

Cryptotechnologies in international payments

Information Paper

Working Group on Cryptotechnology
in International Payments

CONTENTS

Introduction	4
Current challenges in international payments	4
KYC and fraud checks	5
Liquidity costs	5
Regulatory frameworks and reporting requirements	6
Lack of transparency and speed	6
Reliance on a small number of large banks	6
Competitive pressure from non-banks	7
How cryptotechnologies could improve international payments	7
Key characteristics of cryptotechnologies	7
Improved information and risk management	8
Speed, access, and FX	9
Products and services	9
Use cases for cryptotechnologies in international payments	9
Use case: KYC compliance / identity management	10
Use case: International low-value payments	12
Long-term challenges to using cryptotechnologies for international payments	14
IT integration and business process rejuvenation	14
Legal frameworks and security	15
Conclusion	15
Appendix 1: Current initiatives aimed at improving international payments	16

Copyright © 2017 Euro Banking Association (EBA)

All rights reserved. Brief excerpts may be reproduced for non-commercial purposes, with an acknowledgement of the source.

The information contained in this document is provided for information purposes only and should not be construed as professional advice.

The information paper is the result of an analysis carried out by the Working Group on Cryptotechnology in International Payments.

The EBA does not accept any liability whatsoever arising from any alleged consequences or damages arising from the use or application of the information and give no warranties of any kind in relation to the information provided.

TABLE OF FIGURES

Figure 1: Current challenges for international payment stakeholders	4
Figure 2: Benefits of cryptotechnologies in international payments	8
Figure 3: Average cost breakdown of an international payment	10
Figure 4: KYC registry use case	11
Figure 5: Low-value P2P / B2C international payment use case	13

INTRODUCTION

International payments are vital to the global economy, and international payment services are in high demand, particularly from corporates. Deutsche Bank estimates the B2B cross-border payments market at 1.2 trillion USD today, and this market is expected to double by 2019. But as other aspects of business such as communication have modernised over the years, the process of sending and receiving cross-border payments has remained largely unchanged over the past few decades. While communication between banks and their customers may be instant, the reliance on nostro/vostro accounts, multiple intermediaries, deferred settlement procedures, manual reporting and screening procedures mean that it can take days for a payment to reach a beneficiary. Manual Know Your Customer (KYC) procedures, as well as sanctions screening and fraud checks also contribute to delays and high costs for both banks and end users. Banks are under constant pressure to comply with regulatory requirements while remaining competitive with non-bank payment providers that

offer better service and terms to end users. As banks look to improve service in international payments, cryptotechnologies have emerged as a technology that can help drastically lower operating costs for international payments, as well as increase speed, transparency, and service to consumers and corporates. The development of cryptotechnologies for international payments could enable banks to fend off competition in an ever-expanding market while maintaining compliance with key regulatory requirements in markets around the world.

CURRENT CHALLENGES IN INTERNATIONAL PAYMENTS

Before exploring how new technologies can lower costs and improve service in international payments, it is necessary to detail the major issues faced by banks and end users in international payments

	Large correspondent banks	Small- and medium-sized banks	End users (corporates)
Cost of ensuring correspondent KYC compliance	✓	✓	N/A
Service costs to correspondents	N/A	✓	✓
Nostro/vostro liquidity provision		✓	N/A
Unclear regulatory frameworks	✓	✓	✓
Lack of transparency in reporting	✓	✓	✓
Delays in processing / settlement of payments	✓	✓	✓
Dominance of large correspondent banks		✓	
Competition from non-bank payment providers	✓	✓	N/A

Figure 1: Current challenges for international payment stakeholders

Source: Lipis Advisors

today. Major issues include the cost of KYC and fraud checks, liquidity management using nostro/vostro accounts, payments reconciliation and reporting requirements, a lack of transparency and speed, dependence on a small number of global correspondents, and competition from non-bank payment providers.

KYC and fraud checks

Compliance with KYC provisions is perhaps the biggest issue for banks in international payments today. KYC due diligence is something that all banks must perform when on-boarding new customers, whether they are consumers or businesses. KYC procedures, including the documents needed to identify a customer and the verification process required to complete the process, vary by country and client type. In an international payments context, the complexity of the process of onboarding and checking documents to complete KYC procedures is amplified by the fact that different jurisdictions have different standards for onboarding, reporting, and processing new information and that banks are often required to know not only information related to their customers but also information on their customers' customers (KYCC).

This complex and time intensive process causes high costs for large correspondent banks. Different KYC procedures and standards, combined with the need to ensure compliance with anti-money laundering/counter-terrorism financing regulations (AML/CTF) and sanctions screening, lead to these banks performing regulatory screening on all payments it processes, regardless of how many times these same checks have been performed by upstream banks. This process requires banks to bear significant costs in time and resources. Combining this fact with low transaction volumes, the perceived riskiness of sending payments to and from certain jurisdictions, repu-

tational risk and possibility of high fines in the case of non-compliance, and the lack of adequate customer information in some cases has obliged some banks to reduce the number of correspondents they service, which can have negative effects on service to end users.¹

The high cost of KYC compliance also affects the prices charged to smaller banks and end users. The more complex the value chain is for an international payment, the higher these costs will be. These fees are passed on to end users, whether the party sending the payment or the beneficiary who finds that fees have been taken out of the received payment amount. Small and medium-sized banks that rely on larger correspondents to send or receive payments abroad may also be charged fees to cover these costs.

Liquidity costs

High liquidity costs related to the funding of nostro/vostro accounts is another important issue faced by banks of all sizes. Large correspondent banks can hold hundreds or even thousands of vostro accounts for banks in other markets that seek to send or receive payments from abroad.² Funds are exchanged internationally via book transfers between these accounts, and the process of keeping track of outstanding funds and re-capitalising these accounts can present huge costs for nostro account holders. In addition, each bank must keep separate records any time funds are transferred to or from a nostro/vostro account, and the process of reconciling these two sets of records can be complicated by delays in payment processing and manual reconciliation processes.

¹ Committee on Payments and Market Infrastructures, "Correspondent banking," July 2016, pp. 1-10; Financial Action Task Force, "Correspondent Banking Services," October 2016.

² These same accounts are referred to as nostro accounts by the account holder abroad.

Regulatory frameworks and reporting requirements

For both banks and end users, compliance with laws related to reporting and record keeping across different geographies can create a significant burden on efficiency in cross-border payments. A major factor here is the fact that the data included with payment messages differs by standard and geography, and international payments must often be supplemented with non-payment messaging, which must then be reconciled with payment information across multiple parties. Banks need to inform their customers of the different reporting requirements when sending money abroad (e.g. when sending or receiving a payment above a certain amount necessitates reporting to a regulatory authority), and end users (particularly corporates) need to ensure that the quality of their reporting is up to the standards of the local authority. Stakeholders must know what the regulatory requirements are in disparate markets and ensure that the necessary information to comply with these laws are available to banks and end users and that processes are in place to guarantee their quality.

Lack of transparency and speed

A big issue for banks and end users, particularly for businesses sending or receiving payments from abroad, is the inability to determine exactly when a payment will arrive at the beneficiary. In the case of international payments that go through multiple correspondents, it is equally difficult to determine exactly which correspondent is processing a payment at any given time. This lack of transparency is in stark contrast to the transparency provided by businesses such as Amazon, which can tell consumers exactly where a package is even before it has reached the recipient. A similar level of transparency in international payments could be vital to enabling banks to offer new products such as payment tracking, and could also lead to new propositions in global trade

and supply chain finance. And providing transparency of payment status and transaction fees would allow all parties to the transaction to have full visibility of payment flows and have a head start on any business or technical processing that the flow of funds will necessitate.

In addition to this lack of transparency, international payments often require days to reach a beneficiary. In many cases, even simple international payment transactions that are sent directly between two banks via nostro/vostro accounts may have to wait until the end of the processing day to be posted to a beneficiary's account. The inclusion of any correspondent(s) in the value chain between the sending and receiving bank (each of which must perform manual filtering and screening checks) increases the delay in a payment reaching an end user. As markets around the world are actively developing instant payment systems for low-value domestic payments, international payments struggle to guarantee D+0 or D+1 posting, which can lead to delays in any business activity that relies on a payment being made and can lead to a build-up of settlement risk as payments remain in limbo for hours or days at a time. Thus, a growing number of consumers and businesses look to non-bank payment providers for international payment services, reducing potential revenue for banks.

Reliance on a small number of large banks

Another significant issue in international payments is the dominance of a small number of banks that have global or regional reach. Reachability is key in international payments, and the clear majority of banks around the world do not have a global or even regional presence that would enable them to send or receive payments in multiple markets. Small and medium-sized banks often have limited access to correspondent banking networks, or can only access international payment services via larger institutions.

This can constrain reachability, especially as larger correspondent banks reduce the number of correspondents they serve, particularly in far-flung markets. For both smaller banks and end users, service levels are often reliant on whether or not a service is offered by a larger bank.

Competitive pressure from non-banks

The inefficiencies and high costs of international payments have created opportunities for non-banks to compete in the cross-border payment market. Consumers and small businesses increasingly use providers such as PayPal or TransferWise to send and receive funds cross border, while larger businesses (and sometimes even banks) may turn to Western Union to provide reach to some markets. These providers can often provide improved transparency and speed of payments compared to banks, and on average charge lower fees than banks. But fees remain high even with non-bank providers, and these providers may have difficulty in enabling customers to comply with reporting requirements and other regulatory needs. Despite these issues, non-bank providers often represent an improvement over banks in international payments.

HOW CRYPTOTECHNOLOGIES COULD IMPROVE INTERNATIONAL PAYMENTS

The development and maturation of cryptotechnologies – in the form of platforms, networks, and virtual currencies – has the potential to transform the international payments business for all stakeholders.³ Cryptotechnologies offer the potential to drastically

lower costs by increasing transparency, reducing risk, boosting speed, and increasing access to international payment networks. All of this can lead to improved service for both banks and end users.

Key characteristics of cryptotechnologies

Much has been written about the technical aspects of different cryptotechnology solutions, from Bitcoin to Ethereum to Ripple and beyond. Each separate solution has certain unique features. But almost all cryptotechnologies share some of the following core features:

- ▶ A shared, uniform ledger that is replicated among all participants over a network of interconnected computers.
- ▶ Security and accuracy of the ledger is ensured through cryptographic methods.⁴
- ▶ Control of the ledger is decentralised among network participants (no single central counterparty).
- ▶ Once verified, transactions on the ledger are fixed and indisputable.

Many cryptotechnologies differ in the method of verification used to update a ledger. Unpermissioned ledgers such as Bitcoin allow all participants to verify new transactions while permissioned ledgers only enable certain participants to authenticate transactions.⁵ They also differ in the amount of information that is shared among network participants. The concept of private distributed ledgers which limit the information that certain participants can view is

³ For more information, see the World Economic Forum's August 2016 report "The future of financial infrastructure," pp. 46-55.

⁴ As with some legacy networks such as SWIFT, security of the network as a whole is ensured, but it remains vulnerable to so-called "weakest link" attacks. Each node in the network must ensure its own security procedures for accessing the network.

⁵ UK Government Office for Science, "Distributed Ledger Technology: beyond blockchain", 2016, pp. 17-19. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Benefits of cryptotechnologies in international payments

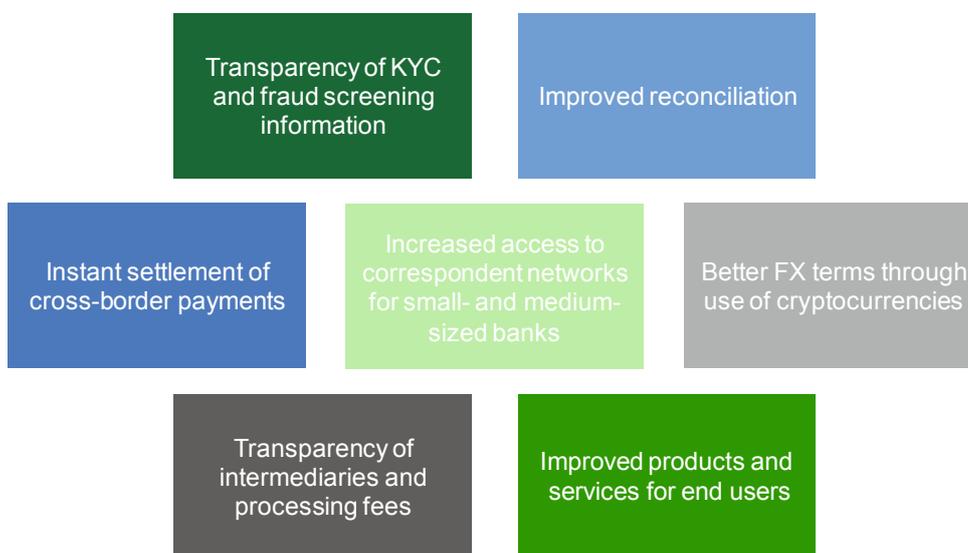


Figure 2: *Benefits of cryptotechnologies in international payments*
Source: Lipis Advisors

becoming more popular as financial institutions actively explore use cases.⁶ But at their core, cryptotechnologies enable all participants in a network to view and exchange information securely over a fixed, indisputable, and distributed ledger. The information exchange can occur instantly or with a delay (e.g. updates to the Bitcoin ledger occur every 10 minutes), and the information could include data related to a trade transaction, information necessary for regulatory reporting, funds transfers, contractual information (smart contracts), and more.⁷

Improved information and risk management

The complete transparency of information among all network participants via a distributed depository of KYC and fraud information could eliminate the

need for individual banks to perform redundant KYC checks by making KYC information freely available to all parties in a transaction. Information transparency could also have hugely beneficial effects on payments reconciliation. Today, when one bank sends money abroad using a correspondent, both banks create separate account ledgers that must be reconciled once a transaction is complete. Using cryptotechnologies, this reconciliation information could be exchanged via a distributed ledger, giving all parties involved instant access to important transaction information without the risk of manual processing errors or asymmetrical information between parties. This could save banks time and resources currently devoted to complicated reconciliation processes, and these cost savings could be passed on to end users.

The reliance on multiple intermediaries to send money abroad means that sending banks often have no idea of the risk profile of a transaction as it is being

⁶ <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

⁷ For more information on cryptotechnologies, please see the EBA report, "Cryptotechnologies, a major IT innovation and catalyst for change," May 2015. https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf

processed. For international payments that involve non-liquid currencies, even the largest correspondent banks may have to rely on multiple intermediaries to ensure that a payment reaches its destination in the proper currency. In addition to the delays in processing (and added service fees), this means that a sending bank often has no transparency as to where the funds are before they reach the beneficiary, which makes controlling settlement risk extremely difficult. The sending bank and the larger correspondent may not know what risks are outstanding until a payment reaches the beneficiary. And the higher the value of a payment is, the higher the risk profile. Cryptotechnologies could drastically reduce this risk burden by both diminishing or eliminating the need for intermediaries and by instantly transferring value from one account to another, thereby avoiding the risk of non-settlement of a pending payment.

Speed, access, and FX

The instant exchange of information between participants presents a huge opportunity to speed up one or more legs of an international transaction. Instead of an international payment posting to a beneficiary's account within days, cryptotechnologies could facilitate D+0 (or faster) processing. It should be pointed out that the speed of message exchange in international payments is not a huge issue today. Indeed, the SWIFT network already enables the exchange of payment messages in near real time. But the exchange of these messages rarely translates into the exchange of funds in a nostro/vostro account. The real benefit of cryptotechnologies in this space lies in the increased automation of this process that will occur once a cryptotechnology-based platform is incorporated into a bank's business and IT processes.

The fact that cryptotechnologies enable the direct participation of small and medium-sized banks in correspondent networks could lead to cost savings for both banks and end users, as it would drastically

simplify the value chain for cross-border payments. Instead of a payment going through multiple correspondents and currencies before reaching its destination, cryptotechnologies could enable a direct link between two banks anywhere in the world. Furthermore, the use of cryptocurrencies could help reduce FX costs. A cryptocurrency could be used to “translate” between two or more fiat currencies. This could lead to cost savings, particularly if one or more of the fiat currencies used are in farther flung markets where FX costs are higher.

Products and services

The ability of smaller institutions to directly exchange international payments with other banks could spur competition by enabling small and medium-sized banks to develop value-added services for their customers that they cannot offer today unless a larger correspondent also offers that service. Even if the democratising effects are not realised in the short-term, the efficiencies gained via cryptotechnologies could allow larger correspondent banks to offer improved services to smaller correspondents. They could even diversify their offerings to enable different service tiers, which could bring added revenue.

USE CASES FOR CRYPTOTECHNOLOGIES IN INTERNATIONAL PAYMENTS

The use of cryptotechnologies will be driven by tangible use cases that benefit banks and their customers. High operating costs inhibit many potential improvements in international payments. Directly addressing these high costs using cryptotechnologies could help banks improve service to end users, increase efficiency, speed up processing times, lower internal costs, and develop new products and services in cross-border payments.

McKinsey cost breakdown of international payments

Average cost: 25 – 35 USD

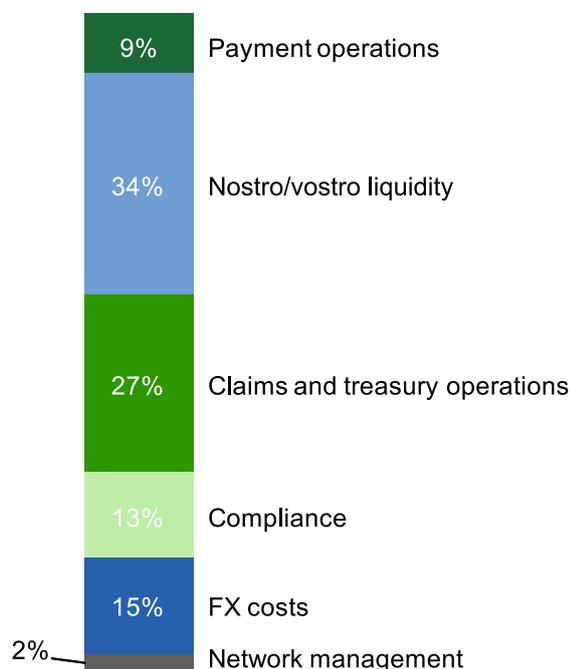


Figure 3: Average cost breakdown of an international payment

Source: McKinsey & Company, "Global Payments 2016: Strong Fundamentals Despite Uncertain Times"

Lowering these costs requires an understanding of the cost structure of an international payment. In its report "Global Payments 2016: Strong Fundamentals Despite Uncertain Times," McKinsey identifies six categories that drive the high cost of international payments for banks and the relative share of overall cost devoted to each category: payment operations, nostro/vostro liquidity, claims and treasury operations, compliance, FX costs, and network management. These drivers lead to an average cost of between 25 and 35 USD per international payment according to McKinsey's research.⁸ The exact breakdown of costs can be seen in Figure 3 above.

While the exact breakdown of costs may differ between banks and according to the currencies and corridors through which an international payment is being sent, McKinsey's cost breakdown nevertheless provides a useful framework for addressing the

general cost structure of cross-border payments and for detailing how specific cryptotechnology use cases can impact operating costs by minimising the effect of certain drivers.

Use case: KYC compliance / identity management

Cost drivers affected:
Payment operations, compliance

The high cost of KYC compliance has led banks around the world to reduce the number of correspondents they serve in international payments. According to Accuity, correspondent banking relationships have decreased by 39% globally since 2013. Over the same period, the total number of banks has

⁸ McKinsey & Company, "Global Payments 2016: Strong Fundamentals Despite Uncertain Times," September 2016.

increased by 7%. The cost of ensuring compliance with KYC and fraud screening procedures increases as the complexity of the value chain for an international payment escalates. Correspondent banks not only have to ensure KYC compliance for banks that they service directly, but also for any correspondents that their customer banks service (know your customer's customer). The uncertainty and high cost of these procedures has driven the reduction in correspondent banking relationships, which has a negative effect on service levels and reach for banks and end users around the world.⁹

Cryptotechnologies can enable increased transparency of KYC and fraud screening information by distributing access to legal identifiers on a shared ledger. Banks could share customer KYC information on a cryptotechnology platform that can be accessed

by other banks and regulators when performing KYC checks on international correspondents. The distributed nature of the platform(s) means that updated information can be viewed by all participants in near real time without the need to rely on a single counterparty to update the ledger. The information available on the platform would encompass a legal identifier for an individual or business, as well as additional information required by national regulators such as business address, bank account identifier information, or tax identification numbers.

It is likely that local regulators will play the role of validating and authorising the legal identifier, and the validation of transactions on the ledger itself could be distributed across participants according to a consensus method agreed to by participants. It is also expected that there will not be one global

Use case: KYC registry / ID management

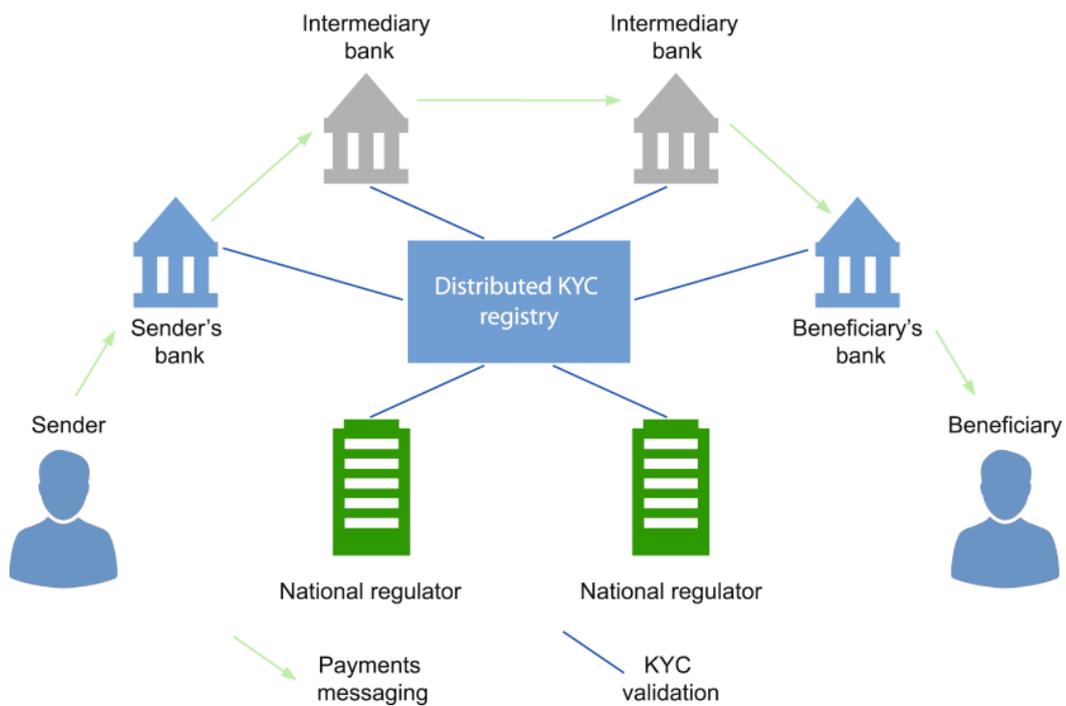


Figure 4: KYC registry use case
Source: Lipis Advisors

⁹ This process is referred to as “de-risking” by a number of bodies, including FATF.
<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html>

cryptotechnology platform for KYC information, but rather several local, national, or regional ledgers that are interoperable. This will allow local communities or banks and regulators to ensure legally compliant, up-to-date information that can be shared with banks around the world.

Practical considerations of cryptotechnology KYC registry

Several hurdles need to be overcome to enable this use case. Foremost is the need for an industry-wide legal identifier that can be used for international payments. There are several legal identifiers in use today that could serve this function, including LEI, BIC, and ISO 17442. Industry stakeholders should decide whether these identifiers are sufficient or whether a new identifier is needed to ease KYC compliance across borders. Determining a legal identifier will require industry cooperation to determine the necessary elements of a legal identifier in an international context.

Banks and regulators will also need to develop governance frameworks for cryptotechnology platforms used to exchange legal identifier information. Decisions must be made on issues such as ledger validation methods, access to the ledger, and the depth of information shared on the ledger. These frameworks are likely to take place on a local or national level, but international cooperation will also be required to harmonise legal identifier information and ensure interoperability between nationally controlled ledgers. The lack of common frameworks could result in fragmented cryptotechnology solutions, which inhibits the utility and benefits of a distributed KYC registry and could decrease the chances of widespread adoption by banks.

Use case: International low-value payments

Cost drivers affected:

Claims and treasury operations, FX costs

The current business model for international payments lacks the efficiency and cost effectiveness needed to enable high volume, low-value cross-border payments. This inhibits use cases and leaves certain market segments such as SMEs and consumers under-served. As such, consumers and small businesses looking for international payment services often rely on non-bank payment service providers such as Western Union or TransferWise to send and receive money cross-border. Cryptotechnologies can help banks compete in this market by increasing efficiency and lowering costs, thereby opening-up opportunities for improved products and services in low-value international payments. The full impact of these changes will come from using cryptotechnologies to exchange value (not just information) across borders, and could also lead to major changes to the international payments business model by reducing the number of intermediaries, expanding access to international payment networks, and increasing the speed of both processing and settlement of payment transactions.

The two main use cases that banks can focus on in this space are P2P cross-border remittances and international B2C/G2C payments. SWIFT estimates the international P2P payment market to represent about 530 billion USD in value, with low-value remittances making up a substantial portion of this market.¹⁰ Even with the introduction of new fintechs such as TransferWise alongside established fintechs like PayPal and traditional remittance providers like Western Union and MoneyGram, the global average cost to end users for sending remittances cross border was 7.42 percent of the transaction value as of Q3 2016. With average fees of over 11 percent of

¹⁰ http://www.alfi.lu/sites/alfi.lu/files/files/16577_Expl2_SWIFT2020_2.pdf

transaction value, banks remain the most expensive remittance provider available to consumers.¹¹ For a foreign worker sending money back to their family, this price can be prohibitively high, and the pressure on banks in this space will only increase as fintechs utilise new technologies to provide improved price and service to their customers.

Low-value B2C/G2C payments provide another attractive use case for banks. Technology is already enabling more and more people to work on a freelance basis from anywhere in the world, but it places obstacles to any freelancer that wishes to send or receive funds across borders. Media companies are increasingly purchasing content from individuals or small businesses operating in foreign markets, and sending small transaction amounts cross border to pay for this content is inefficient when fees can make up 10% or more of the transaction value. Government retirees living abroad can also be disadvantaged by high fees and delays in receiving pension payments. The high fees and lack of transparency provided by

banks for these types of payments both reduces their presence in the market and likely prevents some low-value international payments from being made at all. Banks cannot credibly target this market today, but cryptotechnologies could help them lower costs and increase efficiency by eliminating the need for multiple intermediaries to process international payments, providing transparency on interbank pricing and fees, and by potentially lowering FX costs using cryptocurrencies. A key enabler of this use case (and differentiator between the KYC registry use case) is the use of a cryptotechnology platform to send and receive value, not just information. Few banks are actively looking to leverage cryptotechnologies to open up the market for low-value international payments. This is a particular need for small and medium-sized enterprises (SMEs), which often need more advanced payment products than consumers but less comprehensive services than large corporates. Continued reluctance to explore opportunities in this market may lead to banks being left behind by consumers and businesses looking to send or receive money abroad.

Use case: low-value international payments

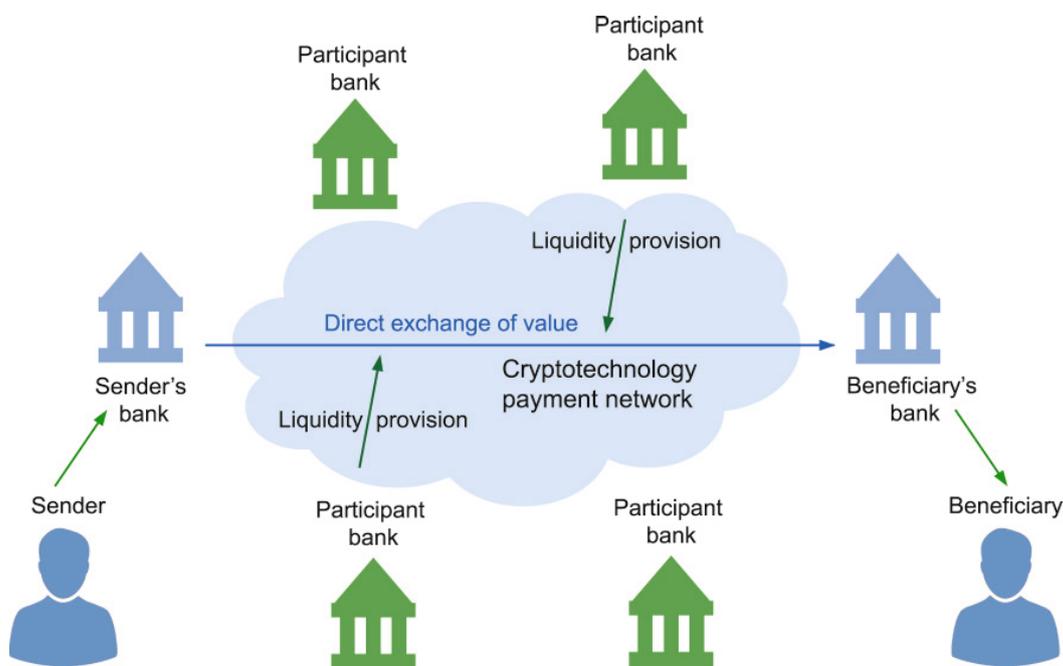


Figure 5: Low-value P2P / B2C international payment use case
Source: Lipis Advisors

¹¹ https://remittanceprices.worldbank.org/sites/default/files/rpw_report_sept_2016.pdf

Practical considerations of low-value international payments

One of the key issues banks will face when leveraging cryptotechnologies to send and receive low-value international payments will be in integrating legacy business services with cutting edge cryptotechnology platforms. Businesses need to comply with regulatory reporting requirements (which differ by market), and any cryptotechnology solution will need to be compliant with these processes. There are also concerns about liquidity management, as current cryptotechnology solutions aimed at sending and receiving value do not address the issue of nostro/vostro liquidity, which can make up about one third of the total cost of an international payment (see Figure 3 above). Lastly, if a native cryptocurrency is used as a bridge between fiat currencies (particularly when one or more non-liquid currencies are being exchanged), there are still concerns about how regulators will respond. Some central banks and national regulators have already gone on record as being against the holding or exchange of cryptocurrencies such as Bitcoin by banks.¹² As such, banks will need to engage local regulators when developing any cryptotechnology solution that relies on a virtual cryptocurrency for any part of an international transaction.

LONG-TERM CHALLENGES TO USING CRYPTOTECHNOLOGIES FOR INTERNATIONAL PAYMENTS

In addition to the practical considerations banks must confront in the short to medium term, there are several long-term issues that must be dealt with to realise the full benefits of using cryptotechnologies for international payments. These issues span the areas of IT, business processes, security, and regulation, and will be crucial to the widespread adoption of crypto-

technologies. While banks can derive near-term value from cryptotechnologies before solving these issues, they would be well advised to begin engaging with these topics today to remain competitive in the future.

IT integration and business process rejuvenation

While the exploration of cryptotechnologies by major banks has become mainstream over the past few years, few banks have integrated cryptotechnologies with legacy IT systems. Instead, cryptotechnology initiatives are pursued in separate silos or pilot projects within one bank or between groups of banks. The full value of cryptotechnologies for banks and the industry at large will come when the technology is integrated with legacy IT systems. This can mean integrating cryptotechnologies as another silo that is linked to legacy systems (e.g. through APIs or common standards) or a more full-scale back office modernisation using cryptotechnologies. This integration will be essential to unlocking new products and services, particularly in corporate payments, which have more onerous reporting and reconciliation requirements. It can also help reduce internal costs and enable cross-selling of products to customers.

The use of cryptotechnologies to distribute information and exchange value can have an immediate impact on lowering operating costs for international payments without the need to fully revamp the business processes banks currently rely on. But cryptotechnologies also have the potential to fundamentally change the process through which cross-border payments are sent and received. Perhaps the biggest change in this context would be the demise of nostro/vostro accounts and complex liquidity management processes. By establishing a distributed network

¹² Nigeria, India and the US are recent examples:

<https://www.cryptocoinsnews.com/indian-central-bank-against-bitcoin-tender/>

https://www.nytimes.com/2016/10/12/business/dealbook/central-banks-consider-bitcoins-technology-if-not-bitcoin.html?_r=0

where banks can send value directly to other banks, there would be no need to maintain liquidity in an account at a larger correspondent bank. Banks could hold their liquidity internally or rely on market makers (perhaps also utilising cryptocurrencies to “translate” between fiat currencies) to send and receive inter-bank payments. If more banks join cryptotechnology platforms and a positive network effects are achieved, international payments will be democratised and service improved for all end users.

Legal frameworks and security

To ensure the widespread participation necessary for the long-term success of cryptotechnology platforms, banks will need to engage central banks, regulators, and other stakeholders to create legal frameworks for the use of cryptotechnologies in payments and other areas of banking. The participation of regulators is key here, as a critical mass of banks is unlikely to seriously pursue cryptotechnologies if they are unsure of how regulators view the ability of the technology to meet regulatory principles such as security, resilience, and transparency. Issues such as access to the ledger, liability, privacy, finality of payments, resilience and security of the technology, and the use of cryptocurrencies need to be clarified. Local and national regulators are invited to determine whether existing legal frameworks are sufficient or if new laws or regulations are needed with respect to cryptotechnologies. These frameworks will likely pertain to the use of cryptotechnologies across multiple business areas beyond international payments to provide a solid legal basis that can enable widespread adoption.

CONCLUSION

The high costs of international payments today are hindering banks’ ability to compete and meet end users’ expectations of speed, transparency, and service. Cryptotechnologies offer an opportunity for banks to drastically lower operating costs and modernise the international payments value chain while continuing to comply with various national regulations. The success of any cryptotechnology initiative will rely on industry collaboration between banks, regulators, and other parties in this ecosystem. By focusing on use cases such as distributed KYC registries and low-value P2P/B2C payments, banks can lower operating costs and improve service, thereby boosting competitiveness and revenues. While major long-term challenges to the use of cryptotechnologies in international payments remain, banks would benefit greatly by engaging other financial institutions and regulators to develop concrete propositions to improve international payments. Without major changes to the international payments value chain, banks risk being left behind in a fast-growing market and leaving significant revenue on the table.

APPENDIX 1: CURRENT INITIATIVES AIMED AT IMPROVING INTERNATIONAL PAYMENTS

Bitcoin

While the use of Bitcoin by banks is generally frowned upon by regulators due to fraud and money laundering concerns, its anonymity, and the cryptocurrency's volatility, Bitcoin is used by consumers and some businesses to send and receive funds cross border. In addition, several companies leverage Bitcoin to ease FX costs and improve B2B payments, particularly in developing economies. BitPesa uses Bitcoin as a bridge between selected African currencies (in Kenya, Nigeria, Tanzania, and Uganda) and other currencies such as the Chinese yuan or US dollar to enable better terms for B2B international payments. Customers of fintechs such as BitPesa never hold or receive Bitcoins, the cryptocurrency is merely used on the back-end to enable FX.

<https://bitcoin.org/en/>

Ethereum

Ethereum is a smart contract platform that runs on a custom built global blockchain (separate from the Bitcoin blockchain). It acts as an application layer and features a native value token called Ether, which functions as "fuel" for the network and is used to pay transaction fees for Ethereum applications. Currently decentralised applications running on Ethereum include investment funding, Internet of Things (IoT) applications, crowdfunding portals, value tokens (cryptocurrencies), music distribution applications, and digital signatures.

In 2016, the Decentralised Autonomous Organization (DAO) was created as a decentralised venture capital fund on the Ethereum blockchain that would fund projects developed on the Ethereum blockchain.

The idea behind the DAO was to create a decentralised business model not tied to any state, persons, or management structure where investors can vote on proposals for Ethereum applications, with funds then dispersed by the DAO. The DAO was crowdfunded in May 2016 and raised over USD 150 million. In June 2016, hackers exploited vulnerabilities in the DAO code and stole 3.6 million ether (about USD 50 million at the time of the hack). As a result of the effort to reclaim the hacked DAO funds, the Ethereum blockchain underwent a hard fork, creating two separate blockchains. Attacks on the original blockchain ("Ethereum classic") continued, and further hard forks were deemed necessary. As of December 2016, Ethereum has undergone four hard forks.

<https://www.ethereum.org/>

Hyperledger

The Linux Foundation's Hyperledger project is an open source, collaborative effort to develop protocols and standards for blockchain technology. The project is not focused on any one industry or any single cryptotechnology architecture. Instead, the project seeks to push interoperability of distributed ledgers across industries and between cryptotechnology platforms that use various consensus models, access methods, and information requirements. Hyperledger members include cryptotechnology companies, large technology firms such as Cisco and IBM, and large financial institutions.

<https://www.hyperledger.org/>

Hyperledger Fabric

Fabric is a modular distributed ledger platform for smart contracts developed by IBM as part of the Hyperledger project. The platform uses a permissioned authentication method with both validating and non-validating nodes. It is an open source project aimed at use by businesses. Development is still in progress. IBM is also looking to combine its work with distributed ledgers/blockchain with its Watson artificial intelligence system with the intention of developing applications for the Internet of Things.

https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

Hyperledger Sawtooth Lake

As part of its participation in the Hyperledger project, Intel has developed Sawtooth Lake, a modular platform that enables companies to build custom distributed ledgers. Sawtooth Lake distributed ledgers support custom data models, transaction languages, and consensus methods. Sawtooth Lake offers users the ability to create custom “transaction families,” and offers three built-in transaction families aimed at frequent use cases, including a ledger service registry (EndPointRegistry), a testing service for deployed ledgers (IntegerKey), and a platform for buying, selling, and trading digital assets (MarketPlace).

<http://intelledger.github.io/introduction.html>

R3

R3 is a bank-owned consortium that includes over 70 of the world’s largest banks with the aim of developing an enterprise-grade global cryptotechnology ledger, researching and testing new cryptotechnol-

ogies, and developing commercial applications to run on cryptotechnology platforms. In November 2016, R3 announced a proof of concept for a shared KYC registry using R3’s Corda distributed ledger platform. The KYC registry allows participants to manage their customers’ identity information and permission other nodes on the network to access this information for KYC purposes. 10 banks are currently participating in the project (including BBVA, ING, Nordea, and UBS).

<http://www.r3cev.com/>

Ripple

The San Francisco-based start-up was one of the earliest companies actively exploring the use of distributed ledgers to send and receive international payments in the interbank space. The Ripple network is an open source, consensus-based distributed ledger that enables near instant settlement of transactions directly between two parties. The network also includes a native cryptocurrency (XRP) that can be used to bridge between fiat currencies (network participants are not required to use XRP when sending or receiving funds). In 2015, Ripple developed Interledger, a protocol designed to enable interoperability between ledgers with the aim of fostering global reach of distributed ledgers and payment networks.

<https://ripple.com/>

SWIFT Global Payments Initiative

SWIFT is the standard network used for international payments messaging between banks around the world. In late 2015, SWIFT announced the Global Payments Innovation (GPI) initiative with the participation of 73 banks.¹³ SWIFT has developed a GPI rulebook for participating banks, and is initially aimed

¹³ As of October 2016, 100 banks have joined the GPI initiative

at B2B international payments. GPI seeks to improve on the speed and transparency of international payments messaging by enabling same-day use of funds, transparency on fees, end-to-end payments tracking, and richer payment information.

Although SWIFT's Global Payments Initiative (GPI) does not currently utilise cryptotechnologies, SWIFT is actively exploring the use of cryptotechnologies in other areas. In November 2016, SWIFT unveiled a blockchain proof of concept aimed at bond trading that includes banks on 4 continents. SWIFT intends to analyse the use of cryptotechnologies to further develop GPI going forward.¹⁴

<https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/the-swift-gpi-initiative>

Visa-Chain partnership

In October 2016, Visa announced a partnership with Chain to develop B2B Connect, a blockchain-based infrastructure aimed at the international B2B payments market. B2B Connect will enable near real-time exchange of high-value B2B payments between banks. Both banks and corporates receive immediate notification of payment finality and full visibility of costs. The network will be a permissioned blockchain operated by Visa, and is expected to be launched in 2017.

<https://chain.com/press-releases/visa-introduces-international-b2b-payment-solution-built-on-chains-blockchain-technology/>

¹⁴ <https://www.finextra.com/newsarticle/29813/sofe-berlin-swift-unveils-blockchain-proof-of-concept>



Contact details

For any additional information, please contact:

Daniel Szmukler
Director
d.szmukler@abe-eba.eu

Euro Banking Association (EBA)
40 rue de Courcelles
F - 75008 Paris
TVA (VAT) n°: FR 12337899694

layout: www.quadratpunkt.de
cover source: © [Lipsis Advisors](#)