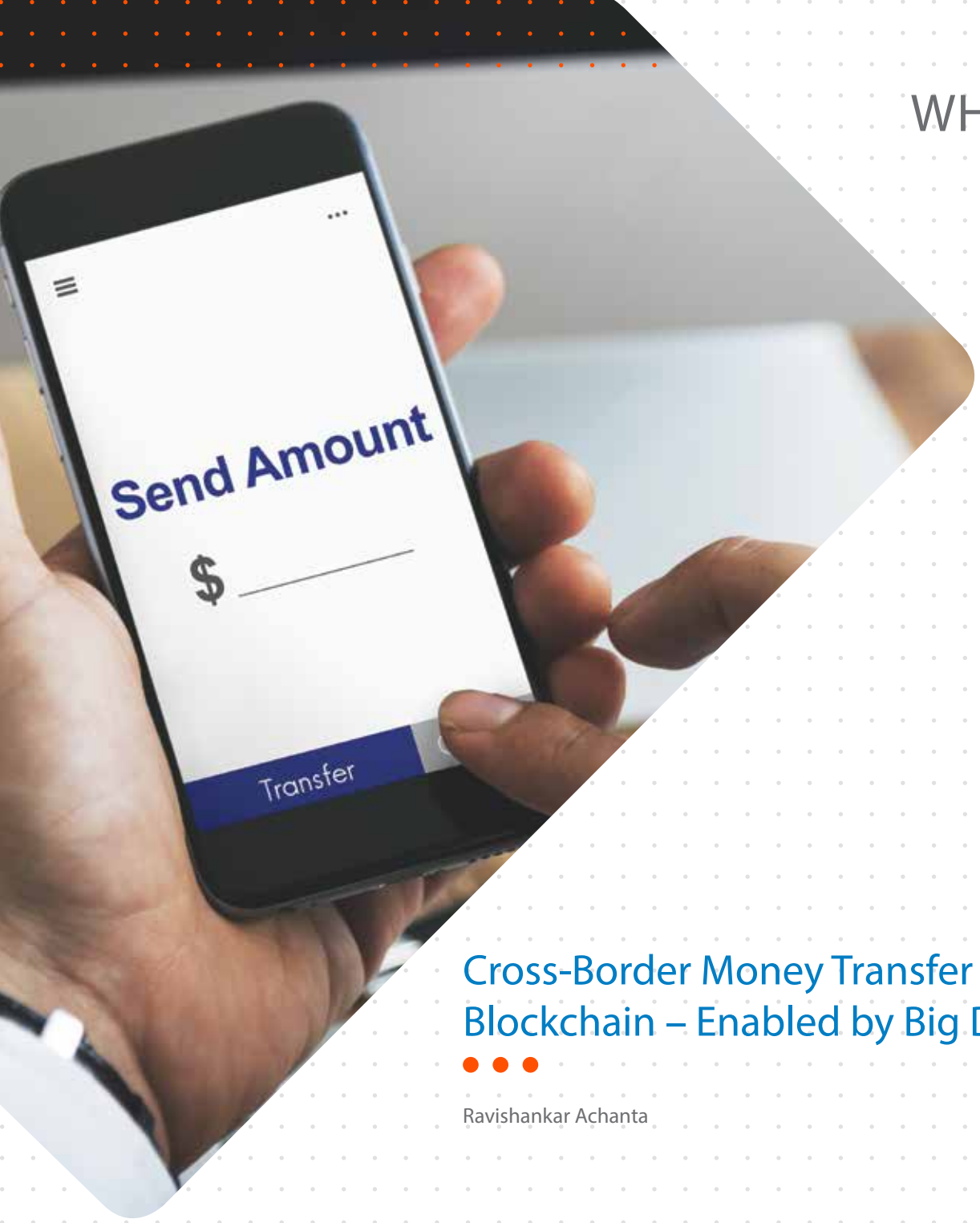
WHITE PAPER



Cross-Border Money Transfer Using Blockchain – Enabled by Big Data

Ravishankar Achanta

Infosys
be more

Abstract

Blockchain has been making a buzz for quite some time now and the 'distributed ledger blockchain' has been widely talked about by banks. Many of the banks and financial institutions have set up innovation labs to conduct proof of concepts to be able to harness the modern day technology around 'blockchain' and 'distributed ledger'. Industry studies have revealed that regulatory and compliance issues are the two biggest factors which are believed to contribute toward internal resistance to adoption of blockchain, and this needs to be duly addressed. An attempt to address this pain point using a point of view of having an additional DATA Layer introduced along the payment process chain involving the blockchain has been voiced.

Using the DATA Layer, the regulatory and compliance requirements around the details of the transaction for due transaction monitoring or validating the details of the originator and beneficiary for FATF or 'sanction screening' can be duly implemented. The amount of suspicious transactions for AML and the transactions through 'high risk countries' could minimize as there would be transparency amidst the network.

Also it has been opined that the best way to get started, is by moving with caution using a stepwise approach to get the dice rolling for Blockchain for intra-group payments first. The implementation would help banks / financial institutions immediately with the costs involved in the generation and processing of the MT202, MT199, MT999, etc., messages. Given the volumes per day, it would be a step in cost saving and reduced turnaround time as also to experience the benefits of the modern day technology of blockchain and distributed ledger. Also given that the scope is around intra-group payments, this would bring in a comfort factor for banks as the boundaries of the payments are known.

Cross-border money transfer and its drawbacks

Remittance is a fund-transfer transaction wherein funds are moved from one account to another account within the same or any other financial institution. In a cross-border payment, SWIFT handles only the movement of messages along the payment chain. The correspondent banks do the actual debits and credits across accounts based on the message and help pass on the value to the final beneficiary.

For example, bank A is sending a euro amount to a euro account in bank D in Germany. The workflow is given below:

- An MT103 (a SWIFT message format) in $US is sent to bank A in the US.
- Bank A sends the payment request to its correspondent bank, bank B via Fedwire and accompanies a debit / credit instruction for onward transmission.
- Bank B does the adjustments and sends a message to its correspondent bank, bank C in Brussels via the SWIFT network.
- Bank C transmits the value via Single Euro Payments Area (SEPA) to bank D in Germany.
- Bank D credits the supplier account in EUR.

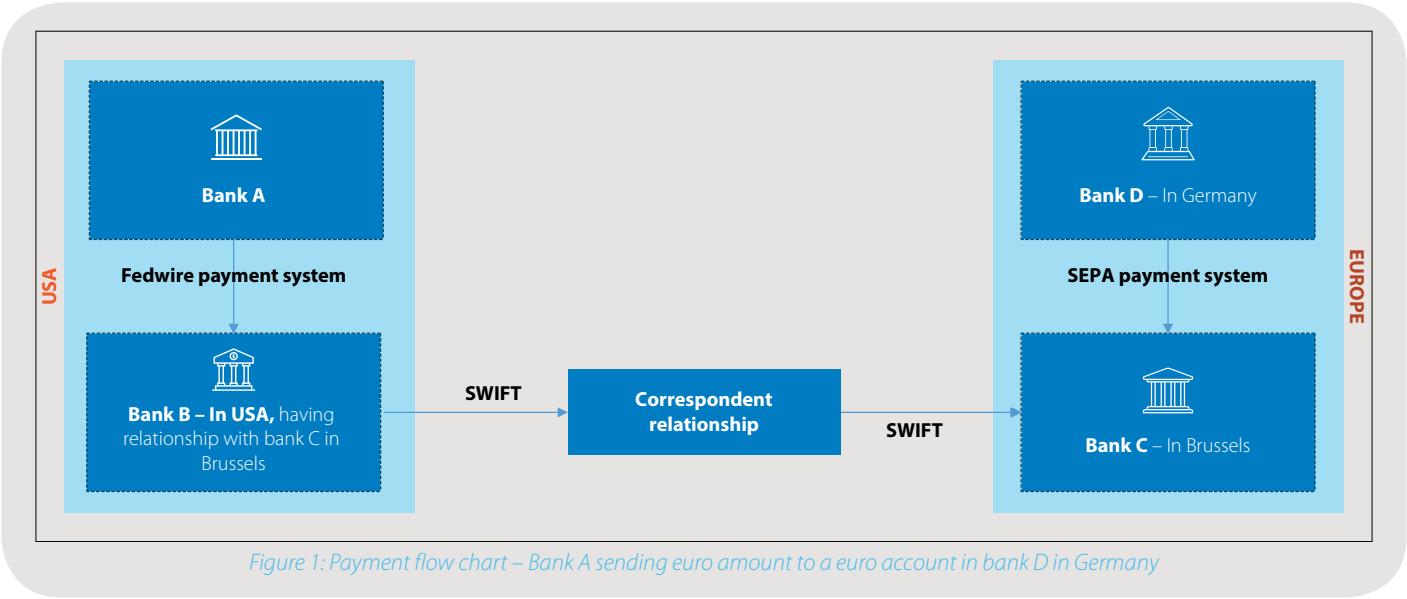


Figure 1: Payment flow chart – Bank A sending euro amount to a euro account in bank D in Germany

As shown in the payment flow chart (Figure 1), the banks charge fees for processing of each transaction, thus increasing the costs involved for all parties concerned. SWIFT charges for transmitting the messages and thus adds to the cost. Since the ledgers are local to the banks, the SWIFT messages ensure the debit entry of one bank's ledger is communicated to another bank so as to pass / post the corresponding credit entry in its ledger. With the increase in the number of payment messages in the chain, fees on SWIFT messages also increase.

The current process of international payments / transfer system with involvement of correspondent banks has the following drawbacks:

- Since no two banks can agree on a transaction based on their own ledger, SWIFT came into being to guarantee and confirm message transmission. Central banks operated as settlement agents to guarantee payments.
- SWIFT charges the bank for processing the payment orders irrespective of whether the bank is at both the receiving and sending end of the instruction.
- A single cross-border payment has to traverse through certain correspondent banks which are involved in activities like receiving, collating, and netting payment messages before retransmitting confirmations / denials to the respective banks. This increases the time to settle.
- Presence of a trusted third party with powers to overwrite and overturn ledger activities needed to have a unified view.
- A central bank typically insists that banks maintain sufficient liquidity in their settlement accounts or nostro accounts maintained with the central banks.
- In case of a cross-border payment for pooled account in certain banks, the originator of the message is modified and populated by an internal bank account number. This raises concern around the data protection and security in the receiving bank.
- Since the payment moves across Fedwire to SWIFT and then through SEPA, the messages involved are varied and different.

What is blockchain and how it can help facilitate cross-border money transfer

Given the shortcomings of the as-is process with cross-border payments, blockchain and the concept of the distributed ledger has been resonating well amidst the banking and financial sector. It has been making a buzz for quite some time now, and the distributed ledger blockchain is also widely talked about by banks.

Blockchain is a universal ledger present in a distributed network which is accessible to everybody in the network. Thus each node in the network will have a complete copy of the entire database or the ledger and any modifications to the same will have to be duly verified by other nodes / parties to validate on the modification done. Thus it requires a consensus of nodes to agree upon the state of the ledger for it to be valid. This would mean that direct transfers can occur instantly now and without fear of manipulation even for cross-border payments, because there are no intermediaries or correspondent banks involved. The underlying concept of distributed ledger makes it possible for the banks to have a bilateral, visible, and immutable transfer of value, adjudicated by the settlement agency.

Critical factors understood to be addressed for an industry-wide adoption of blockchain

Many banks and financial institutions have set up innovation labs to conduct proof of concepts (PoC) to be able to harness the modern day technology around blockchain and distributed ledger. According to a recent industry survey conducted by Accenture, it was found that around 30 percent of organizations are involved in conducting PoCs along with other FinTech companies, while 27 percent of the organizations are involved in formulating a strategy around the same. Among the PoCs being explored, below is the sequence of priorities attached by various organizations:

- Intra-bank cross-border payments
- Cross-border remittances
- Corporate payments
- Inter-bank cross-border payment systems
- Person-to-person payment

While the benefits of blockchain like the enabling of trust, user empowerment, reliability owing to decentralized network, enhancing transparency, reduced time for settlement of transactions, and reduced transaction costs were known to the financial services conducting PoCs. The below set of critical factors were understood to be addressed for industry-wide adoption of distributed ledger technology (DLT), which evolved as part of their proof of concepts.

- **Standardization** – Lack of standardization in formats. With globalization, we have several global standards for messaging Society for Worldwide Interbank Financial Telecommunication (SWIFT), Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT), Electronic Banking Internet Communication Standard (EBICS), ISO20022, and ISO8583.
- **Cost and time benefit with added payment transparency** – Cross-border payments continue to be expensive. It is difficult to assess and deduce charges incurred through multiple correspondent banks. The identity of the involved banks are not always known between sender and beneficiary bank and hence, the lack of transparency.
- **Data protection and privacy** – There is a strict need to ensure that there is no breach of data and that the data is not modified at any point of the chain.
- **Compliance and regulatory reporting** – Adhering to the compliance and regulatory reporting like the anti-money laundering (AML), know your customer (KYC), financial action task force (FATF), and others in order to ensure there is sufficient payment transparency and to keep a tab on the high-risk corridors or high-risk payments.
- **Collaboration** – Cooperation among payment service providers to create inter-operable blockchains. Need for an extensive global network.

What benefits does blockchain bring in, when leveraged for cross-border money transfer

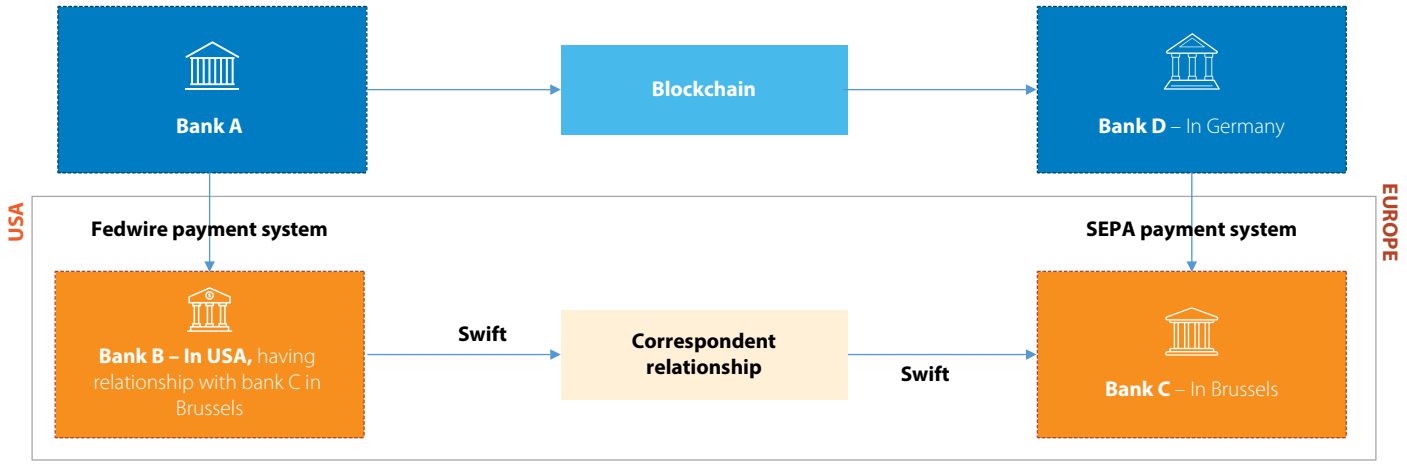


Figure 2: Money transfer from bank A to bank D through blockchain eliminating the 3rd party as highlighted

As depicted in Figure 2, blockchain brings in the following benefits:

- It leads to the exclusion of any middlemen, central agencies, or correspondents from the payment processing. Transaction is amidst the parties who have entered into a bilateral agreement, thus ensuring trust is in place.
- Reduced cost with minimal charges along the payment chain. In addition, SWIFT charges for the processing of the messages if the messages are routed through it. As of result of such charges, the correspondent banks / central agencies add to the cost of processing the payment, for activities like receiving, collating, and netting payment messages before retransmitting confirmations / denials to the respective banks.
- Reduced turnaround time for settlement as there is no need for central agencies and movement of messages.
- The intraday liquidity need not be ensured with the central banks. Since it is a distributed ledger and the nodes of the network have a copy of the balances as they are maintained in the settlement accounts with the other banks, the balances are duly maintained.
- Since the details of the transaction are encrypted and hashed, there is hardly any possibility to modify the data.
- Subject to no messages being transmitted, the challenges around the standardization are minimized too.
- Increased payment transparency with distributed ledger as sender and receiver are the nodes of the network / chain.

The challenges around the data protection and privacy could be addressed to some extent with the use of a private or permissioned blockchain where anybody cannot anonymously jump on the network and become a node. Such an arrangement will require the parties to register or enter into a bilateral agreement and access transactions using a private key amidst the trusted parties of the network. Also, everybody is aware of the level of difficulty to hack the underlying hashed transactions in the block.

As part of the R3 consortium, around 11 banks have been experimenting with the distributed ledger on a global private network by connecting on a private peer-to-peer distributed ledger, underpinned by Ethereum technology and hosted on a virtual private network, which is based on Microsoft Azure public cloud platform.

The consortium addresses challenges for collaboration to a certain extent. However, after the recent news of the exit of some of the major players from the R3 consortium, blockchain is becoming a battleground where competition has taken the driving seat instead of collaboration. This is clear, because there are no rules to the game currently and no standards have been defined.

While most of the critical factors seem to be amenable to a fair resolution, the biggest challenge is with respect to regulatory reporting. Many of the blockchain use cases suggest removal of middlemen including regulatory agencies, while a point of view to have a collaborative approach to avoid less disruption around this area having known the conservative approach of the banks or financial institutions, is being proposed.

Each of the regulatory reporting / transaction monitoring activity wants absolute payment transparency and would like to have the details of the parties involved to conduct customer due diligence / FATF / Dodd-Frank / sanction screening checks / AML / KYC / Basel III, or others. Industry study has revealed that the regulatory and compliance issues are the two biggest factors, which are believed to contribute towards internal resistance to adoption of blockchain and need to be duly addressed.

Collaborative approach to regulatory reporting by leveraging big data

It is believed that the challenge around maintaining compliance with regulators can be achieved by introducing an additional data layer along the payment process involving the blockchain. In the data layer, the registered details of the banks captured for entering into transactions within the nodes / networks of the permissioned blockchain need to be ingested. Similarly, the transaction details across the blockchain need to be ingested in the big data environment. Once these details are available, the data needs to be transformed as it is in hash format and a join with the registered details of the bank will enable extraction of the details for each of the transactions.

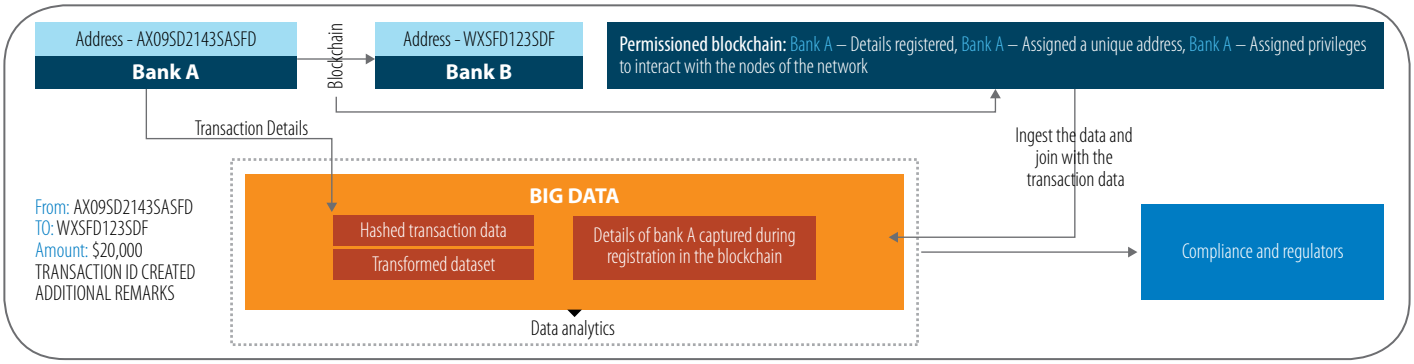


Figure 3: Structure showing the intra-group payments happening among the branches of the same bank or subsidiaries

The procedure as in Figure 3 can be implemented seamlessly for intra-group payments where payments happen amidst the branches of the same bank or subsidiaries. This framework can help avoid sending MT202 and acknowledgment of the same using a MT999, a MT910, or an MT900. Intra-group traffic data is less hand-picked by the regulators, and here it is also easy to enter into a bilateral agreement. Intra-group payments can be both domestic and cross-border. Domestic includes inter-branch payments within the same country, while cross-border includes inter-branch payments outside the country. In the above arrangement as depicted in Figure 3, the following transaction can be posted.

Debit	Ledger account of bank A which is exposed on the network. A common account for bank A
Credit	Ledger account of bank B which is exposed on the network. A common account for bank B

Now in order to extend this framework to the originator and beneficiary, the linkage needs to be expanded as follows:

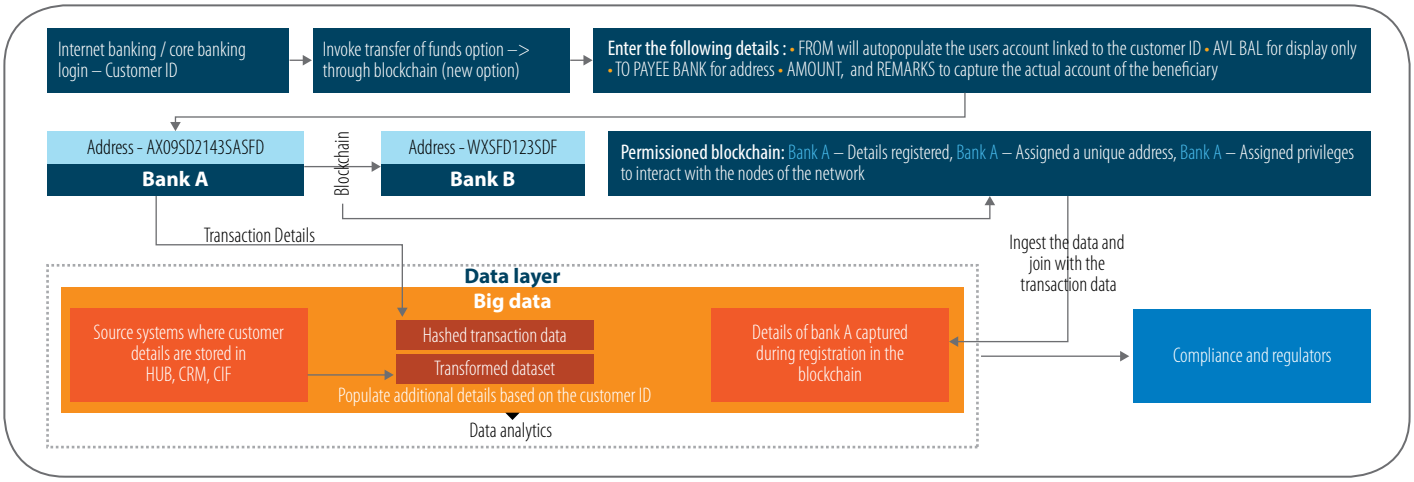


Figure 4: A framework showing a collaborative approach to regulatory reporting by leveraging big data

Three transactions can be posted as shown in Figure 4.

Transaction posted at bank A

Debit	Debit the customer / originator of the payment
Credit	Credit the settlement account for bank B as maintained in bank A

Transaction posted on blockchain

Debit	Ledger account of bank A which is exposed on the network. A common account for bank A which will be like a mirror account for the settlement account maintained for the banks.
Credit	Ledger account of bank B which is exposed on the network A common account for bank B which will be like a mirror account for the settlement account maintained for the banks.

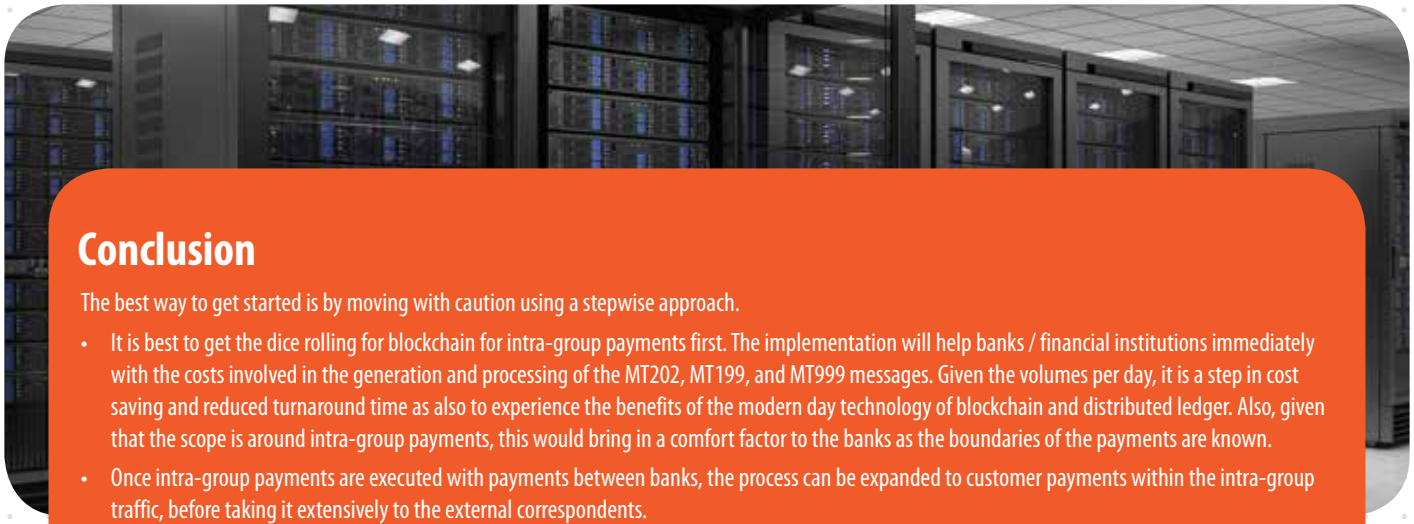
Transaction posted at bank A

Debit	Debit the settlement account for bank A as maintained in bank B
Credit	Credit the beneficiary customers account

Like internet banking, the user logs in using their customer ID credentials. The transaction carries the hashed account number of the originator and beneficiary in the additional information. For regulatory reporting, the details of the originator and beneficiary can be linked to the respective customer details database to extract all the relevant details like name, address, and other personal details. Since the transaction is between the nodes of the network, the transactions through high-risk corridors will be curtailed or minimized.

The customers are not provided with an individual address to connect to the node as it will expose a copy of all the customers' ledgers to each other. Given the volumes of the customers and to serve confidentiality and data privacy to the user, only the bank accounts are the part of network nodes. Using the data layer, the regulatory and compliance requirements around the details of the transaction for due transaction monitoring or validating the details of the originator and beneficiary for FATF or sanction screening can be duly implemented. The amount of suspicious transactions for AML and the transactions through high-risk countries are minimized as there is transparency in the network. Benefits of introducing a data layer enabled by big data:

- The ingest of data like customer details / registration details to the blockchain once scheduled and mapped from the source system tables can be automatically scooped or moved to the big data environment.
- The join of the underlying customer details with the hashed transactions in the block can also be done in the big data environment without disrupting the chain. Regulators would like to see the details which are not in hash format. Hence, a mechanism to either push a copy of the transaction before being hashed or attached to the block of the blockchain, can be thought-through, too.
- The data layer serves as a golden source of information for any regulatory / compliance / investigation purpose.
- A self-service business intelligence (BI) approach can be adopted wherein the access to the data visualization tools will be provided to a group of users who can then slice and dice data to their needs without moving the data from the environment. This ensures data governance in place and also helps the regulators or compliance or other departments to conduct independent analyses around the data.
- In the big data environment, the data can be duly partitioned by region, country, and date to keep the housekeeping simple and much cleaner.
- Given that the transaction data is in the big data environment, the automation of the FATF can be duly planned to be implemented validating the details of the originator and the beneficiary on name, address, and account-related details.



Conclusion

The best way to get started is by moving with caution using a stepwise approach.

- It is best to get the dice rolling for blockchain for intra-group payments first. The implementation will help banks / financial institutions immediately with the costs involved in the generation and processing of the MT202, MT199, and MT999 messages. Given the volumes per day, it is a step in cost saving and reduced turnaround time as also to experience the benefits of the modern day technology of blockchain and distributed ledger. Also, given that the scope is around intra-group payments, this would bring in a comfort factor to the banks as the boundaries of the payments are known.
- Once intra-group payments are executed with payments between banks, the process can be expanded to customer payments within the intra-group traffic, before taking it extensively to the external correspondents.

About the Author

Achanta Ravishankar

Lead Consultant, Cards & Payments Practice, Domain Consulting Group, Infosys

Ravishankar is passionate about the role of digital innovation in transforming the financial services landscape and focuses on new disruptive technologies and business models impacting the cards & payments industry. He has significant experience in banking IT with a focus on payments module, consultancy, training, implementation, and data analytics on large-scale implementation projects in Europe and the Middle East.

He can be reached at Ravishankar_Achanta@infosys.com.

References

https://www.finextra.com/news/fullstory.aspx?newsitemid=28356

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

http://panther/icetsblockchaincoe/files/2016/07/Blockchain-for-Cross-Border-Payments.pdf

https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html

http://www.consultancy.uk/news/12801/the-benefits-and-use-cases-for-blockchain-technology-in-banking

For more information, contact askus@infosys.com

Infosys be more