not only can each allow their regulated intermediaries to convert reserves to CEs (and CEs to reserves), but each central bank can also expand its balance sheet directly by trade on the platform.

A first example is the issuance of CEs in foreign currencies. While X-C is designed to foster trade and settlement in posted CE representation of domestic currencies by domestic central banks, there are cases in which access to an alternative version of a major currency could be desirable. For example, a regional version of X-C where the United States (U.S.) does not participate could find it efficient to settle in U.S. dollars.[132] If that were the case, a domestic central bank of the region could escrow reserves denominated in dollars and issue dollar CEs on the platform. Of course, this would require trust and/or external audits to ensure that the dollars would be available to be redeemed outside the platform. Note that this would be nothing other than a dollar stablecoin issued by a non-US central bank that would be native to the platform in which such issuing central bank participates. This highlights the underlying risk of reneging on the convertibility of CEs to a currency that such central bank cannot issue. Thus, this possibility should be explored with extreme care, when it may be proved to be a relevant use case, and only in circumstances in which this risk can be mitigated.

Another example is the implementation of domestic liquidity windows. Domestic liquidity provision to regulated entities is usually collateralized. Banks, for instance, pledge eligible collateral,[133] get liquidity in the form of central bank reserves to meet some obligation or some regulatory ratio, and charge a cost.[134] To implement such a financial safety net on X-C, eligible domestic collateral would be deposited at the central bank in advance, and then a certificate of this security would be issued on the platform.[135] This representation of the security does not need to be tradable, as it can be useful as an input for other contracts.[136] A party could show that it has an eligible security and thus has the right to tap a central bank liquidity window. This contingent liquidity could, for instance, lower the costs of borrowing, as the lender would know that the borrower would have access to CEs issued by its central bank.

[132] For example, SIPA is a multilateral payment platform where Central American countries trade. The settlement asset is U.S. dollars. Buna is another example in the Middle East that also uses U.S. dollars.

[133] Government securities are a very common pledgeable collateral, but central banks can decide to accept other types. The Eurosystem, for example, also accepts corporate bonds and including corporate bonds and asset-backed securities (see figure 3 The Eurosystem collateral framework explained (europa.eu).

[134] The cost is a choice of central banks that allows these liquidity windows to be accessed more regularly or on a more exceptional basis.

[135] An open question is whether eligible collateral would differ from country to country being the choice of each central bank (as it is today) or whether if it could instead be one general list for the platform.

[136] Of course, it could be tradable and a market for such securities could be created. But this is not directly related to cross-border transactions, so it is outside the scope of this paper.

Smart contracts can also be used to deploy cross-country liquidity. Participating central banks could establish borrowing and lending arrangements in which they could get CEs from another central bank that participates in the platform and use those to provide liquidity to its domestic private platform participants. These arrangements could be like liquidity bridges[137] (if relatively routine), to currency swaps (if used in more exceptional circumstances), or to regional financial arrangements.[138] To implement this, central banks can commit via escrow accounts and atomic intertemporal swaps to exchange CE certificates among themselves, as with credit lines and asset swaps but at an enhanced level relative to what is done currently.

Central banks can also implement contingencies for better risk sharing as their balance sheets are subject to shocks, strengthening the global financial safety net. Indeed, in this FX context, one could view the hybrid borrowing/lending-insurance contract as a swap line from one central bank to another. That is, a borrowing/lending contract that is called only in times of stress, in which the lender does not seek to gain from movements in FX rates (thus providing a subsidy to the borrower during these times of stress). Cryptography is also needed as with the private hybrid borrowing/lending-insurance contracts presented in section 4.3. This would allow central banks to keep their FX positions, policy, and reserve goals to themselves but still use that information to tailor swap line contracts and to achieve a degree of policy coordination.[139]

FX intervention rules can also be implemented on X-C. Intentions embodied in messages and actual bids from central banks can be aggregated in a privacy-preserving fashion.[140] Each participating central bank can communicate its preference for volatility bands for FX rates that reflect its policy choices given its risk aversion and reserve commitments. For example, a central bank can input contingent bids in auctions. These input parameters are not known to anyone, but a smart contract can find the best bands that satisfy all central banks and their reserve commitments, and automatically intervene when these volatility limits are reached. This would be an improvement on how swap lines are currently used.[141] This use of X-C's multilateral privacy-preserving bidding schemes could provide additional coordination tools and trust building among central banks, thus expanding access to international financial safety nets. It also strengthens central banks' credibility, as it allows them to make commitments on the X-C platform that imply losses when FX rates move outside these bands.[142] Since insurance mechanisms (as the one described in the previous paragraph) are linked to the volatility of FX rates, the implementation of these multilateral volatility smoothing rules could complement risk sharing too.

[137] See CPMI (2022b) for a summary of the risks involved and highlights that the case for establishing such bridges depends on context. It could also be noted there are very few existing liquidity bridges in operation today.

[138] For example, countries can pool resources to leverage financing when they receive shocks. These resources could be tied ex-ante to FX volatility. If volatility were to be above a certain threshold, funds could be released.

[139] See Townsend and Zhang (2021).

[140] See Lo (2011) and Lo and de Castro (2020).

[141] See Zhang (2021).

[142] See Lafarguette and Veyrune (2022) discuss how these ideas could be applied to induce volatility smoothing in the legacy FX market.

6. Conclusions

This paper presents a vision for a multilateral exchange and contracting platform. It proposes a design that centralizes payments and settlement and that integrates functionality needed for cross-border transactions: streamlining compliance, reducing the cost of FX conversion, and better managing financial risks. The paper also shows how new technologies can be leveraged to better organize payments and associated financial markets. These new technologies are ledgers with unique states, programmability that allows for automated financial contracts (“smart contracts”), and encryption which ensures privacy, and can alleviate the underlying obstacles to trade. These technologies allow the design of a multilateral exchange system where participants can truthfully share information with smart contracts but can retain privacy relative to other parties.

While new technology and appropriate economic design can go far in improving cross-border transactions, there are hurdles that require multinational coordination at a legal and political level. These include governance agreements, and aligned AML/CFT, legal, and regulatory frameworks. Furthermore, further reflections are needed to ensure the operational stability of platforms given their systemic nature. Finally, further work is needed to ensure regional platforms are interoperable. This will help counter geopolitical fragmentation.

Other important questions arise in terms of the role of the public sector (both country authorities and international organizations) in operating and developing platforms. The role of the private sector to ensure adoption and sustainable business models should also be further explored.

However, while these are all difficult issues, private solutions are being explored, tested, and deployed. However, not all may align with policy objectives like monetary sovereignty and financial stability, and some may create excessive market power, or evade international or domestic regulatory frameworks. This paper instead offers a solution where technological innovations are leveraged by the public sector for public policy objectives.

References

Abbe, E. A., Khandani, A. E., & Lo, A. W. (2012). Privacy-preserving methods for sharing financial risk exposures. American Economic Review, 102(3), 65-70. www.princeton.edu/~eabbe/publications/AKL_AER.pdf

Abidin, A., Aly, A., Cleemput, S., & Mustafa, M. A. (2016). An mpc-based privacy-preserving protocol for a local electricity trading market. In S. Foresti & G. Persiano (Eds.) *Cryptology and network security* (pp. 615–625)

Amplus (2020). https://www.bundesbank.de/en/tasks/payment-systems/publications/amplus/amplus-859690

Arrow, K. J., & Debreu, G. (1954). Existence of an equilibrium for a competitive economy. Econometrica: Journal of the Econometric Society, 265-290. https://www.jstor.org/stable/1907353

BdF-MAS (2021), Liquidity Management in a Multi-Currency Corridor Network https://www.banque-france.fr/sites/default/files/media/2021/11/15/bdf-mas-onyx_liquidity_management_in_a_multi-currency_corridor_network_vfinal_-_12112021_0.pdf

BIS Innovation Hub (2021) Inthanon-LionRock to mBridge: Building a multi CBDC platform for international payments, https://www.bis.org/publ/othp40.htm

BIS Innovation Hub (2022), Using CBDCs across borders: lessons from practical experiments. https://www.bis.org/publ/othp51.htm

Bindseil, U. (2004). Monetary policy implementation: Theory, past, and present. OUP Oxford.

Bindseil, U., & Pantelopoulos, G. (2022). Towards the holy grail of cross-border payments. Available at SSRN 4057995.

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J. D., Nielsen, J. B., Nielsen, K., & Pagter, J. (2009) Secure multiparty computation goes live. 325–343. https://doi.org/10.1007/978-3-642-03549-4_20

Castro, L. D., Lo, A. W., Reynolds, T., Susan, F., Vaikuntanathan, V., Weitzner, D. J., & Zhang, N. (2020). SCRAM: A Platform for Securely Measuring Cyber Risk. https://hdsr.mitpress.mit.edu/pub/gylaxji4/release/3

Chen, S., Goel, T., Qiu, H., & Shim, I. (2022). CBDCs in emerging market economies. BIS Papers. https://www.bis.org/publ/bppdf/bispap123.pdf

CPSS-IOSCO (2012), Principles for Financial Market Infrastructures (PFMI), Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions https://www.bis.org/cpmi/publ/d101a.pdf

CPMI (2019). Wholesale digital tokens. December 2019, https://www.bis.org/cpmi/publ/d190.htm

CPMI (2022a). Extending and aligning payment system operating hours for cross-border payments. Final Report. May 2022, https://www.bis.org/cpmi/publ/d203.pdf

CPMI (2022b). Central bank liquidity bridges for cross-border payments, July 2014 https://www.bis.org/cpmi/publ/cb_bridges.pdf

CPMI, BISIH, IMF, and WB (2022), Options for access to and interoperability of CBDCs for cross-border payments, July 2022, https://www.bis.org/publ/othp52.htm

CPMI, IMF, and WB (2022), New multilateral platforms and arrangements in cross-border payments, Forthcoming.

Debreu, G., & Scarf, H. (1963). A limit theorem on the core of an economy. *International Economic Review, 4(3)*, 235-246.

Du, S., & Zhu, H. (2017). What is the optimal trading frequency in financial markets?. *The Review of Economic Studies, 84(4)*, 1606-1651.

Dubey, P., & Sondermann, D. (2009). Perfect competition in an oligopoly (including bilateral monopoly). *Games and economic behavior, 65(1)*, 124-141.

Dubey, P. (1982). Price-quantity strategic market games. *Econometrica: Journal of the Econometric Society*, 111-126.

Faruqui, U., Huang, W., & Takáts, E. (2018). Clearing risks in OTC derivatives markets: the CCP-bank nexus. *BIS Quarterly Review December*. https://www.bis.org/publ/qtrpdf/r_qt1812h.htm

Federal Reserve of Boston and Massachusetts Institute of Technology Digital Currency Initiative (2022), Project Hamilton Phase 1. A High-Performance Payment Processing System Designed for Central Bank Digital Currencies, https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx

Edgeworth, Francis Ysidro (1881). Mathematical psychics: An essay on the application of mathematics to the moral sciences, volume 10. Kegan Paul, 1881.

Ethereum White Paper, https://ethspring.com/docs/introduction/introduction/1-ethereum-101#smart-contract

Feyen, E., Frost, J., Natarajan, H., & Rice, T. (2021). What does digital money mean for emerging markets and developing economies? In *The Palgrave Handbook of Technological Finance* (pp. 217-241). Palgrave Macmillan, Cham.

FSB (2017). Review of OTC derivatives market reform: Effectiveness and broader effects of the reforms https://www.fsb.org/2017/06/review-of-otc-derivatives-market-reform-effectiveness-and-broader-effects-of-the-reforms/

FSB (2022). Report on LEI. Forthcoming.

Garratt, Rodney (2019). An Application of Shapley Value Cost Allocation to Liquidity Savings Mechanisms, Working Paper.

Garrido, J., Liu, Y., Sommer, J., and Viancha, J. S. (2022). Keeping Pace with Change: Fintech and the Evolution of Commercial Law. *FinTech Notes*, 2022(001). https://www.elibrary.imf.org/view/journals/063/2022/001/article-A001-en.xml

He, Chusu, Milne, Alistair, & Zachariadis, Markos (2022). Central Bank Digital Currencies and International Payments. https://swiftinstitute.org/wp-content/uploads/2022/05/SWIFTInstitute_CBDCInternationalPayments_PublishedMay2022.pdf

Hertig, A. (2020). Ethereum 101. https://ethspring.com/docs/introduction/introduction/1-ethereum-101#smart-contract

IMF (2022), The Rapid Growth of Fintech: Vulnerabilities and Challenges for Financial Stability, *Global Financial Stability Report* Chapter 3. https://www.imf.org/en/Publications/GFSR/Issues/2022/04/19/global-financial-stability-report-april-2022#Chapters

Lafarguette, R., & Veyrune, M. R. M. (2021). Foreign Exchange Intervention Rules for Central Banks: A Risk-based Framework. International Monetary Fund. https://www.elibrary.imf.org/view/journals/001/2021/032/article-A001-en.xml

Lee, Michael, Martin, Antoine and Townsend, Robert M. (2022a), Optimal Design of Tokenized Markets. Working Paper

Lee, Michael, Martin, Antoine and Townsend, Robert M. (2022b), Zero Settlement Risk Token Systems, Working Paper

Leinonen, Harry (2005). Liquidity, risks and speed in payment and settlement systems: a simulation approach. Bank of Finland https://helda.helsinki.fi/bof/handle/123456789/9355

Mehrling, Perry (2013). Essential hybridity: A money view of FX. *Journal of Comparative Economics 41.2* (2013): 355-363.

Narula, N. (2018) Presentation for the Bank of Canada and Sveriges Riksbank conference on CBDC https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5e28b4bca9d3422148400c95/1579726012763/Redesigning+digital+money_++What+can+we+learn+from+a+decade+of+cryptocurrencies_%281%29.pdf

Narula, N., Vasquez, W., & Virza, M. (2018). zkledger: privacy-preserving auditing for distributed ledgers. In *Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation* (pp. 65-80).

Neilson (2022). Three big ideas for tokenized finance. https://www.soonparted.co/p/onyx-tokenized-finance

Ostroy, J. M., & Starr, R. M. (1974). Money and the Decentralization of Exchange. *Econometrica: Journal of the Econometric Society*, 1093-1113.

Parkes, D. C., Rabin, M. O., Shieber, S. M., & Thorpe, C. (2008). Practical secrecy-preserving, verifiably correct and trustworthy auctions. Electronic Commerce Research and Applications, 7(3), 294-312.

Ramseyer, G., Goel, A., & Mazières, D. SPEEDEX: A Scalable, Parallelizable, and Economically Efficient Distributed EXchange. https://www.scs.stanford.edu/~geoff/papers/speedex.pdf

Rizaldy, Ryan and Sun, Tao (2022). Lessons from Asian E-Money Schemes for the Adoption of Central Bank Digital Currency. *IMF Working Paper* (Forthcoming).

Rostek, Marzena, and Marek Weretka. (2015). Dynamic thin markets. *The Review of Financial Studies 28.10* (2015): 2946-2992. https://academic.oup.com/rfs/article/28/10/2946/1580141

Shapley, Lloyd & Shubik, Martin (1977). "Trade Using One Commodity as a Means of Payment," *Journal of Political Economy, 85(5),* pp.937–968.

Soderberg, G., Bechara, M., Bossu, W., Che, N. X., Kiff, J., Lukonga, I., & Yoshinaga, A. (2022). Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons. FinTech Notes, 2022(004). https://www.elibrary.imf.org/view/journals/063/2022/004/article-A001-en.xml

Spector, M. & Townsend, R.M. (2020). Notes on Townsend Wallace coordination problem. Working paper.

Townsend, R. M., & Wallace, N. (1987). Circulating Private Debt: An Example with a Coordination Problem. In *Contractual Arrangements for Intertemporal Trade*, Edward C. Prescott and Neil Wallace (eds.), Minneapolis: University of Minnesota Press.

Townsend, R. M. (1988). Information constrained insurance: the revelation principle extended. *Journal of Monetary Economics, 21(2-3)*, 411-450.3

Townsend, R. M. and Zhang, N. (2020), Innovative financial designs utilizing homomorphic encryption and multiparty computation, Working Paper.

Townsend, R. M. Zhang, N., and Zhao, Y. (2022), A Primer on Encryption, Working Paper. https://www.leadmit.com/_files/ugd/33f99a_3b12ddf1473640f2a486457ec2963d09.pdf

Varian, H. R., & MacKie-Mason, J. K. (1994). Generalized Vickrey auctions. https://www.deepblue.lib.umich.edu/bitstream/handle/2027.42/50432/gva3.pdf?sequence=1

Vickrey, W. (1961). Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance*, 16(1), 8-37.

Weill, P. O. (2020). The search theory of over-the-counter markets. *Annual Review of Economics*, 12, 747-773.

Wicksell, K. (2013). *Lectures on Political Economy (Routledge Revivals): Two Volumes*. Routledge.

Yellen, J. (2013). Interconnectedness and Systemic Risk: Lessons from the Financial Crisis and Policy Implications. https://www.federalreserve.gov/newsevents/speech/yellen20130104a.htm

Zetzsche, D. A., Anker-Sørensen, L., Passador, M. L., & Wehrli, A. (2021b). DLT-Based Enhancement of Cross-Border Payment Efficiency–a Legal and Regulatory Perspective–. https://www.bis.org/publ/work1015.pdf

Zhang, N. X. Y. (2021). Encryption to implement mechanism design solutions (Doctoral dissertation, Massachusetts Institute of Technology).

PUBLICATIONS

A Multi-Currency Exchange and Contracting Platform

Working Paper No. WP/2022/217