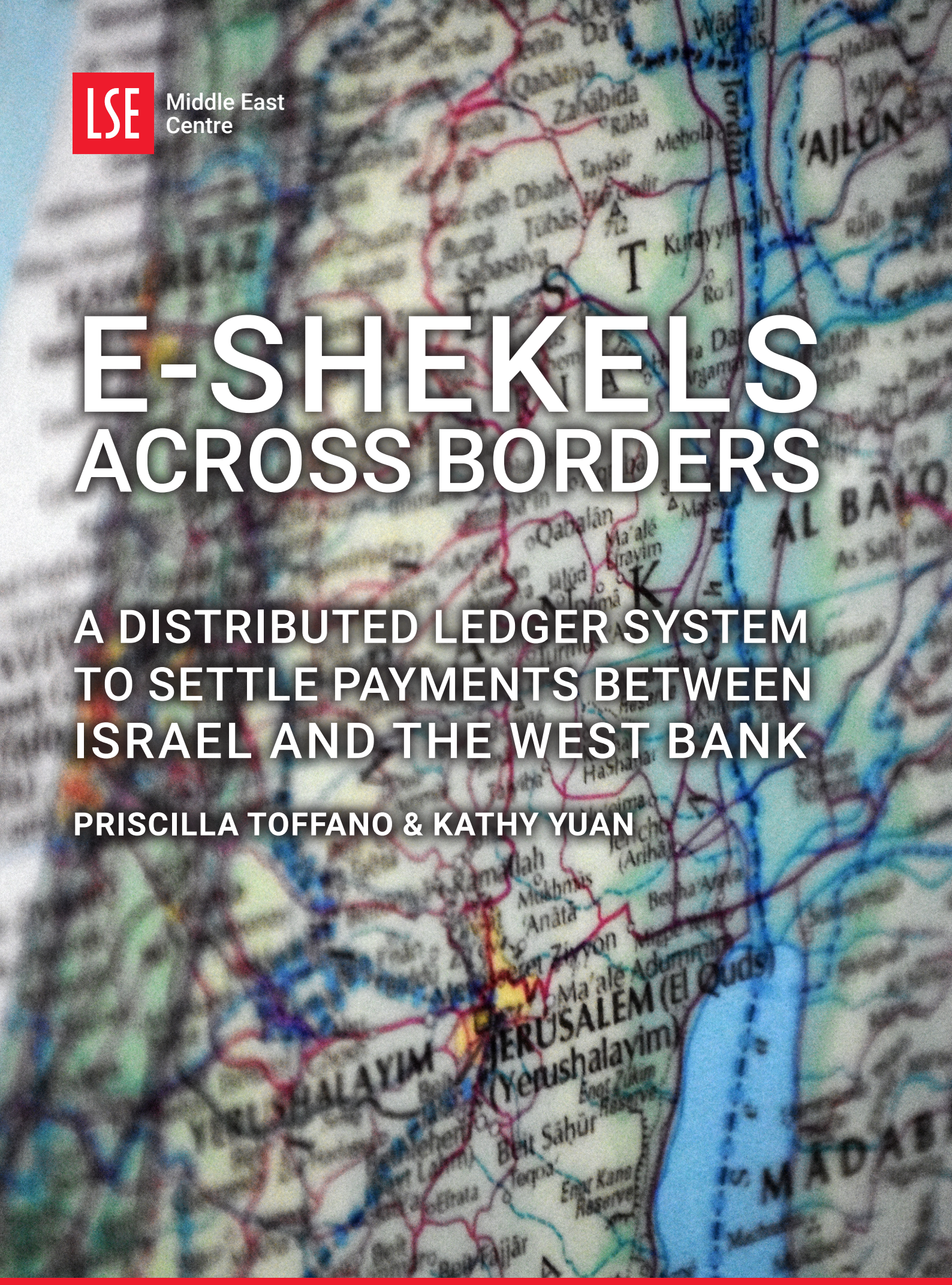


E-SHEKELS ACROSS BORDERS

A DISTRIBUTED LEDGER SYSTEM TO SETTLE PAYMENTS BETWEEN ISRAEL AND THE WEST BANK

PRISCILLA TOFFANO & KATHY YUAN

LSE Middle East Centre Paper Series | 28 | April 2019

About the Middle East Centre

The Middle East Centre builds on LSE's long engagement with the Middle East and provides a central hub for the wide range of research on the region carried out at LSE.

The Middle East Centre aims to enhance understanding and develop rigorous research on the societies, economies, polities and international relations of the region. The Centre promotes both specialised knowledge and public understanding of this crucial area and has outstanding strengths in interdisciplinary research and in regional expertise. As one of the world's leading social science institutions, LSE comprises departments covering all branches of the social sciences. The Middle East Centre harnesses this expertise to promote innovative research and training on the region.

Publications Editor
Jack McGinn

Cover Image
A map of Israel and the West Bank.

LSE Middle East Centre

E-Shekels Across Borders: A Distributed Ledger System to Settle Payments Between Israel and the West Bank

Priscilla Toffano & Kathy Yuan

LSE Middle East Centre Paper Series | 28
April 2019

About the Authors

Priscilla Toffano is an economist at the International Monetary Fund and Visiting Fellow at the LSE Middle East Centre.

Kathy Yuan is a Professor of Finance at the London School of Economics.

Abstract

Beginning in 2016, Israeli banks announced their intention to sever correspondent ties with their counterparts in the West Bank, citing risks around money laundering and terror financing. This paper contributes to the discussion about how to save Palestinian/Israeli transactions by proposing a private, permissioned distributed ledger system, jointly owned by the Palestinian and Israeli central banks, where Israeli and Palestinian banks can exchange e-shekels to settle payments.

1. Introduction

Transactions between Israelis and Palestinians are settled with correspondent banking. In 2016, Israeli banks announced their intention to sever correspondent ties with their counterparts in the West Bank, mainly because of risks around money laundering and terror financing. As the termination of correspondent services could have significant economic and security impacts, the Palestinian and Israeli authorities have since then been trying to find a long-term solution.

This paper contributes to the discussion on how to save Palestinian/Israeli transactions by proposing a new system that uses distributed ledger technology to process payments between Israel and the West Bank. In particular, we propose to set up a private permissioned distributed ledger jointly owned and supervised by the Bank of Israel and the Palestine Monetary Authority, where Israeli and Palestinian banks can exchange a digital representation of the shekel, the 'e-shekel'. A 'co-agency' would be established to hold collateral backing e-shekels in circulation and to settle transactions off the ledger when needed. We argue that transferring correspondent services from the bank to the ledger could improve the processing of cross-border transactions in terms of resiliency, efficiency, performance and auditability. This could then provide banks with new incentives to process cross-border transactions.

While proofs of concept testing the feasibility of a distributed platform to complete domestic interbank payments have already been presented, including by the Bank of Canada (Project Jasper) and the Monetary Authority of Singapore (Project Ubin), this is the first paper discussing the technical details of using a central bank-issued digital currency to guarantee the survival of cross-border payments when correspondent banking is failing, in the context of a real-life case.

2. The Problem

Israeli-Palestinian Economic Framework and Strains to Correspondent Services

The domestic and cross-border aspects of the Israeli and Palestinian economies are complex and overlapping. The Oslo II Accord[1] divides the West Bank into three administrative areas: Areas A and B, under different levels of Palestinian Authority (PA) jurisdiction; and Area C, over which Israel retains full control. This differs from the institutional structure of the financial system. The West Bank and Gaza (WBG) has an independent banking system (including Palestinian banks operating in Area C and Gaza) that is supervised by the Palestine Monetary Authority (PMA).

However, the WBG does not have its own currency and uses the new Israeli shekel (NIS), issued by the Bank of Israel (BoI), as its main currency.[2] The legal status of the NIS as a means of payment for all purposes, including official transactions, is specified in the 'Paris Protocol'.[3] The structure of the Palestinian economy – with 70 percent of Palestinian imports and 85 percent of exports to and from Israel, and 17 percent of the labour force in the West Bank working in Israel and the settlements[4] – defines the practical importance of the NIS in the daily lives of Palestinians and explains the high volume of NIS-denominated transactions each day within the same currency area, but between two different jurisdictions.

Non-cash payments between Israelis and Palestinians take place mainly through cheques and wire transfers. Table 1 shows the evolution of these payments in recent years. In 2016, cheques worth NIS 8.5 billion were issued by Palestinians for Israeli beneficiaries and cheques worth NIS 8 billion were issued by Israelis for Palestinian beneficiaries. Outward and inward money transfers[5] were valued at around NIS 9.8 billion and NIS 18.4 billion, respectively. Cumulatively, payments in 2016 amounted to NIS 44.7 billion, equivalent to 86 percent of WBG's GDP, and 3.6 percent of Israeli's GDP. For the WBG these volumes are in line with those typically passing through retail payment systems, often only about as high as the country's annual GDP

[1] The Oslo II Accord was signed on 28 September 1995 and envisioned the establishment of a Palestinian interim self-government in the Palestinian territories, but fell short of the promise of negotiating a comprehensive peace agreement and an independent Palestinian state after the interim period.
[2] Together with the Jordanian dinar and the US dollar.
[3] The Protocol on Economic Relations, also called the 'Paris Protocol' and incorporated in the Oslo II Accord, establishes the general framework governing Palestinian/Israeli economic relations. For the section establishing the NIS as the means of payments for all purposes, see Art IV.10.a.
[4] International Monetary Fund, 'West Bank and Gaza's IMF Report to the Ad-Hoc Liaison Committee', August 2016.
[5] Outward transfers are transfers issued by Palestinians to Israeli beneficiaries (e.g. payments of companies and government institutions settling their liabilities to Israel). Inward transfers are transfers issued by Israelis to Palestinian beneficiaries (e.g. remittances and clearance revenue collected by Israel on behalf of the PA).

Table 1: Non-Cash Payments between Palestinian and Israeli Counterparts

Items (in NIS billion)	2010	2011	2012	2013	2014	2015	2016
Cheques drawn on Palestinian banks	4	4	5.5	7.1	8.2	8	8.5
Cheques drawn on Israeli banks	3.6	5.6	4	4.7	6.6	7	8
Outward transfers	13	8	9	9	10	8	9.8
Inward transfers	11	10	13	13	14	14	18.4
TOTAL	31.6	27.6	31.5	33.8	38.8	37	44.7

Source: Palestine Monetary Authority

Article IV of the Paris Protocol specifies that NIS payments between Palestinian[6] and Israeli banks are to be settled via clearing houses connected to each other. Specifically, 'the clearing of money orders and transactions between banks operating in the WBG and banks operating in Israel will be done between the Israeli and Palestinian clearing houses on a same working day basis'. WBG and Israel each have four clearing houses,[7] though none are connected to each other due to different legal, business and technological systems. Israeli/Palestinian payments are thus treated as 'cross-border' and settled via correspondent banking.

The Bank for International Settlements defines correspondent banking as 'an arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks.'[8] Wire transfers, cheque clearing and cash management are examples of services correspondent banks can provide. In this respect, Article IV of the Paris Protocol specifies that the Israeli and Palestinian sides will allow correspondent relations between each other's banks.

Bank Hapoalim and Discount Bank in Israel have provided the WBG's Bank of Palestine with correspondent services related to the clearing of cross-border transactions and the management of NIS liquidity[9] for decades. But the situation changed in 2007 when

[6] The term 'Palestinian banks' refers here to all banks operating either in the West Bank or in Gaza, including those foreign-owned. From Section 3 onwards, the term will refer only to banks operating in the West Bank, including those foreign-owned. This is because the scope of this paper extends only to payments between Israel and the West Bank.

[7] The clearing houses are: (i) the Check Clearing Houses (settling paper-based payments, mainly cheques); (ii) the Automatic Clearing Houses (settling inter-bank movements not based on paper or cash, like salary payments and tax rebates); (iii) the Switch Clearing Houses (settling credit card payments); and (iv) the Real Time Gross Settlement Clearing Houses (settling transactions in real time, but without the possibility of cancellation).

[8] Committee on Payments and Market Infrastructures (CPMI), 'Correspondent Banking', Bank for International Settlements, July 2016.

[9] As with other economies with no currency of their own, NIS circulating in WBG originate from

Hamas, classified as a terrorist group in Israel and many other countries, took control of Gaza after winning the legislative elections. Soon after the Israeli Cabinet declared Gaza a hostile entity and in 2009 Israeli banks interrupted all correspondent services provided to banks in Gaza,[10] claiming that it was impossible to verify that the transactions were not benefitting Hamas. As the West Bank continued to be governed by the PA, Israeli correspondent banks continued to process transactions with banks operating in the West Bank while the BoI assumed the role of servicing NIS cash shipments from Palestinian banks, though with a monthly limit.[11]

However, in 2016 the Israeli correspondent banks started to threaten to interrupt correspondent relations with counterparts in the West Bank too.[12] These threats reflect a complex interplay of legal and economic, domestic and international factors, that should not be read in isolation but rather with consideration toward the development of correspondent banking at a global level.

Factors Affecting the Provision of Correspondent Services and Costs of Severing Correspondent Ties between Israel and the West Bank

Various reports since 2016[13] have analysed the causes of the scaling back of correspondent services, especially those provided to certain jurisdictions and customers considered unprofitable or risky. Two set of factors have been identified and discussed. The first set of factors is related to the change in the macroeconomic and regulatory landscape that emerged after the 2008 financial crisis. The more rigorous capital and liquidity requirements enforced to strengthen the resilience of the banking sector have increased the cost for banks to hold risk in their balance sheets, pushing some to sever correspondent services, in particular when they were not considered a core activity. Expansionary macroeconomic policies to boost growth have also made correspondent banking less profitable by compressing the margins and reducing the interest earned from respondent banks' balances.

---

cross-border flows. Once NIS banknotes are deposited in WBG banks, excess cash has to be transferred to Israel as needed to manage liquidity and conduct non-cash financial transactions.

[10] Even if the Palestinian financial system did not split up and banks in Gaza continued to be supervised by the PMA.

[11] The limit was, in large part, established because of Israeli concerns that a portion of cash deposits in the West Bank could not be explained by official transactions and could in fact be illicit. Moreover, as the amount of cash shipments increased over time, the processing capacity of the BoI's Cash Department also became a limiting factor.

[12] International Monetary Fund, 'West Bank and Gaza's IMF Report to the Ad-Hoc Liaison Committee', August 2016, April 2017, August 2017, March 2018, September 2018; Yehuda Sharoni and Maariv Hashavua, 'Hapoalim threatens to sever ties with Palestinian banks over legal fears', *Jerusalem Post*, 18 February 2016.

[13] Michaela Erbenova et al., 'The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action', IMF Staff Discussion Note, June 2016; Committee on Payments and Market Infrastructures, 'Correspondent Banking', Bank for International Settlements, July 2016; International Monetary Fund, 'Recent Trends in Correspondent Banking Relationships – Further Considerations', March 2017; Financial Stability Board, 'FSB Correspondent Banking Data Report – Update', March 2018; Financial Stability Board, 'FSB action plan to assess and address the decline in correspondent banking', March 2018.

The second set of factors is related to the increased costs of correspondent banking because of (i) the higher costs of regulatory compliance, particularly in relation to economic and trade sanctions, tax transparency initiatives and Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT) regulation; (ii) the high degree of uncertainty as to what exactly constitutes compliance, for example on the need to conduct due diligence on a customer's customer; and (iii) the increasing penalties levied against banks for regulatory breaches. For certain banks these costs have become so high that there is no business justification in continuing to provide correspondent services.

Many of these factors operate in the Israeli-Palestinian context too. The cost of monitoring and processing the high volume of transactions, often small in value, between the two areas has been mentioned as a specific factor contributing to the reluctance of Israeli banks to handle transactions with the West Bank. The perceived need to conduct due diligence on Palestinian customers, and the difficulty to do so given geographical and linguistic barriers, was also a concern for Israeli banks. Moreover, distrust of the quality of the AML/CFT regulatory regime in the WBG has been voiced on various occasions by the Israeli authorities.[14] Finally, difficulties in ascertaining whether the Israeli banking system is used to channel funds to terrorist entities could result in Israeli correspondent banks facing charges for violating anti-terrorism laws, with potentially high financial and reputational costs (see Section 5 for a deeper discussion). But while the Israeli banks' threats to not engage with the Palestinian system are understandable from a commercial point of view, the termination of correspondent services runs against the Paris Protocol and could have significant economic and security impacts for both Israel and the West Bank.

In terms of the potential loss of activity, large commercial transactions between Israel and the West Bank are most at risk. If the parties involved are unable to access alternative correspondent services via banks abroad, transactions may be cancelled, reducing the volume of trade. The lack of correspondent services would necessitate the use of cash for medium- and small-sized transactions, with a more prominent role for money changers. Were trade to be disrupted and become more informal, this could undermine efforts to broaden the tax base in the West Bank and negatively impact fiscal revenue. The problem of excess accumulation of liquidity[15] in Palestinian banks would worsen. More informality would also undermine the PMA's efforts to promote financial inclusion, reducing the proportion of the population using financial services. Taken to its extreme, the nature of financial and commercial transactions in the West Bank could degenerate to what has already occurred in Gaza, with no official means of payment other than cash, and vulnerable parts of the population finding it difficult to manage cash flows, build capital and savings, and mitigate economic shocks.[16] The combined effect could go so far as to paralyse the Palestinian banking system, which could then lead to the collapse of the PA itself.

[14] 'West Bank and Gaza's IMF Report to the Ad-Hoc Liaison Committee', International Monetary Fund, August 2016 and September 2018.

[15] The problem of the build-up of 'excess' NIS cash in Palestinian banks' vaults derives from increasing formal and informal flows of NIS cash entering the West Bank together with the limited cash services Israeli banks and the BoI offer to Palestinian banks to manage their liquidity. Excess NIS liquidity creates an opportunity cost and a security risk for Palestinian banks. See also footnote 11.

[16] Tracey Durner and Liat Shetret, 'Understanding Bank De-Risking and Its Effects on Financial Inclusion', Global Center on Cooperative Security Research Report, November 2015.

Since imports from and exports to WBG represent only 2 and 6 percent, respectively, of total Israeli imports and exports,[17] the economic cost of severing correspondent banking services would be much lower for Israel. This cost would mainly fall on Israeli trading companies, which absorb around half of the imports from WBG, and construction firms. The move to more informality could create added incentives to under-report VAT receipts, with the potential for fiscal losses. However, the cost to financial security would be much higher. Increasing the share of cash transactions would decrease the ability to monitor illegal activity, contrary to the objectives of the international AML/CFT framework. The economic and political strains upon the West Bank could also spill over into Israel with associated security risks.

Taking into consideration these potential costs, both the Palestinian and Israeli authorities have tried to prevent a collapse in correspondent banking relations. The Palestinian authorities have focused on strengthening their AML/CFT controls to adhere to international standards and respond to the concerns expressed by the Israeli correspondent banks. In 2015 they joined the regional Financial Action Task Force-style body (MENAFATF), adopted a new AML/CFT law and a decree to implement targeted financial sections. In 2016 they updated the law and instructions for reporting entities, requested the first assessment by MENAFATF and engaged international partners. In 2017 they started a National Risk Assessment with support from the World Bank and involved the IMF in a multi-year technical assistance project to help further strengthen WBG's CFT legal framework.[18]

The Israeli authorities focused on providing reassurance to the Israeli correspondent banks in the short term, while trying to study a mechanism to save cross-border transactions in the long term. In January 2017, the Israeli Security Cabinet's Ministers approved the recommendations of a team headed by the Finance Ministry Director and including representative of the Justice, Foreign and Defence Ministries, along with representatives of the intelligence community. The recommendations were for the Attorney General to provide Israeli banks with immunity in Israel concerning the correspondent services provided to Palestinian banks, and for the Treasury to provide the Israeli banks with full financial indemnity in case of AML/CFT-related lawsuits abroad.[19] This arrangement aimed at persuading the Israeli banks to maintain correspondent services with the Palestinians while a long-term solution was developed.

In October 2018 it was announced that the PMA and the BoI had reached an agreement on a new mechanism to facilitate transactions between Palestinian and Israeli banks. This would consist of setting up an Israeli government agency that could replace the

[17] International Monetary Fund, 'West Bank and Gaza's IMF Report to the Ad-Hoc Liaison Committee', August 2016.

[18] Box 3 in International Monetary Fund's 'West Bank and Gaza's IMF Report to the Ad-Hoc Liaison Committee', August 2017.

[19] International Monetary Fund, 'West Bank and Gaza's IMF Report to the Ad-Hoc Liaison Committee', April 2017; Barak Ravid, 'Amid Fears of PA collapse, Israeli Banks given Immunity for Deals with Palestinian Banks', *Haaretz*, 22 January 2017; Yaacov Benmeleh, 'Israeli Bank to Seek Extra Cover from Palestinian Ties', *Bloomberg*, 24 October 2017.

private Israeli correspondent banks in dealing with their Palestinian counterparts. While the details of the agreement and its prospective timetable have yet not been divulged, it may be assumed that the Israeli government agency will differ from the Israeli private correspondent bank mostly in its ownership structure. If this is the case, the discussion about the challenges in providing correspondent services to Palestinian counterparts would also apply for the proposed agency.

This paper aims to contribute to the discussion on how to save Israeli/Palestinian transactions by illustrating how distributed ledger technology (DLT) could be used to improve the efficiency and resiliency of the cross-border payment system and by proposing a role the government agency could play in it. In the remainder of the paper, Section 3 presents a new DLT-based system where a digital asset, the e-shekel, can be used to settle cross-border payments between Israel and the West Bank. Section 4 discusses the type of technological platform through which this payment system could be operated and mentions some early examples of distributed ledgers that have been used for interbank payments. Section 5 illustrates the pillars of the international AML/CFT order and reflects on how to maintain or improve compliance. Section 6 discusses the benefits that could be achieved by the new payment system, and concludes.

3. A Distributed Ledger Payment System for Israel and the West Bank

Distributed Ledger Technology for Cross-Border Payments

The fundamental challenge in exchanging a digital asset is that it is easy to counterfeit and replicate, so it can be claimed by more than one owner and spent more than once. Conventional payment systems handle counterfeiting and double-spend issues by verifying and clearing all digital transactions through a central authority with a global view of the transaction ledger and the power to block any transaction it deems invalid. These centralised payment systems must be trusted by their users and suffer from the problem of a so-called 'single point of failure'.[20] In 2008, a paper written by Satoshi Nakamoto[21] proposed a solution to this problem by showing how 'proof-of-work' could help achieve consensus among unknown and untrusting nodes in a network without the need to rely on a central authority.[22] This breakthrough opened the door to the possibility of using DLT to exchange digital assets peer-to-peer over distributed networks.

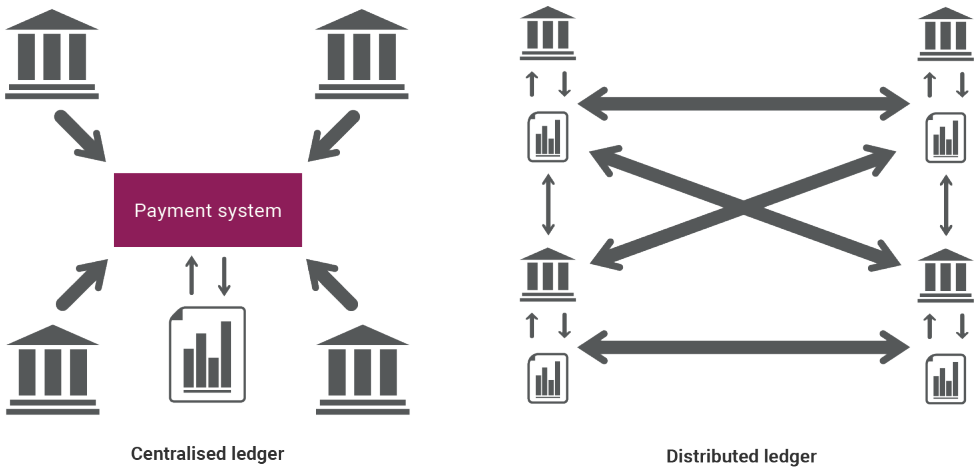
[20] A single point of failure is a critical system component that, if it fails, stops the entire system from working.

[21] Satoshi Nakamoto is the name used by the unknown person or people who authored 'Bitcoin: A peer-to-peer electronic cash system' in 2008.

[22] A consensus mechanism based on 'proof-of-work' requires the nodes proposing a change to the ledger to demonstrate that it was costly for them to issue the proposal in order to get it accepted by the other nodes as true. For more details about how this consensus works, see Robleh Ali, John Barrdear, Roger Clews and James Southgate, 'Innovations in payment technologies and the emergence of digital currencies', Bank of England's Quarterly Bulletin, 2014 Q3.

A distributed ledger (DL) is a database that is shared among the participants to a network (see Figure 1). Each participant is represented on the network by her computer, called a node. The database is updated after the nodes agree, through a consensus mechanism, on any new data entry to the ledger. While consensus mechanisms can be of various types,[23] they all allow the nodes to maintain a single, updated database where no two nodes have a conflicting view of the data. A DL also supports so-called 'smart contracts', which are digital contracts where lines of codes implementing human-readable legal prose can be automatically executed when certain predefined conditions are met.

Figure 1: Differences between a Centralised and a Distributed Ledger



Source: Santander InnoVentures (2015)

A transaction on a DL tells the network that the owner of some digital value has authorised the transfer of such value to someone else. In the absence of a central authority, the first thing the network needs to verify is that the node proposing the transaction actually owns the value it wants to transfer. Cryptography is important in this respect because it allows to create public/private keys that control access to digital assets. A private key is a random number that can be applied to the digital fingerprint of a transaction[24] to produce a signature. This signature is used to prove ownership of a digital asset and allows one the possibility to spend it. A public key is generated by applying a one-way cryptographic function to the private key and allows anyone with access to both it and the transaction fingerprint to verify the signature. So when spending a digital asset, the owner presents the public key and the signature and every node in the network can verify ownership.[25]

Transactions are similar to lines in a double-entry bookkeeping ledger where the digital value that the owner wants to spend enters as a debit against the receiver's account (forming an 'input' to the transaction) and as a credit against the sender's account (forming

[23] Besides proof-of-work, consensus mechanisms could be based on proof-of-stake, proof-of-elapsed-time, Practical Byzantine Fault Tolerance or Federate Byzantine Agreement, among others.
[24] The digital fingerprint of an input, such as a transaction, is the 'hash' of that transaction obtained by applying the hash algorithm to the input. Such an algorithm takes an arbitrary-length data input and produces a fixed-length deterministic result. For any specific input the resulting hash will always be the same.
[25] Andreas M. Antonopoulos, 'Mastering Bitcoin', O'Reilly Media Inc., 2017.

an 'output' of the transaction). The value sent to the receiver's address (the output of the transaction) is payable to whoever can present a signature from the key corresponding to the receiver's public address. This is normally the receiver herself, who holds her private/public keys in her digital wallet.[26] As every transaction's input references previous outputs, the transactions create a chain of ownership that tracks the source of the value exchanged on the DL from the moment it was first generated. Cryptography is also used to ensure the immutability of the chain by making it easy to spot if a previously validated transaction is deleted or modified.

The combination of these features is at the base of the potential to use DL for payments. In particular, the fact that data is distributed among the network's participants rather than stored in a central server eliminates the problem of a single point of failure and improves the network's resiliency. Once cryptography and consensus mechanisms are used to certify ownership of funds and solve the problem of double-spending, payments in digital assets can be very fast and do not need to rely on a central authority. As all participants see and use the same synchronised ledger, expenditures to reconcile records with other counterparties and legal disputes because of erroneous data entries are eliminated. Finally, the possibility for the nodes to monitor transactions in real time can minimise fraud while smart contracts reduce contract uncertainty and counterparty risk.[27]

DLT's potential benefits can be maximised in the area of cross-border payments. This is because, in the absence of a global payment infrastructure, cross-border payments must pass through a complex series of bilateral correspondent banking relationships that make them particularly slow, opaque and expensive. These bilateral relations require banks to hold idle liquidity and incur credit risk. Before they reach their destination, payments can be routed through many intermediaries, all relying on their own internal ledgers that need to be reconciled and can contain erroneous entries. This can escalate in costly disputes that require manual and personalised payment operations, adding to the costs. Moreover, the significant market power of correspondent banks allows them to extract revenue through direct fees and FX spreads.[28]

As a matter of fact, DLT is already used for peer-to-peer cross-border payments. This happens, for example, when users exchange fiat money into some privately issued digital currency[29] (e.g. Bitcoin, Litecoin, Dogecoin) held in digital wallets through the spokes (e.g. ATM machines, point of sale terminals, online interfaces), transfer the digital currency across borders over the hub (the virtual currency's secure network) to the payee's digital

[26] A digital wallet is an application that serves as the primary user interface and is typically a collection of addresses and the keys that unlock the funds within.

[27] David Mills et al., 'Distributed ledger technology in payments, clearing, and settlement', Finance and Economics Discussion Series 2016-095, Board of Governors of the Federal Reserve System, 2016; Committee on Payments and Market Infrastructures, 'Distributed ledger technology in payment, clearing and settlement: An analytical framework', February 2017.

[28] Dong He et al., 'Fintech and Financial Services: Initial Considerations', IMF Discussion Note 17/05, 2017.

[29] A privately issued digital currency is a form of digital money that is not issued by the central bank, but is privately created. It can be defined as a software enabling a public ledger of transactions, coupled with protocols and software that maintain security (see Susan Athey et al., 'Bitcoin Pricing, Adoption, and Usage: Theory and Evidence', SIEPR Working Paper No. 3469, 2016).

wallet and exchange it back into foreign fiat money through the spokes.[30] In this setting, intermediaries such as correspondent banks are no longer needed and payments can be faster and more transparent.

The volatility of the exchange rate for virtual to fiat currencies though has been a major hurdle for their use as mainstream means of payment. To obviate this problem, privately issued digital currencies pegged to a stable asset (e.g. Tether, BitUSD, Dai), also called 'stablecoins', have been designed and, while many of them have failed to keep the peg or faced accusations of not being able to provide audits for their collateral assets, it is too soon to judge their usefulness for cross-border payments.

Besides private stablecoins, recent work has focused on public stablecoins, issued by central banks either by pegging the price of an already existing cryptocurrency (e.g. Bitcoin pegged to the USD) or by flexibly supplying 'central bank-issued digital currencies' (e.g. Fedcoin and CAD-coin).[31] Research on the latter option has developed along two dimensions: studying the impact that digital currencies would have on monetary policy and financial stability[32] and analysing how central bank-issued digital currencies could serve as settlement assets for interbank payments.

Project Jasper[33] was the first to experiment with how a central bank and participating financial institutions would complete an interbank payment on a DL. The project offered insights on the functioning of a wholesale payment system using different DLT platforms and how modern payment system features could be incorporated in the DLT-based architecture.[34] Project Ubin[35] also aimed at testing the feasibility of using a central bank-issued digital currency for interbank payments and developed three different prototypes with specific Real Time Gross Settlement (RTGS) functionalities, each running on a different DL platform. Finally, the Bank of Canada, Bank of England and Monetary Authority of Singapore participated in a report exploring proposals for more efficient models for processing cross-border transactions, including via a central bank-issued digital currency.[36] Our proposal to settle transactions between Israelis and Palestinians extends the ideas of Projects Jasper and Ubin to a cross-border dimension.

---

[30] Dong He et al., 'Fintech and Financial Services: Initial Considerations', IMF Discussion Note 17/05, 2017.

[31] See Rod Garratt, 'CAD-Coin versus Fedcoin', R3 Report, April 2017.

[32] John Barrdear and Michael Kumhof,'The macroeconomics of central bank issued digital currencies', Bank of England working papers 605, 2016; Max Raskin and David Yermack, 'Digital Currencies, Decentralized Ledgers, and the Future of Central Banking'. NBER Working Papers 22238, 2016; Michael D. Bordo and Andrew T. Levin, 'Central Bank Digital Currency and the Future of Monetary Policy', NBER Working Papers 23711, 2017; Walter Engert and Ben Fung, 'Central Bank Digital Currency: Motivations and Implications', Bank of Canada Staff Discussion Paper 2017–16, 2017, among others.

[33] Payments Canada, Bank of Canada and R3, 'Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement', White Paper, 2017.

[34] James Chapman et al., 'Project Jasper: Are distributed wholesale payment systems feasible yet?', Bank of Canada, Financial System Review, June 2017.

[35] Deloitte and Monetary Authority of Singapore, 'Project Ubin: SGD on Distributed Ledger', Report, 2017; Associations of Banks in Singapore and Monetary Authority of Singapore, 'Project Ubin Phase 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies', Report, 2017.

[36] Bank of Canada, Bank of England and Monetary Authority of Singapore, 'Cross-border interbank payments and settlements', 2018.

Performance Criteria and Trade-offs in a DLT-based Payment System

Before presenting the technical details of the DLT-based payment system we propose, the basic performance criteria the system should comply with are the following:

- **No double spending:** the payment system should embed a consensus mechanism that ensures the impossibility of spending the same digital asset twice.
- **Stability:** each digital asset should be backed by a verifiable collateral.
- **Security:** the system should be safe from outsiders' hacking and insiders' collusion.
- **No single point of failure:** payments should continue to be processed even when participants to the system fail or withdraw.
- **Scalability and efficiency:** the system should be able to process the current-day average volumes of transactions within an acceptable time frame and costs.
- **Privacy:** the system should protect the privacy of users and of transactions' details.
- **Compliance with regulation:** the system should be in compliance with regulation, such as that on AML/CFT, corruption and tax evasion.

No DLT-based payment system can achieve all these criteria at once because trade-offs exist among some of them. The most important points of tension concern no single point of failure versus scalability and efficiency, and privacy versus compliance with regulation. An analysis of these trade-offs is useful in choosing, among the many available, the type of ledger and consensus protocol that is best suited to this specific case.

In an area characterised by instability and conflict, the possibility of processing transactions in a network potentially opened to everyone but without each having to know and trust the other, and without the need to rely on a central authority, is undeniably interesting. This possibility is offered by DLT-based payment systems that operate on *public, permissionless ledgers*[37] and implement proof-of-work consensus protocols. These decentralised payment systems are censorship-resistant,[38] continue to process transactions in close to real time even when multiple nodes fail or withdraw and offer full transparency of the transaction space. However, all these features come with a cost.

Finding consensus among nodes who do not know or trust each other is time and energy-consuming. This results in fewer payments processed in the same amount of time relative to the current infrastructure, and in the need for high storage space on every node for storing information, which is costly. Moreover, full visibility into the transactions' details, needed to avoid double spending, can improve the ledger's integrity and transparency but damage users' legitimate interests by revealing information on important parts of their business to their competitors. Finally, proof-of-work consensus protocols only deliver settlement finality in probabilistic terms, meaning that there is always a non-zero probability that a completed payment is subsequently reverted.

[37] A ledger is 'public' if everyone can read and initiate transactions and 'permissionless' if everyone can validate and maintain the ledger. The most famous example of a public, permissionless ledger is the bitcoin blockchain.

[38] This means that there is no party in the system that can prevent another making or receiving a payment.

Another important trade-off is related to anonymity versus compliance with regulation. The payment system's final users might prefer anonymity to protect privacy, avoid consumer profiling and defend against the stealing or hacking of their private information. This can be achieved with public, permissionless ledgers through pseudo-anonymity.[39] However, anonymity also carries with it a negative externality for society, because it can facilitate money laundering and the financing of terrorism, corruption and tax evasion, allowing a rise of illicit activities that puts the financial integrity of the economy at risk. Therefore, there is a tension between satisfying legitimate user preferences for privacy and mitigating risks to financial integrity.

To fulfil businesses' requirements such as the need to comply with regulation, transaction throughput, settlement speed and data privacy and confidentiality,[40] a number of firms and commercial banks including the R3 Consortium, the Hyperledger Initiative, J.P. Morgan, Ripple and Visa have built *private, permissioned platforms*.[41] These platforms can afford much cheaper and faster ways to achieve consensus because they are opened only to a pre-vetted group of known users that leverage their bilateral trust to process transactions. This means that transactions' parties are identified and transactions' data do not need to be distributed to the entire network, but also that integrity and transparency of the ledger are reduced, and that special nodes are needed to supervise the network and ensure that no double spending has occurred. These special nodes introduce a degree of censorship and potential single points of failure (Section 4 provides an account of some private permissioned platforms).

Table 2: Differences between Public Permissionless (PL) and Private Permissioned (PD) Ledgers

	Censorship resistance	Users' anonymity	Trust among users	Consensus mechanism	Diffusion of transactions' details	Single points of failure	Scalability	Settlement finality
PL	Yes	More	Not needed	Slow and expensive	Entire network	Less	Less	Probabilistic
PD	No	Less	Needed	Fast and cheap	Parties to the transactions + supervisors	More	More	Deterministic

[39] For example, the bitcoin ledger traces transactions to specific addresses and so does not provide full anonymity, but the addresses themselves are not associated with the real names of their owners, offering pseudo-anonymity.

[40] Privacy is the right to control the degree to which information are shared. Data confidentiality mechanisms ensure that individuals or organisations are prevented from accessing data that they are not authorised to access.

[41] A ledger is 'private' if only a selected group of users can read and initiate transactions, and 'permissioned' if only a trusted group of users validate and maintain its integrity.

A Private Permissioned Ledger for Payments in E-Shekels between Israel and the West Bank

We propose to solve the problem of correspondent relationships' failure between Israel and the West Bank by taking correspondent services to the ledger. If implemented in the appropriate way, this incremental change would eliminate the reliance on a single correspondent entity (Bank Hapoalim or the Israeli government agency in Israel and Bank of Palestine in the West Bank) and generate other key benefits (see Section 6) that could ensure the survival of cross-border transactions between Israelis and Palestinians.

The payment system we propose is similar to the interbank payment systems discussed in the proofs of concept coordinated by the Bank of Canada (Project Jasper) and by the Monetary Authority of Singapore (Project Ubin), but with two key differences. The first is that we suggest using DLT to assure the survival of cross-border payments, rather than to improve the efficiency of domestic interbank payments. The second is that our DLT-based payment system incorporates two, rather than one, central banks. This has two main consequences related to the collateral's verification and the settlement across different jurisdictions.

Our proposal involves the setting up of a private permissioned distributed ledger (DL) jointly owned by the BoI and the PMA[42] to process cross-border transactions between Israel and the West Bank. The BoI and PMA operate two supervisory nodes in the ledger. Participant nodes belong to some Israeli and Palestinian commercial banks that are pre-vetted for AML/CFT regulation and identified in the ledger.

The banks pledge shekel deposits for 'e-shekels' (a digital representation of the shekels) that can be exchanged over the platform according to the process detailed below. Every e-shekel is backed 1:1 by shekel deposits either in Israel or in the West Bank. This means that the use of e-shekels does not imply any increase in money circulating in the banking systems.

Optimal digital currency design depends on the circumstances of the economy and the preferences over anonymity and security in payments that range from cash-like (maximising anonymity) to deposit-like (maximising security)[43] digital currency. Given the significance of AML/CFT risk in our setup (see Section 5), we recommend an e-shekel with an anonymity not superior to that provided in existing deposit accounts.

In a domestic setting, the collateral is typically held in an omnibus account at the central bank (Project Jasper) or in an account at the commercial banks (Project Ubin). In both cases, the central bank verifies the validity of the collateral and issues the correspondent digital currency. When the digital currency needs to be redeemed, the DL platform connects to the domestic RTGS system where bank accounts are debited or credited in line with the transactions that took place on the DL.

[42] Joint ownership of the DLT platform, although not required to solve the issue at stake, could contribute to build trust between the Palestinian and the Israeli banking systems by reinforcing the cooperation between the central banks on governance frameworks, common standards and cybersecurity requirements, and the monitoring of cross-border transactions.

[43] Itai Agur, Anil Ari and Giovanni Dell'Ariccia, 'Central Bank Digital Currencies: Design Tradeoffs and Implications', forthcoming.

In our setting, two new problems arise. Firstly, it is cumbersome for the BoI to verify the validity of the collateral held at the PMA or at the Palestinian banks, and for the PMA to verify the collateral held at the BoI or at the Israeli banks. Secondly, it is possible that trading flows between Israel and the West Bank would have the effect of concentrating e-shekels in one area, while collateral is held in the other. In this case, settling payments off the DL may require transferring shekel deposits across borders. While verifying the collateral would still be difficult, the two central banks could solve the issue of trade imbalances with an agreement to transfer shekel deposits when necessary, similarly to the ad-hoc agreements between the PMA and BoI that have been used to manage NIS liquidity in the West Bank.

In this paper we propose another method for tackling the problems of collateral verification and trade imbalances at the same time. This involves the setting up of a jointly-owned specialised agency (a 'co-agency') where all banks participating in the DL hold a collateral account. The Israeli public agency recently proposed to deal with Palestinian banks could assume some of the functions of the co-agency. This co-agency would be formed of two parts: a Palestinian division that receives the Palestinian collateral and is continuously linked to the Palestinian domestic payment system; and an Israeli division that receives the Israeli collateral and is continuously linked to the Israeli domestic payment system. Both parties verify each other's collateral at the co-agency. After the collateral verification, the Palestinian and Israeli divisions request the respective central banks to issue e-shekels in line with the collateral provided by the banks and distribute it according to each bank's contribution.

Once the banks receive the e-shekels, they can exchange them over the distributed platform to clear[44] cross-border payments (see Figure 3). On the other hand, the settlement[45] of payments can be achieved on or off the ledger. If trade flows are more or less symmetric (of equal size in West Bank and Israel) or are low vis-à-vis domestic shekel deposits, e-shekels do not need to be reconverted into shekel deposits and can stay on the DL. In this case, settlement occurs in near-real time when consensus is reached among the nodes of the network and the common ledger is updated with the new ownership positions of the relevant counterparties. But if trade flows are high vis-à-vis domestic shekel deposits or are asymmetric (of unequal size in West Bank and Israel), and result in the concentration of e-shekels in one area (Israel or the West Bank), this area might need to retrieve the collateral that backs them. In this case, settlement occurs off the ledger when the Palestinian and Israeli divisions at the co-agency connect to each other to transfer the collateral, which is subsequently transferred to the domestic payment systems through the continuous link maintained by the respective divisions.

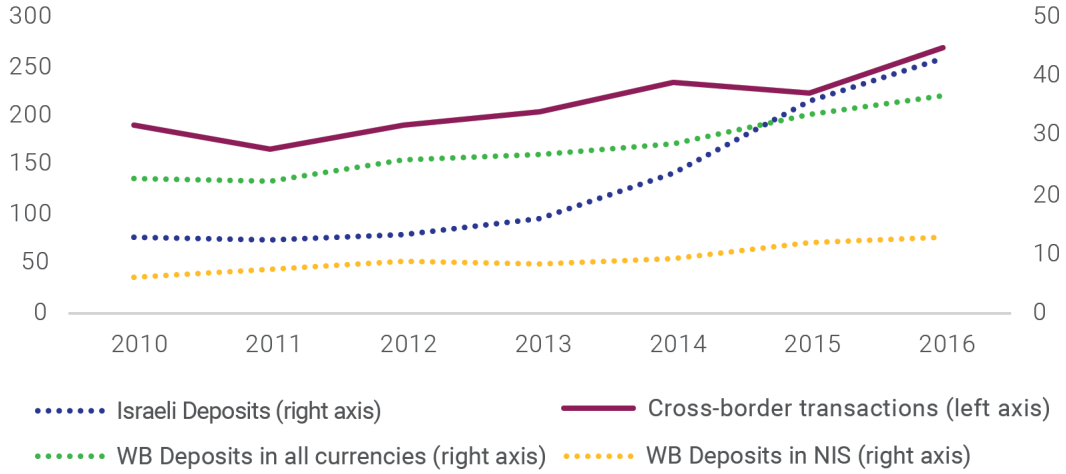
Between 2010 and 2016, gross cross-border transactions were on average NIS 35 billion per year, around 30 percent of the average annual Israeli demand deposits in the same

[44] Clearing is the process of determining who owes what to whom. In the case of correspondent banking, clearing includes banks sending messages to each other, typically through SWIFT, and the netting out of payments.

[45] Settlement is the actual exchange of funds between the parties to a transaction.

period, 125 percent of the West Bank's average annual deposits and 4 times the West Bank's average annual deposits in NIS (See Figure 2). Approximating the daily cross-border payments to NIS 135 million and considering their historical volatility, the daily amount of shekel deposits needed on the DL platform to back the e-shekels is around NIS 150 million.[46] Considering for simplicity that Israelis and Palestinians could each provide half of it, this amounts to around 7 percent of daily Israeli deposits in 2016 and more than half the daily deposits in all currencies raised in the West Bank in the same year.[47]

Figure 2: Gross Cross-Border Transactions; and Deposits (NIS billion)



Source: Palestine Monetary Authority and Bank of Israel

This is a considerable amount of deposits to pledge as collateral for cross-border transactions, in particular for the Palestinians, but it can be reduced given two facts. The first is that liquidity multipliers in an interbank network have been estimated to lie in the range between 0.8 (crisis times) and 5 (normal times), so even a relatively subdued value of 2 allows for halving the collateral required in the payment system.[48] The second is that, together with deposits, excess NIS liquidity in the Palestinian banking system[49] could also be used as collateral, which would incidentally reduce the costs incurred by Palestinian banks.

[46] To compute the daily average of collateral needed on the DL to back to e-shekels we divide the annual payments between Israelis and Palestinians by 260 (the working days in a year) to obtain the daily payments, take the average of the daily payments and add 2/3 of their volatility.

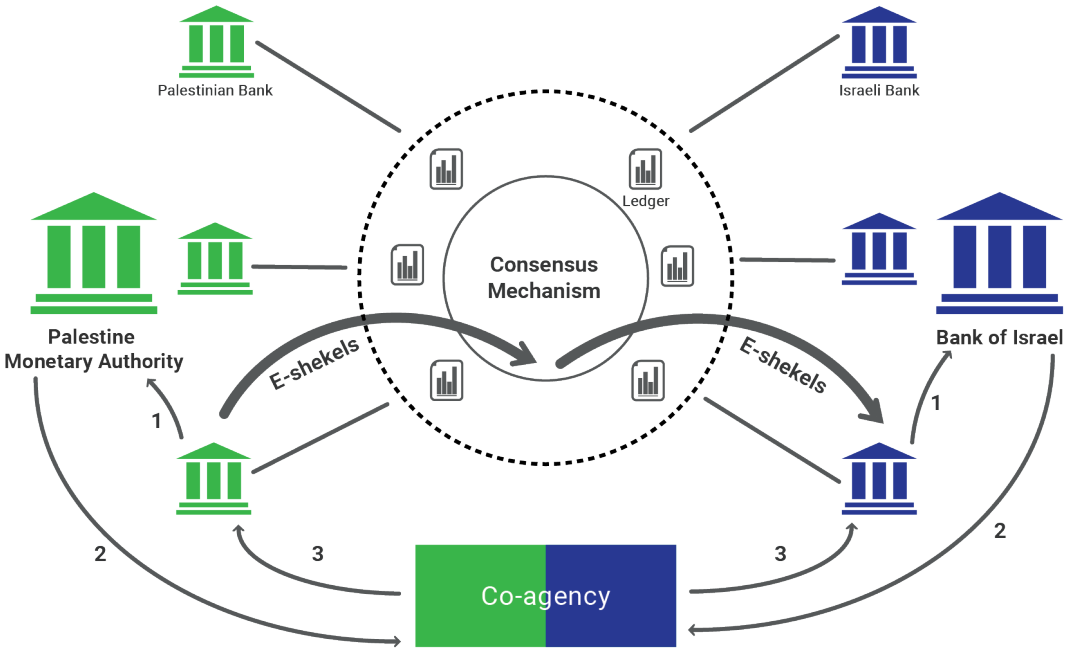
[47] Daily average deposits in Israel and the West Bank are computed by dividing the annual deposits by 260 and taking the average.

[48] Edward Denbee, Christian Julliard, Ye Li and Kathy Yuan, 'Networks Risks and Key Players: a Structural Analysis of Interbank Liquidity', FMG Discussion Papers dp734, 2017.

[49] See footnote 15.

Transactions in e-shekels are equivalent to transactions in central bank money and as such carry no credit risk. Similar to the Faster Payments scheme in the UK, our payment system is fully collateralised and every e-shekel in circulation is backed by a shekel held at the co-agency. This means that, even if the bank receiving the payment credited its customer's account before settlement had occurred and the sending bank went bankrupt in the meantime, the co-agency would still have the resources to settle the payment.

Figure 3: DLT-Based Payment System for Cross-Border Transactions



Note that e-shekels can travel in either direction.

Notes- 1: Bank instructs central bank to transfer NIS balance from its current account into a collateral account at the co-agency. **2:** Central bank sends NIS balance to co-agency as collateral for e-shekels. **3:** Co-agency sends an equivalent balance of e-shekels to the bank's digital wallet.

However, this payment system remains subject to geopolitical and liquidity risks. The first of these occurs if e-shekels' redemption cannot be honoured because of a conflict between the two parties that breaks down the link between the Palestinian and the Israeli divisions at the co-agency. The second occurs if a bank is not able to meet its payment obligations as they arise because incoming payments are not sufficient to support outgoing payments. This could cause a 'gridlock' in the system where no bank is willing or able to be the first to send funds to another and the payments' flow is interrupted.

Given the absence of credit risk but the presence of liquidity risk, a deferred net settlement (DNS) model could be used for settling cross-border payments off the ledger. Under DNS, payment instructions are accumulated over time and settled on a net basis after a certain period, which allows participants to economise on the liquidity required to complete settlement. In relation to the specific liquidity needs of the platform, mechanisms to coordinate incoming and outgoing payments could also be introduced. Project Jasper and

Project Ubin show that liquidity saving mechanisms used in centralised payment systems can work in decentralised settings as well, even if they introduce a single point of failure.[50]

To encourage banks to participate in the payment system and increase the networks' liquidity, several incentive schemes and protocols can be implemented. Throughput guidelines and time-varying tariffs are examples aimed at increasing money's velocity by incentivising timely payment processing or by punishing delayers. Ripple's pathfinding algorithm[51] can also be introduced as a supplementary alternative to the default direct bilateral transaction algorithm embedded in our proposal. This algorithm prescribes that every node maintains a limited order book for receiving and sending requests with relative fees so that the cheaper trades can be executed. Finally, the system could reward banks' liquidity provision. This can be measured in terms of speed of transaction processing, cost of sending and/or receiving payments or total amount of transactions validated and/or intermediated.

An important part of the payment infrastructure is how nodes decide that an Israeli/Palestinian transaction is legitimate. On one hand, DLT allows every node to see and record all transactions taking place in the network and participate to the consensus mechanism. This transparency increases the resilience of the network because all transactions' data are gathered on all nodes, and improves trust and auditability in the system, since each node sees every transaction and contributes to its validation. Besides methods based on proof-of-work, RSCoin[52] illustrates an example of this type of transparent consensus mechanism. On the other hand, banks prefer to not disclose data on the transactions they process because this could reveal their business models and liquidity positions, to the benefit of competitors. Transparency has then to be balanced with privacy concerns (see the above discussion on trade-offs).

Section 5 provides an account of existing distributed platforms supporting consensus mechanisms aiming at taking into consideration the banks' need for privacy and confidentiality. They are all based on differentiating the roles of the nodes in the network such that nodes involved in a transaction are the only ones that see and agree upon that transaction's details; while special trusted nodes are responsible for confirming that no double spending of the digital asset has occurred in that transaction, and are the only ones to maintain a global transactions' ledger. In our setting, the PMA and BoI, playing a fundamental supervisory role in their respective financial systems and enjoying good bilateral relations, would be the special nodes that are trusted by the others in the system.

Ultimately, the choice on the consensus mechanism depends on the mix of transparency and privacy that the Israeli and Palestinian banks would find more useful. Different types of consensus mechanisms, in relation to the different levels of privacy and transparency needed in the relationships between banks in the network, can be supported by the DL.

[50] Appendix 2 in Payments Canada, Bank of Canada and R3, 'Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement', White Paper, 2017; Associations of Banks in Singapore and Monetary Authority of Singapore, 'Project Ubin Phase 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies', Report, 2017.
[51] Ripple's pathfinding algorithm allows a transfer to find a cheaper (although possibly not the cheapest) path from the sender to the receiver (see Ripple's whitepaper, 2017).
[52] George Danezis and Sarah Meiklejohn, 'Centrally Banked Cryptocurrencies', UCL working paper, 2015.

Step by step

More specifically, a payment between a Palestinian importer and an Israeli exporter on the DLT-based payment system we propose would work as follows:

In Step 1 (**pledging of central bank money versus e-shekel**), the Israeli banks pledge shekel deposits by instructing the BoI to transfer a balance from their current accounts into a collateral account at the co-agency (Israeli division). In exchange, an equivalent balance of e-shekels is created on the co-agency node's DL account and sent to the digital wallet of the individual Israeli banks. Similarly, Palestinian banks pledge shekel deposits with the PMA, which are sent to the co-agency (Palestinian division). In exchange the Palestinian banks receive e-shekels. As the collateral is held at the co-agency, it can be verified by both Israeli and Palestinian parties.

Table 3: Pledging of Israeli (A and B) and Palestinian (C and D) Banks

	Before		Shekel-deposits pledged for e-shekels		Distribution of e-shekels to banks' wallets	
	Domestic Payment Systems	Distributed Ledger	Domestic Payment Systems	Distributed Ledger	Domestic Payment Systems	Distributed Ledger
Bank A	100	0	90	0	90	10
Bank B	100	0	80	0	80	20
Bank C	100	0	70	0	70	30
Bank D	100	0	60	0	60	40
Co-agency	0 0	0 0	30 70	30 70	30 70	0 0

In Step 2 (**payment request from a Palestinian importer to pay an Israeli exporter**), the Palestinian importer instructs her Palestinian Bank D to make a payment to the Israeli Bank A of the Israeli's exporter in order to pay for her imports. The Palestinian bank creates a payment request on the distributed ledger specifying the transaction details and sends it to the Israeli bank.

In Step 3 (**consensus mechanism**), the payment request is validated through the consensus protocol by a group of Israeli and Palestinian banks (see above and Section 5 for a discussion on possible consensus methods). This includes verifying that the Palestinian node is authorised to operate on the ledger and has enough e-shekels in its account to proceed with the payment.

After consensus is reached, in **Step 4** (**payment clearing**) the Palestinian Bank D exchanges e-shekels with the Israeli bank A on the DL via their wallets (see Table 4, with payments highlighted).

Table 4: Payment in E-Shekels from Bank D to Bank A

	Before				Bank D makes a payment to Bank A			
	Domestic Payment Systems		Distributed Ledger		Domestic Payment Systems		Distributed Ledger	
Bank A	90		10		90		20	
Bank B	80		20		80		20	
Bank C	70		30		70		30	
Bank D	60		40		60		30	
Co-agency	30	70	0	0	30	70	0	0

In **Step 5 (payment settlement on or off the ledger, and e-shekels' redemption)**, the payment can be settled on the DL platform if e-shekels stay on the platform and do not need to be reconverted into shekel deposits. This can happen if trade flows are more or less symmetric or small vis-à-vis domestic shekel deposits. In this context, the DL provides a clearing and settlement platform operating in near-real time.

In the most general case, the payment is settled off the distributed ledger when the co-agency's divisions link to each other for the collateral's transfer and, subsequently, send an instruction file to their domestic payment systems so that Palestinian Bank D's account is debited while Israeli Bank A's account is credited. Table 5 illustrates the settlement off the ledger (e-shekels' redemption). The frequency of the settlement mainly depends on the building-up of trade imbalances and the authorities' preferences.

Table 5: Settlement Off the Ledger (E-Shekels' Redemption)

	Before				E-shekels are returned to the Co-agency's node				Co-agency credits/ debits banks' accounts + returns collateral			
	Domestic Payment Systems		Distributed Ledger		Domestic Payment Systems		Distributed Ledger		Domestic Payment Systems		Distributed Ledger	
Bank A	90		20		90		0		110		0	
Bank B	80		20		80		0		100		0	
Bank C	70		30		70		0		100		0	
Bank D	60		30		60		0		90		0	
Co-agency	30	70	0	0	30	70	40	60	0	0	0	0

4. Technological Platforms

As discussed earlier, permissioned distributed ledgers have been designed to address the financial industry's needs in terms of privacy, confidentiality, identification of transactions' parties and scale (see Table 2). Corda, Hyperledger Fabric and Quorum are examples of permissioned DLT platforms that, while still in a development phase, have been tested by financial institutions to make interbank payments in Project Jasper and Project Ubin. All three provide a way to process transactions among a group of entities that are identified and vetted and, by relying on the known identities of the participants, can use less expensive consensus protocols that do not require proof-of-work. These platforms promise to achieve confidentiality via encrypting business data and zero knowledge proofs, and privacy by making transactions visible only to the parties involved. Since it is difficult to assess if these claims are accurate and if these platforms are ready to be used in reality, this section serves only to demonstrate that similar platforms can potentially be used in the Palestinian/Israeli case. It also provides a high-level description of how Corda, Hyperledger Fabric and Quorum work as discussed in the related white papers and in Project Ubin, but does not endorse the use of any before further independent analysis is carried out.

Corda

Corda is an open source permissioned distributed ledger developed by the R3 consortium to record, manage and synchronise individual agreements between financial institutions.[53] The foundational object in Corda is the 'state object', which is a digital document recording the existence, content and current state of an agreement between Corda parties. States can represent facts of any kind, for example identity information, KYC data, loans and IOUs. As well as any information about the fact itself, the state also contains a reference to the smart contract that governs its evolution. The ledger evolves over time through transactions that will consume states as inputs and produce new states as outputs (UTXO model).

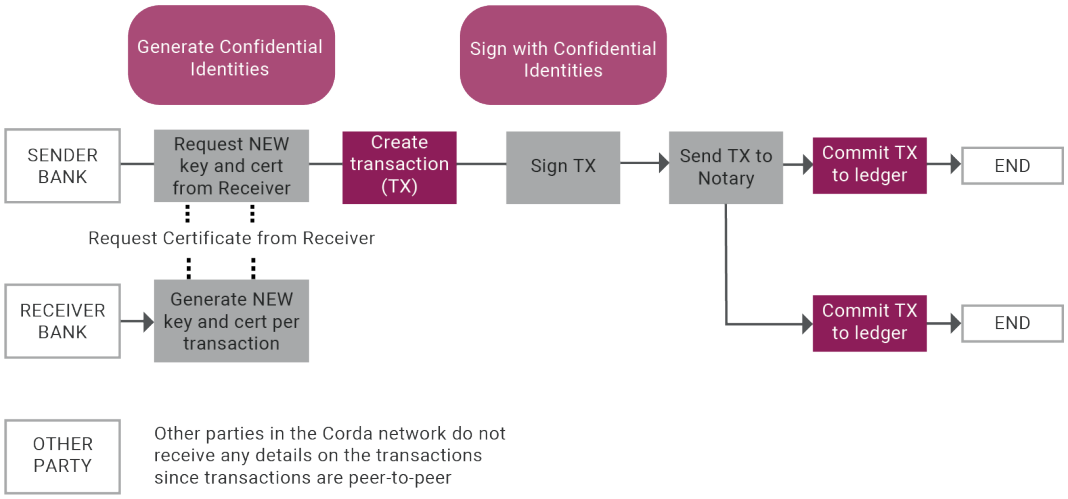
A Corda network is an authenticated peer-to-peer network of nodes, where each node hosts Corda services and executes applications known as CordApps that should enable parties to coordinate actions without a central controller. A network map service publishes the public keys and corresponding IP addresses to identify and contact any node. To protect participating nodes' privacy, a transaction in Corda aims at being processed, validated and recorded only by the parties involved in it. This means that the global transactions ledger should not be shared among all nodes, but each node should maintain a separate database storing the fraction of the ledger that corresponds to the set of transactions in which it has participated. As nodes should not be able to see all transactions that take place in the network, they would need to trust a notary service to guarantee the uniqueness of the states that are being spent in a transaction.

[53] Richard Brown et al., 'Corda: An Introduction', August 2016; Mike Hearn, 'Corda: A distributed ledger', November 2016; Richard Brown, 'The Corda Platform: An Introduction', May 2018.

A transaction where a sender bank's node intends to spend consumable states by transferring it to a receiver bank's node involves the following steps (See Figure 4):

- Sender and receiver swap and verify new confidential identities to sign the transaction. This aims at ensuring that even if a third party gets access to an unencrypted transaction, they cannot identify the participants without additional information.
- The sender creates a new transaction proposal that references the input states, and signs it.
- The notary verifies the uniqueness of the states that the sender wants to spend by checking that it has not already signed other transactions that consume any of the proposed input states. If no double spending has occurred, the notary signs.
- Sender and receiver check that the proposed transaction is valid by verifying that the associated contract code runs successfully and has the required signatures; and that any transactions to which this transaction refers are also valid. If this is the case, they sign.
- If the transaction has achieved both uniqueness and validity consensus, the sender and the receiver commit it to the respective ledgers.

Figure 4: Transaction Flow of Fund Transfers with Corda



Source: Project Ubin Phase 2

Hyperledger Fabric

Hyperledger Fabric is an open source permissioned distributed platform developed by IBM in the framework of the Linux Foundation's Hyperledger Initiative.[54] The Fabric platform is underpinned by a modular architecture that aims at allowing for plug-and-play components to meet the requirements of different industry-use cases. Examples of pluggable components are a membership service provider responsible for associating entities in the network with cryptographic identities, an ordering service establishing consensus on the order of transactions and broadcasting blocks to the network's nodes, and consensus protocols.

The nodes in the Fabric network are called peers and are of different types. Endorsing peers have the task of validating transactions against the endorsement policy defined by Chaincode, a program that implements the logic agreed by the network's members. Orderer peers receive endorsed transactions from every channel in the network, order them chronologically by channel, create blocks of transactions per channel and deliver it to all peers. They are the central communication channel and are responsible for the consistent state of the ledger across the network. Anchor peers do not validate transactions but receive transactions' updates and broadcast them to the other peers.

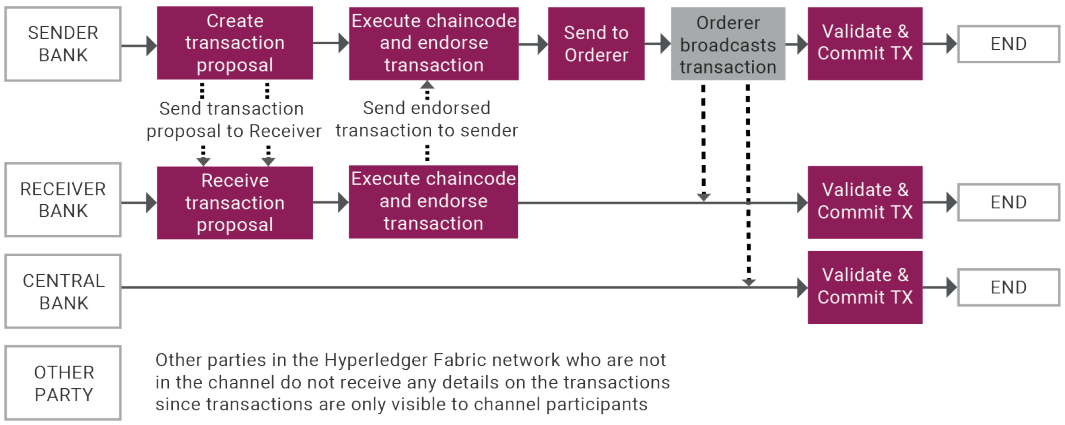
The distinctive feature of the Fabric platform is that it should allow nodes to create bilateral channels for private transactions. Only the participants to the channel validate the transactions and commit them to the ledger, which should allow isolation of confidential data. Besides bilateral channels, peers participate in two multilateral channels important for traceability of transactions and gridlock resolution.

A transaction between a sender bank's node and a receiver bank's node is executed in their bilateral channel as follows (See Figure 5):

- The sender sends a transaction request to the receiver via the Client application.
- The endorsement policy specifies which peers need to vouch for the correct execution of the transaction. If these are, for example, the sender and receiver, they verify that the transaction proposal is well formed, it has not been submitted already, the signature is valid and the sender is authorised to propose the transaction. Chaincode is then executed against the current state database to produce transaction results.
- If the transaction is approved, it is sent to the Orderer peer that includes it in a block and forwards it to the Anchor peers.
- Anchor peers broadcast the block to the other peers in the network, which update their local ledger with the latest block.

[54] Kelly Olson et al., 'Sawtooth: An Introduction', 2018.

Figure 5: Transaction Flow of Fund Transfers with Hyperledger Fabric



Source: Project Ubin Phase 2

Quorum

Quorum is a permissioned distributed ledger protocol that was developed by J.P. Morgan to provide the Financial Services industry with an implementation of Ethereum[55] that supports transactions and contract privacy.[56]

In the Quorum network there is no function-specific node that requires a different configuration and all nodes operate the same set of components: a Quorum node, a Constellation node and Quorum Decentralised Apps. The Quorum node is very similar to an Ethereum node in order to take advantage of the developments in the Ethereum community. The Constellation node consists of two components: the Transaction Manager, responsible for storing, granting access and exchanging encrypted transaction data, and the Enclave, responsible for storing private keys and encrypting/decrypting data. The Quorum Decentralised Apps are computer applications that orchestrate various payment execution functions.

To satisfy financial institutions' need for privacy, Quorum developers have extended the Ethereum transaction model to accommodate for private transactions whose payloads should be visible only to the parties involved in the transactions. While public transactions are executed by all nodes in the network, before broadcasting a private transaction the sender's Quorum node replaces the original payload with a hash (the data's digital fingerprint) of the encrypted payload. Using Constellation, parties to the transaction will be able to replace the hash with the actual payload and execute the contract code, while the others will only see the hash and will not execute the code. While this approach should preserve the privacy of the parties in the private transaction, it does not support prevention

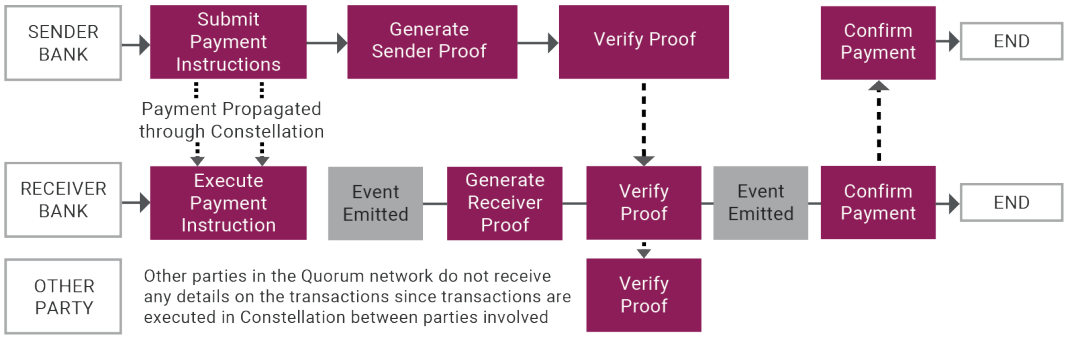
[55] Ethereum is an open-source, public, permissionless distributed platform that supports smart contract.
[56] Quorum whitepaper, 2016.

of double-spending for the digital assets exchanged. To prevent double-spending, J.P. Morgan and Zcash partnered to create a Zero Knowledge Security Layer (ZLS). This is a protocol aimed at enabling balance validation without revealing any information about the sender, the receiver or the quantity of assets transferred.[57]

A transaction in Quorum works as follows:

- The sender bank's Decentralised App invokes a private smart contract to generate a private transaction between the two parties, and a public smart contract to execute a public transaction in all nodes of the network.
- Both sender and receiver banks generate proofs to show that no unauthorised funds have been introduced or taken out of the network. Verification of proofs are public and performed by all nodes via ZLS.
- If all conditions are met, the receiver's Decentralised App executes the contract code to move the amount from the sender in a single atomic transaction.

Figure 6: Transaction Flow of Fund Transfers with Quorum



Source: Project Ubin Phase 2

Project Ubin's Phase 2 described and compared three distributed ledger prototypes using Corda, Fabric and Quorum. It discussed the aim of all three platforms to ensure privacy by distributing information on a need-to-know basis. It also described the sharding (partitioning) of data in Corda and Fabric as a way to provide good scalability and performance, even if noticed that complexity increases with the number of channels in Fabric. According to Project Ubin, resiliency seems better in Quorum where the network can still function normally if any node fails, while the Notary and the Orderer nodes introduce a single point of failure in Corda and Fabric. A way to overcome this could be through introducing multiple Notary and Orderer nodes. Settlement finality seems good across all platforms, even if the execution time taken for ZKP generation in Quorum poses a concern as participating nodes may drop off during the gridlock resolution cycle, thus invalidating the entire settlement. This is supposed to improve with better ZKP algorithms.

[57] For an explanation of ZLS see: https://github.com/jpmorganchase/quorum/wiki/ZSL

While all these platforms could potentially be used to process cross-border transactions in the payment mechanism we propose, they are still in a development phase and it is difficult to assess when they will be suited for application in real cases. Moreover, the mix of resiliency of the ledger, scalability, efficiency and privacy needed in the Palestinian/Israeli case could require the development of another technological platform specifically targeted at this case.

5. Anti-Money Laundering and Counter-Financing of Terrorism Regulation

The international approach to AML/CFT regulation is shaped by the Financial Action Task Force (FATF), an intergovernmental body that sets global standards to combat money laundering and terrorist financing. The pillars of the FATF order are the 2012 Recommendations, centred on the ideas of risk-based approach and customer due diligence (CDD).[58] A risk-based approach to AML/CFT means that financial institutions are expected to identify, assess, understand and report the ML/FT risks to which they are exposed and take measures commensurate to those risks in order to mitigate them. In this context, financial institutions are required to conduct ongoing due diligence on their customers, by verifying their identities, understanding their activities, identifying beneficial owners[59] and evaluating the associated risk. At a minimum, due diligence should run some basic checks such as verifying that customers are real people, screening them against watchlists and evaluating the involvement of politically exposed persons (PEP).[60] But if higher risks are identified, enhanced due diligence (EDD) calls for additional investigations that can end up in the freezing of transactions and assets.

Correspondent banks are also expected to conduct due diligence on their customers, that is, on the respondent banks.[61] This includes gathering sufficient information on the nature of the respondents' business, their reputation and the quality of the supervision in the jurisdiction in which they operate. It also entails the monitoring of the respondents' transactions with a view to detecting any unusual activity, change in risk profile or deviation from the correspondent arrangement. Where needed, correspondent banks follow up with respondents by requesting more information on specific transactions or customers. This process of information sharing is cumbersome for both respondent and correspondent banks. The former need to share information bilaterally and on an ongoing basis, packaged in the specific way requested by each correspondent. The latter need to process, often manually, such information.

[58] Recommendations 1 and 10 in Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation', 2012.

[59] According to FATF, beneficial owner refers to the natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

[60] Recommendation 12.

[61] Recommendation 13.

Among the key services provided by correspondent banks there is the processing and execution of transactions for their respondents' customers, often located in another jurisdiction. With respect to these indirect customers, correspondent banks have been uncertain if there exists an obligation to conduct due diligence in the same way they do for their direct customers (a practice known as 'know your customer's customer' or KYCC), or not. As this uncertainty has been recognised as among the main reasons leading banks to decline to provide financial services to certain customers and jurisdictions, both FATF[62] and other national regulators[63] have clarified that banks are not expected to conduct, as a matter of course, due diligence on the respondents' customers.

But despite these reassurances, KYCC remains an important concern for Israeli banks in dealing with Palestinian indirect customers with whom they are not in contact. This is because even after receiving additional information on specific transactions or customers from the respondent banks, it may still be difficult to obtain reasonable assurances about their legitimacy. In this respect, the Israeli National Risk Assessment[64] identifies the risk that the Israeli banking system will be exploited to transfer money to terrorist elements, especially as entities in Gaza may use financial services companies' shadow accounts at banks in the West Bank for this purpose.

The difficulty in tracing the identity of the initiators and the final beneficiaries of the transfer is also daunting for Israeli and Palestinian banks because they can be exposed to anti-terror lawsuits, particularly in the US where citizens can pursue claims related to international terrorism. For example, Arab Bank, Hapoalim and Discount Bank were involved for more than thirteen years in a lawsuit where hundreds of American citizens accused the banks of having facilitated terrorist attacks in Israel and having conducted transactions that ultimately benefitted Hamas.[65] Whatever the final result, being the defendant in such an investigation is very expensive and reputationally damaging.

Since a DLT-based payment system delivers the possibility of monitoring transactions in real time and recording the transaction history in an immutable way, the contribution that our proposal makes for AML/CFT compliance is related to the improvement of supervision and auditing practices. First, supervisory nodes having full visibility on all cross-border transactions would be able to share information with the banks on suspicious transactions taking place in the ledger in real time. This constitutes an improvement with respect to current practices where problems can be identified only long after transactions have taken place.

Moreover, auditors could directly access the ledger to verify the entire population of transactions on a continuous basis, rather than verifying only a sample of transactions by

[62] Financial Action Task Force, 'FATF Guidance –Correspondent Banking Services', October 2016.
[63] US Department of the Treasury and Federal Banking Agencies, 'Joint Fact Sheet on Foreign Correspondent Banking', August 2016.
[64] Israel Money Laundering and Terror Financing Prohibition Authority, 'Non-classified Version: National Risk Assessment on Terror Financing', 2017.
[65] Marc Perelman, 'Two Israeli Banks Accused of Sending Millions of Dollars to Hamas Entities', *Forward News*, 12 December 2007.

asking clients or third parties to provide information. Such extensive auditing coverage can serve to increase trust in the payment system. As transactions recorded in a distributed ledger cannot be erased or be tampered with, the cost of prevention and detection of fraud can also be reduced.

The rest of the AML/CFT processes remains unchanged. To be admitted to the distributed ledger platform we propose, banks would still need to implement rigorous AML/CFT controls both on their customers and on their counterparts. Transactions in e-shekels remain compliant with FATF Recommendation 16 on wire transfers, by incorporating information on originator and beneficiary of the payment, and the exchange of high-quality information between Israeli and Palestinian banks remains crucial to produce that confidence that ultimately enables cross-border transactions.

To decrease the cost of due diligence and KYCC processes, financial institutions, standard setters, tech-firms and regulators around the world are developing new methodologies. The most important are related to Know Your Customer (KYC) utilities, Legal Identity Identifier (LEI) codes, emerging technologies and user-centric ID systems.

- KYC utilities are centralised databases storing CDD information.[66] Respondent banks access such a utility to provide the initial information on their customers' identities, business and transactions, and update it in line with a standardised template. They retain full control on their data and decide which banks have access to it. Correspondent banks can retrieve information as needed. This approach allows one (i) to eliminate the duplication of respondent banks' reporting and produce better data as banks need to maintain only one set information, (ii) to maintain a more comprehensive customer's profile as transactions related to a single customer reported by several respondents could be aggregated, and (iii) to more easily identify systemic trends by aggregating information across customers, products and regions.
- The LEI is a 20-digit alphanumeric reference code uniquely associated with legal entities' data, such as their official name, their address, their headquarters' or fund manager's address and their country of legal formation. The LEI can be used to facilitate AML/CFT screening by unambiguously identifying legal entities engaging in financial transactions. While this is not particularly useful as a tool for identifying banks, as they usually already know each other, it could be used to identify banks' customers [67] and consolidate information by identifying transactions of the same entity reported by different financial institutions. By eliminating the ambiguity that is sometimes associated with names, LEI's use within payment messages could also be a way to support the implementation of Recommendation 16 on information to be included in wire transfers.
- Emerging technologies can be applied to areas such as due diligence and transactions monitoring. For example, video KYC can be used to authenticate the customers' identity when customers do not have access to branches. Natural Programming

[66] Examples of KYC utilities are Bankers Almanac, Depository Trust & Clearing Corporation (DTCC)'s Clarient Entity Hub, KYC.com (Markit/Genpact), SWIFT KYC Registry, Thomson Reuters Accelus.
[67] This is more challenging though because LEI exists only for legal entities and not for individuals.

> Language technology enables firms operating in multiple jurisdictions to better process complex names with different spellings in different languages. In this way, checking customers' names against agreed watchlists is easier and adverse media searches can be automated. Within KYC utilities, data analytics and machine learning could improve identifying trends and suspicious individuals by developing a more complete transactional profile of customers and could contribute to automating suspicious activity reports. Decision-tree based systems with rules to identify transaction outliers and trigger alerts are important for transaction monitoring.[68]

There are two main obstacles to the adoption of KYC utilities or any other information sharing mechanism:

- The first is that the ultimate legal responsibility on performing CDD on the respondent banks currently lies solely with correspondent banks so, unless the information-sharing mechanism envisaged decreases the number of CDD checks they have to perform, banks might still need to invest the same amount of resources in due diligence. This would decrease the appetite to invest additional resources in information-sharing mechanisms or other technologies.
- The second is that privacy laws often prohibits the sharing or storing of CDD information. One of the key concerns is indeed that information, especially when exchanged across borders, can be shared without due process of law, misused or leaked to track and profile users.

Both these issues call for a coordinated approach among countries and stakeholders. First, correspondent entities would find it more attractive to use information-sharing mechanisms such as KYC utilities if they could rely on the information these utilities provide. This could happen with the development of standards that guarantee the quality of the data the utilities hold and some form of external accreditation process to test compliance with the standard.[69] Second, AML/CFT and data protection authorities should clarify the extent to which transferring data to comply with AML/CFT regulation is permissible[70] and the different jurisdictions could discuss ways to share information across borders without undermining confidentiality.[71]

A promising alternative to strike the balance between information sharing and privacy protection is the development of user-centric IDs stored on a DL. In these systems, each person has an 'identity wallet' that she can access from her mobile phone and is associated with a cryptographic public key (functioning as the person's ID number) and a private key (functioning as her password and digital signature). The wallet stores time-stamped

[68] Financial Conduct Authority, 'New technologies and Anti-Money Laundering Compliance', March 2017.

[69] In February 2018 the Wolfsberg Group published their Correspondent Banking Due Diligence Questionnaire to collect KYC information to assess risk. This could become a standard set of questions that a correspondent can ask a respondent.

[70] Financial Action Task Force, 'FATF Guidance – Private Sector Information Sharing', November 2017.

[71] Egmont Group of Financial Intelligence Units, 'Enterprise-wide STR Sharing: Issues and Approaches', 2011.

documents from trusted authorities (such as passport authorities, banks or credit rating agencies) certifying that the person has certain attributes (for example, has a US passport, is over 21, or has a credit rating over 700) that she can share whenever needed. The first benefit is privacy, because this person can control with whom she shares her personal information and how much information she shares. The second benefit is security because, unlike for KYC utilities, information is not stored in a centralised database. This method would also allow to sidestep privacy laws that prohibit the creation of centralised databases for customer data because it gives information control back to the customer herself.[72] The idea of a user-centric ID is being tested in Canada in a project connecting the Canadian government with the largest banks and telecoms on a permissioned ledger.[73]

6. Benefits of the Proposal and Conclusion

We have proposed a new payment system to process cross-border transactions between Israel and the West Bank. This system involves the setting-up of a private permissioned ledger, owned and supervised by the PMA and the BoI, where Israeli and Palestinian banks can exchange e-shekels backed 1:1 by shekel deposits held at the co-agency. Given the importance of money laundering and terrorism financing risk, banks participating to the distributed ledger would enforce strong AML/CFT controls and exchange deposit-like e-shekels, not providing any more anonymity than that in existing deposit accounts. Consensus mechanisms to validate transactions will depend on the level of trust that exists among participating banks and can vary for different groups of banks within the network. We have argued that the new payment system would provide the following direct advantages over correspondent banking:

- **Reduction of any single point of failure:** Reliance on one correspondent bank/government agency in Israel and one correspondent bank in the West Bank to settle cross-border transactions provides a classic example of a single point of failure, namely the possibility that the loss of one entity poses a threat to all transactions. This entails a huge investment of resources to ensure business continuity and the set-up of alternative arrangements. Distributed ledgers allow participants to maintain and share mutually agreed records of transactions. This strengthens the resilience of the payment system because, when one node fails or withdraws, transactions can continue via others. Even if certain types of ledgers and consensus mechanisms can introduce points of failure (such as those introduced by Notary and Orderer nodes), these are typically less severe than in today's correspondent banking infrastructure and could be improved by implementing these services as a cluster operated by multiple parties.
- **Higher speed and lower cost of transactions:** Payments via correspondent entities are particularly slow and expensive and can take several days to settle. Participants to a distributed ledger can make transactions in near real-time and without relying

[72] Michael Pisa and Matt Juden, 'Blockchain and Economic Development: Hype vs. Reality', Center for Global Development Policy Paper 107, 2017.

[73] SecureKey Technologies and IBM are working together to build a digital identity network in Canada using the Hyperledger Fabric distributed ledger.

on intermediaries. They just need to send a payment request, validate it according to a consensus mechanism and exchange the digital asset over the network. If the settlement of the payment takes place off the ledger, this can still take some time depending on the evolution of cross-border trade and the authorities' preferences. Operating costs are also reduced because the use of the same synchronised ledger eliminates the duplication and inconsistencies that often occur between separate information repositories, and the related legal disputes.

- **Elimination of credit risk:** While correspondent entities typically take on some credit risk by extending credit to each other, transactions in e-shekels are equivalent to transactions in central bank money and as such carry no credit risk. Even if the bank receiving the payment credited its customer account before settlement had occurred and the sending bank went bankrupt in the meanwhile, the co-agency would still have the resources to settle the payment.
- **Better supervision and auditing:** The possibility to get full visibility on all transactions allows supervisory nodes to continuously monitor what is happening on the ledger. If suspicious transactions are detected, supervisory nodes can share the information with the relevant nodes. This constitutes an improvement with respect to current practices where problems can be identified only after transactions have taken place. Rather than having to rely on infrequent updates from third parties, auditors can also directly access the ledger to verify all transactions in almost real time. As transactions recorded in a distributed ledger cannot be erased or be tampered with, the cost of prevention and detection of fraud can also be reduced.
- **Reduction of physical barriers:** Physical barriers restrict movement between Israel and the West Bank. The exchange of a digital asset (e-shekels) over a distributed ledger eliminates the need to physically move means of payment, such as cheques,[74] across areas. Movement of collateral may still be needed for the settlement of payments off the ledger.
- **Reduction in the building-up of excess NIS liquidity in the Palestinian banking system:** Excess NIS cash in Palestinian banks' vaults could be used as collateral backing the e-shekels, after having been verified by both parties at the co-agency. This would decrease opportunity and security costs for Palestinian banks and allow future traceability of the cash within the payment system.
- **Increase in some banks' profitability:** Several reward schemes and protocols can be implemented to attract banks to the payment system. For example, banks could be rewarded for providing e-shekel liquidity, in terms of speed of payments' processing, cost of sending and/or receiving payments and total amount of transactions validated and/or intermediated.

[74] In 2016, the Knesset passed the Electronic Check Clearing Law to substitute physical cheque clearing with electronic clearing. This also aims at eliminating the need to physically move cheques across the West Bank and Israel.

- **Use of smart contracts to decrease counterparty risk:** The use of smart contracts to automate recurrent transactions, like the payment of salaries to Palestinians working in Israel, could have the beneficial effect of diminishing counterparty risk in an uncertain environment.

Some of these benefits can be obtained in other ways but their simultaneous achievement within this payment system could result in a better profitability/risk mix for banks and encourage them to participate in the system and increase its liquidity. Also, the development of a new platform could be a means to solve legacy constraints, even if adequate testing will be required given the early stage of development of DLT.

While we have discussed the introduction of this new payment system only to support settlement of transactions between Israel and the West Bank, the platform we propose could become useful in case the Palestinians, through the process outlined in the Paris Protocol, decided to introduce their own (digital) currency. In particular, this platform could allow Palestinian banks to trade e-shekels and e-shekels' derivatives among themselves, potentially allowing settlements in a digital currency. One path forward would be to allow Palestinian banks to issue an e-shekel derivative – a 'p-shekel' – in proportion to their e-shekel deposits at the co-agency. These p-shekels could be used for interbank borrowing and lending, and retail trades. The PMA would be responsible for protecting the integrity of the Palestinian financial system by actively monitoring the participating banks' balance sheets. The benefits and challenges in introducing a digital currency in the Palestinian domestic market are left to future research.

Middle East Centre

Middle East Centre
London School of Economics
Houghton Street
London, WC2A 2AE


@LSEMiddleEast


@lsemiddleeastcentre


lse.middleeast


lse.ac.uk/mec