Blockchain Technology and Cross-Border Transactions

To what extent can blockchain technology increase the efficiency and security of cross-border transactions in the context of the current banking system?

Subject: Computer Science

Word Count: 4000

Table of Contents

I. Introduction: Bitcoin, Blockchain, and Applications

Blockchain was first conceptualized by Satoshi Nakamoto in 2008 when he published the Bitcoin whitepaper, proposing a groundbreaking peer-to-peer electronic cash system.[1] Bitcoin represents a virtual unit of currency that can be transferred over a network to facilitate financial transactions. Blockchain is the key innovation[2] of Bitcoin that enables transactions to be made in a secure, trackable, and open manner. A blockchain is an open, distributed ledger that records all past transactions in a verifiable and permanent way. Once recorded, the data in a blockchain cannot be altered without the consensus of network majority, enabling high security and high fault tolerance.

Blockchain will serve as the focus of this investigation. While initially proposed to implement Bitcoin, it has the potential to revolutionize data exchange in a plethora of industries as it enables a secure way to exchange and trace authentic information, a key characteristic that existing internet lacks. This paper will elaborate on the application of blockchain in the global payments industry, focusing on the research question: To what extent can blockchain technology increase the efficiency and security of cross-border transactions in the context of the current banking system?

II. Overview of Bitcoin

Unlike conventional currencies, Bitcoin is entirely virtual. The total number of Bitcoin that can exist is capped at 21 million.[3] New Bitcoin is generated at a fixed rate every ten minutes

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, accessed November 26.

[2] Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain,* (Beijing, OReilly, 2018), 2.

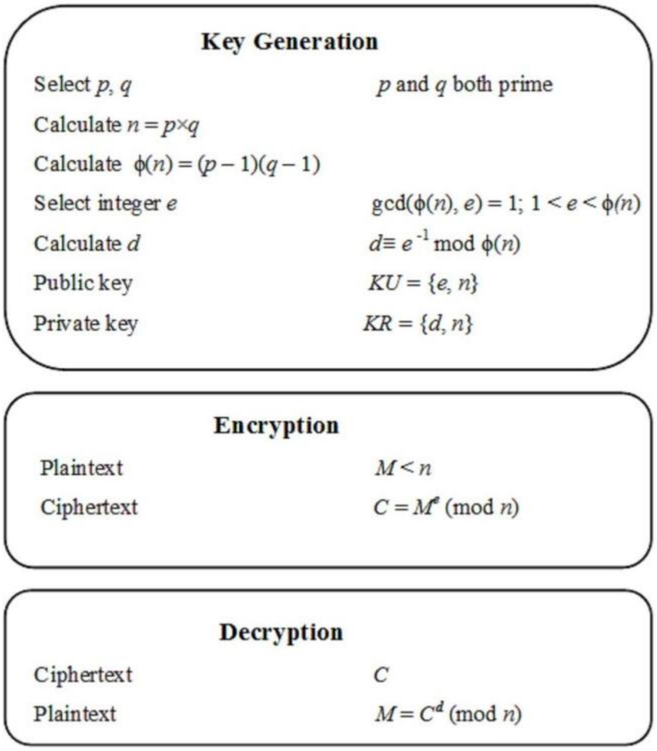
[3] Antonopoulos, *Mastering Bitcoin,* 213-269.

and is rewarded to a participating node in the network who competes to validate and record transactions made. The fastest participant to validate and bundle newly settled transactions is rewarded with new Bitcoin.

Bitcoin employs asymmetric cryptography to conduct secure financial transactions. Asymmetric cryptography[4] creates a set of public key and private key to encrypt and decrypt data. The public key is known by everyone while the private key is only known by the owner. A message encrypted using the public key can only be decrypted using the private key, and vice versa. In the Bitcoin network, the public key of each participant is also put through the SHA256 and RIPEMD160 hash functions to generate the participant's address. All Bitcoin participants can use the public key to either validate the authenticity of a message from the owner or send out a message that only the owner can decrypt. For a Bitcoin transaction, the sender uses his private key and the receiver's public key to encrypt the private message. The encrypted message, along with other necessary information, such as the address of the sender and receiver, is sent out to the network as one transaction. While all participants can receive and verify the transaction, only the receiver can unlock the private message with his own private key and the sender's public key.

[4] "Asymmetric Algorithms," Asymmetric Algorithms - Cryptography 2.9.dev1 Documentation, accessed December 1, 2019.

The public and private key pair must have a mathematical relationship with each other in order for a message to be encrypted with one key and then decrypted with another to obtain the same message. The most common algorithm used to generate a set of public and private key is the Rivest-Shamir-Adleman (RSA) algorithm,[5] which relies on calculations related to two large prime numbers (Fig. 1).



Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

Decryption

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

Fig. 1. RSA public and private key generation algorithm.[6]

More advanced asymmetric cryptography algorithms have emerged since RSA, including the Elliptical-curve cryptography (ECC) approach.[7] ECC uses points over finite regions on an

[5] "Asymmetric Algorithms," Asymmetric Algorithms - Cryptography 2.9.dev1 Documentation.

[6] Shihab A. Shawkat, "The RSA Algorithm," ResearchGate, accessed December 2, 2019.

[7] Antonopoulos, *Mastering Bitcoin,* 60-62.

elliptical curve to define public and private key pairs. Bitcoin utilizes ECC as it requires less computing power and offers better security than RSA.

Additionally, Bitcoin implements a distributed, peer-to-peer system that eliminates the need for a central authority. Each Bitcoin transaction is broadcasted to all participants in the network for verification and logging. As a network majority consensus must be reached for a transaction to be validated, transactions made on the Bitcoin network can lead to an abundance of network traffic, limiting the maximum rate transactions can be completed. On average, only seven Bitcoin transactions can be done per second.[8]

The advent of Bitcoin introduced an unprecedented method of exchanging currency and performing transactions in a secure, efficient, and borderless manner.

III. Overview of Blockchain Technology

Blockchain technology enables digital transactions to be made in a trusted and virtually irreversible manner. Blocks consist of a bundle of exchanges that are carried out and accumulated on the network. A blockchain can be visualized as a stack of blocks that are each linked to each other.

In the Bitcoin network, participants begin creating a block by independently validating each transaction in the block against given consensus rules. Validation of the blocks themselves is done by searching for a valid proof-of-work (PoW) algorithm. A PoW algorithm consists of a

[8] "Transaction Rate," Blockchain.com, Accessed December 2, 2019.

piece of data that when hashed through the SHA256[9] cryptographic hash algorithm, corresponds to a value starting with a certain number of zero bits. A hash is a one-way function, meaning that while a hash can be generated from data, the data cannot be generated from a hash. Thus, data integrity can be effectively guaranteed. The difficulty of generating the PoW algorithm is readjusted to ensure that every ten minutes, a valid PoW is generated.

Participants also have to create the hash for the block, which will serve as a digital fingerprint to identify the block (Fig. 2). The hash is composed of three blocks of metadata. The first 32-byte block is a reference to the parent block's hash, serving as the block's linkage to the global blockchain. The second block includes the difficulty target for the PoW algorithm, the creation time for the block, and the nonce, each taking up 4 bytes. The nonce is the piece of data used to find a valid PoW that meets the difficulty target. The last component is the 32-byte Merkle tree root. This tree provides a summary of all the transactions included in the block and is generated through recursive hashing of transactions until one root hash is obtained. A binary tree is specifically used because it enables an efficient logarithmic $O(\log_2(n))$ running time of verifying data integrity for a large number of transactions.[10]

[9] Patrick Nohe, "What Is the Difference Between SHA-1, SHA-2 and SHA-256?," Hashed Out by The SSL Store™, accessed November 26, 2019.

[10] Antonopoulos, *Mastering Bitcoin,* 195-211.

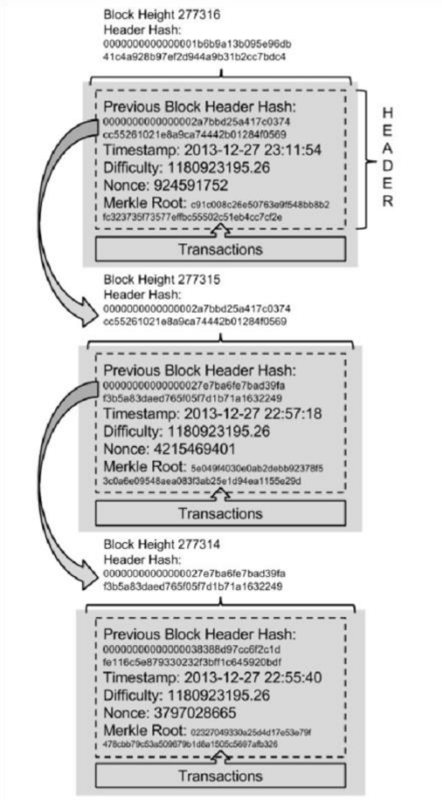

Block Height 277316
Header Hash:
000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4
Previous Block Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e
Transactions
HEADER
Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Previous Block Header Hash:
00000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d
Transactions
Block Height 277314
Header Hash:
00000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Previous Block Header Hash:
0000000000000000038388d97cc6f2c1d
fe116c5e879330232f3bff1c645920bdf
Timestamp: 2013-12-27 22:55:40
Difficulty: 1180923195.26
Nonce: 3797028665
Merkle Root: 02327049330a25d4d17e53e79f
478cbb79c53a509679b1d8a1505c5697afb326
Transactions

Fig 2. Blockchain: blocks linked together using hash in a chain.[11]

Once a participating node has successfully generated a hash of a block that meets the target through a process called “mining,” it broadcasts the block and its hash to the network. Then, the other nodes distributed across the network verify and further propagate the finished block. While validating the new block, each node adds the block to its own copy of the global blockchain and starts creating the next block. Because the nodes must include the hash of the parent block in the hash of the next candidate block, they implicitly express confirmation of the PoW of the parent block. As the block propagates through the entire network, a network wide consensus will be reached without the need for a central authority.

[11] Antonopoulos, *Blocks linked in a chain by reference to the previous block header hash*, *Mastering Bitcoin*, 201.

The stacking of blocks on top of each other, linked together by references to their parent block, makes it exponentially harder to change or manipulate any transactions already made because it would involve redoing PoWs for all blocks, which requires enormous amount of computing power. Moreover, since every node has a copy of the same blockchain, the system can only be broken if more than half of the nodes have been compromised, which is theoretically possible, but practically improbable. Thus, it can be said that blockchain's structure make the recorded history of transactions immutable, secure, and trustworthy.

IV. Current Cross-border Transaction System

Today's cross-border financial transactions must traverse through various intermediaries before it can reach the final recipient. Due to reliance on these intermediaries, the current international payment system has various weaknesses related to processing time and costs, operational risks, and lack of transparency.[12]

As the monetary value in banks involved in international payments are not usually stored on the same ledger,[13] the transaction must traverse through trusted third parties (TTPs), such as the SWIFT[14] (Society for Worldwide Interbank Financial Telecommunications) system, a global messaging platform that sends and receives instructions for money transfer, and correspondent banks,[15] who have direct access to the ledger of the foreign currency. Typically, the

[12] Bank of Canada and the Monetary Authority of Singapore, "Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies," Accenture, accessed November 26, 2019.

[13] Steven Bragg, "Ledger Account," AccountingTools, accessed November 14, 2019.

[14] Ravishankar Achanta, "Cross-Border Money Transfer Using Blockchain – Enabled by Big Data," Infosys, accessed November 11, 2019.

[15] Will Kenton, "What You Should Know About Correspondent Banks," Investopedia, accessed November 18, 2019.

correspondent bank carries out the debits and credits detailed in the SWIFT message and send the value from the sending bank to the intended receiving bank (Fig. 3).

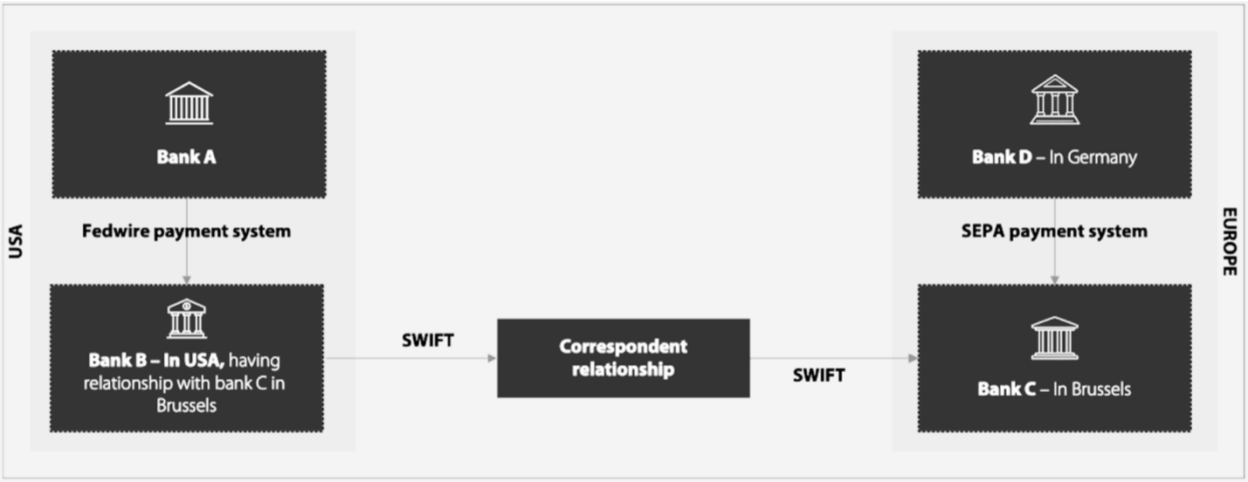


Fig. 3. Current payment flow chart for transaction between Bank A and Bank D.[16]

The weaknesses of the current international banking system are listed below:

1. Intermediaries charge hefty fees for their services. Additionally, due to operating hour differences and issues related to service availability, foreign exchange transactions typically take more than two days to settle.
2. As the actions involved in carrying out cross-border transactions are not tightly synchronized due to the presence of TTPs, there is an increased operational risk of inconsistent payment and one party gaining at the expense of another.[17]

[16] Achanta, *Payment flow chart – Bank A sending euro amount to a euro account in bank D in Germany*. "Cross-Border Money Transfer Using Blockchain – Enabled by Big Data."

[17] Xiaohang Zhang, et al, "Cross-Border Settlement Systems: Blockchain Models Involving Central Bank Money," R3, accessed November 13, 2019.

3. There have been cases where funds in an international transaction are lost along the payment chain due to the lack of real-time payment tracking, which can have serious economic consequences.

V. Applicability of Blockchain in Cross-border Transactions

Blockchain is a fitting candidate to address the existing inefficiencies in the cross-border financial systems as it enables fast, secure, and borderless transactions.

Currently, only sovereign legal currencies are accepted for financial transactions, thus, blockchain technology must be applied to legal currencies. Due to inherent differences between legal currencies and virtual currencies, a number of issues must be addressed to make blockchain suitable for implementation in cross-border transactions.

1. Cross-border financial transactions are typically not public and cannot be recorded and verified on a completely open ledger. This leads to the problem with balancing private and public aspects of international transactions. Should the ledger be centralized, allowing access only to authorized entities? Should it be completely distributed? Should it be a hybrid of both?
2. Bitcoin participants are rewarded for their engagement in verifying and recording new transactions. In the context of financial systems, how can businesses and individuals transacting across borders be incentivized to use blockchain technology?
3. Bitcoin uses computing-intensive PoW and network consensus for enhanced security. However, PoW does not produce any real value and is expensive to generate. In addition, it is theoretically possible that an adversary with an enormous amount of resources could

overwhelm the network and break the consensus rule. To prevent any possibility of this occurring in legal financial systems, more reliable mechanism must be used.

4. The Bitcoin network can only do seven transactions per second. On average, typical financial systems handle tens of thousands of transactions every second. How can the Bitcoin protocol and network be changed to allow for much higher throughput and better scalability?
5. While blockchain is built to be secure and immutable, it does not guarantee the authenticity of the participants and legality of the transactions, leading to widespread use of Bitcoin in illegal transactions. This must be prevented if blockchain is to be applied to legal financial systems.

VI. Solutions Offered by Blockchain Technology

A. Solutions to Current Problems in Cross-Border Transactions

1. On a blockchain, transactions need less than a second to settle rather than days. Moreover, the costs of transactions made on the blockchain network will be significantly lower than those charged by TTPs, which costs well above $25 per transaction.[18]
2. Blockchains can utilize smart contracts, which are executable code triggered by designated events, to address the operational risks and desynchronization of the current payment chain. A specific type of smart contract, Hash Time-Locked Contracts (HTLC),[19] can be used to guarantee the reliability and immutability of transactions. HTLC design allows for transactions to be sent directly on blockchain networks without

[18] "International Wire Transfer Fees," Veem, accessed November 14, 2019.

[19] Antonopoulos, *Mastering Bitcoin*, 296-297.

the need for intermediaries. It can manage all parts of the transaction between two systems in different countries, synchronizing actions to ensure atomicity,[20] meaning that either all parts of the transaction will happen, or none will happen. Thus, I suggest the inclusion of a framework to implement the constructs of HTLC, which includes a timeout mechanism, a method to lock the asset, and a private disclosure between parties to complete transaction acceptance, for the application of blockchain into cross-border transaction systems.

3. Blockchain addresses the lack of payment transparency associated with the current payment chain as each transaction will be broadcasted to nodes, who continuously track, validate, and update its own copy of the ledger independently. The entire history of transferred goods will be recorded and traceable.

B. Solutions to Applicability Problems of Blockchain in Cross-Border Transactions

1. Cross-border financial transactions should not be distributed in a completely open manner like Bitcoin. However, if the ledger is centralized, it becomes an easier target for adversaries to manipulate transactions and topple the system. One compromise option is to broadcast transactions only to a limited number of nodes designated by participating entities in the blockchain.

2. With blockchain, transactions can be done in a more efficient manner at a lower cost, incentivizing individuals and corporations to participate in cross-border transaction systems implementing blockchain. Additionally, transactions made on a blockchain come

[20] Bank of Canada and the Monetary Authority of Singapore, “Enabling Cross-Border High Value Transfer.”

with significantly lower business risk for transacting parties. In the current system, it is difficult to gain sufficient information of the cross-border business counterparty for an accurate assessment of risks involved. For example, as an importer typically pays after receiving goods from the exporter, the exporter is at risk and has no reliable way to confirm if the importer has sufficient funds or is willing to pay in a timely manner. One option with blockchain is to stipulate that once the importer receives a shipment, the associated smart contract will be triggered to execute the payment immediately.

3. A more reliable and efficient verification process must replace the PoW protocol and network majority rule used by Bitcoin. As transactions made in financial systems must be 100% correct, a complete network consensus should be required. Complete network consensus can also render it extremely difficult for malicious attacks as they would need to overwhelm all nodes as once. A new validation protocol can also be implemented, where each node first verifies a transaction independently, broadcasts its verification result to others, and completes the verification process only after receiving results from all others node. With a limited number of nodes, a complete consensus can be achieved efficiently. In the rare case that an anomaly is detected on the network, for instance, if not all nodes agree to the same outcome, human intervention would be called to handle the anomaly.
4. On the Bitcoin network, transactions are validated and accepted with a network wide consensus. This process is overly time-consuming for financial systems that process a much higher volume of transactions. However, if the transaction is only sent to a small

number of designated nodes and PoW is eliminated, transactions can be validated significantly faster, enabling much higher throughput.

5. The Bitcoin authentication process must be altered to render more secure transactions. Currently, public keys and associated addresses are used to authenticate Bitcoin users. However, the actual identity of the user is unknown. In financial systems, all transactions are regulated, and the legality of transacting parties must be guaranteed, mostly through offline examination of proper documents such as a business license. The obvious choice is to use a similar system when using blockchain. Public keys can still serve as the basis of authentication but would each need to be associated with the authenticated ID of a legal entity. This system, in combination with existing practices of financial institutions, can discourage illegal transactions. In addition, since the private key will not be used in any other places, the risk of malicious or unintended disclosure is low, reducing the likelihood of ID theft.

VII. Models of Implementation

As discussed above, there exists a considerable gap between theory and practice in regards to the application of blockchain into current financial systems. This section presents the various ways to harness the opportunities that blockchain offers.

A. Model 1: Direct Access

Model 1 is a faithful adoption of blockchain. It supports direct transactions between sender and receiver using one distributed ledger on a common blockchain. This model assumes that banks can access both domestic and foreign networks, and each can hold wallets in both networks. Thus, a bank can directly transfer payments to other participants in the foreign network.

This model implements a HTLC contract with hash verification and time expiration verification,[21] which follows the below sequence (Fig. 4).

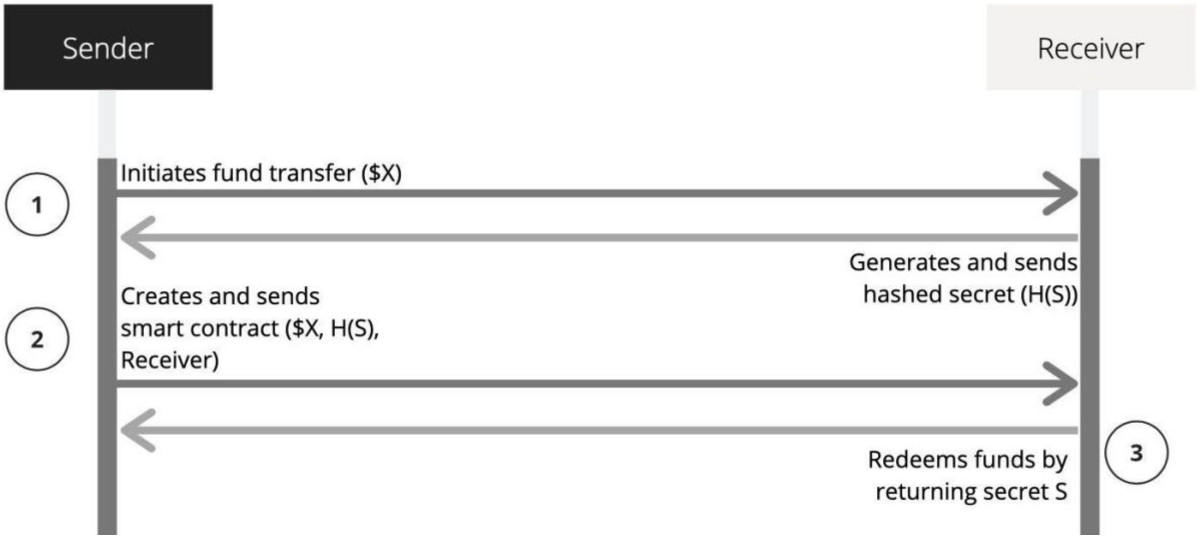
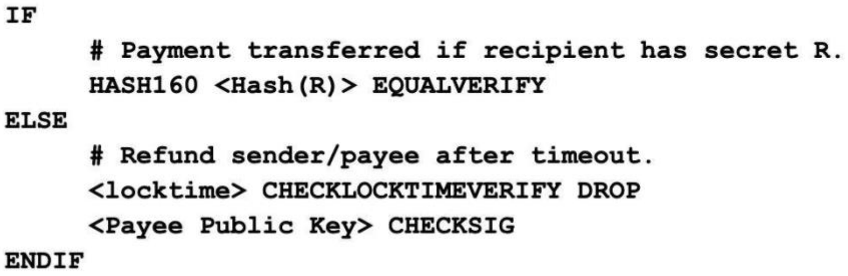

Sender
Receiver
1
Initiates fund transfer ($X)
Generates and sends hashed secret (H(S))
2
Creates and sends smart contract ($X, H(S), Receiver)
3
Redeems funds by returning secret S

Fig. 4. HTLC sequence for direct transaction made on blockchain.

1. A secret and its hash will be generated by the receiver. The secret will function as a crucial component in guaranteeing the atomicity of the transaction.
2. The sender requests the hashed secret from the receiver and creates a smart contract containing information on the receiver and amount of funds to be transacted. The sender sets a time expiration window for the transaction and includes the hashed secret in the locking script of the contract (Fig. 5). The transaction must be carried out within the time expiration window, or it will be voided.

[21] Antonopoulos, *Mastering Bitcoin*, 296-297.



```
IF
     # Payment transferred if recipient has secret R.
     HASH160 <Hash(R)> EQUALVERIFY
ELSE
     # Refund sender/payee after timeout.
     <locktime> CHECKLOCKTIMEVERIFY DROP
     <Payee Public Key> CHECKSIG
ENDIF
```

Fig. 5. Script implementing an HTLC.

3. The sender transmits the smart contract and the hashed secret to the receiver.
4. The receiver claims the funds in the smart contract by using the hashed secret to retrieve the original secret and unlock the transaction.

Model 1 eliminates the need for an intermediary, increasing the speed of transaction settlement while using HTLC to guarantee security. However, there are problems that arise from the lack of intermediaries. In the current banking system, many intermediaries are regulatory agencies upon whom governments rely on to implement regulatory safeguards.[22] Banks remain reluctant to allow transactions to bypass these third parties because with decentralization comes additional risks of disintermediation and threats to activities that banks act as a central coordinator in.[23] For instance, removing the oversight of Financial Action Task Force (FATF) rules can introduce risks of money laundering and terrorist financing into the global economy. Thus, it is crucial to provide a way to send transaction details to these agencies and conduct regulatory processes on a blockchain.

[22] Julie Maupin, "Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy," Centre for International Governance Innovation (2017), accessed October 10th, 2019.

[23] Alexis Collomb and Klara Sok, "Blockchain/Distributed Ledger Technology (DLT): What Impact on the Financial Sector?," Digiworld Economic Journal 103 (2016), accessed November 26, 2019.

B. Model 2: Additional Data Layer

Model 2 attempts to address the challenges around maintaining compliance with conservative banks by ensuring that transaction details, including the parties involved and amount transacted, are made available to regulatory agencies.

Similar to Mode1 1, Model 2 assumes that the banks involved in the transaction are on the same ledger and operate on a common blockchain. Funds can be directly transferred from the sender to the receiver once they have joined a permissioned blockchain. The HTLC sequence of this model follows the same sequence as Model 1.

However, Model 2 includes an additional data layer to be ingested in a big data environment, where the data can be transformed and provided to regulators (Fig. 6). The data layer[24] should consist of two components, one being the hashed transaction details contained in the smart contract, which would be ingested by the sending bank. The second component would be the registered details of both the sender and receiver captured when entering a transaction on the blockchain. Once both pieces of data are in the big data environment, the hashed transaction details can be transformed and joined with the registered details, enabling the extraction of transaction information.

[24] Achanta, “Cross-Border Money Transfer Using Blockchain – Enabled by Big Data.”

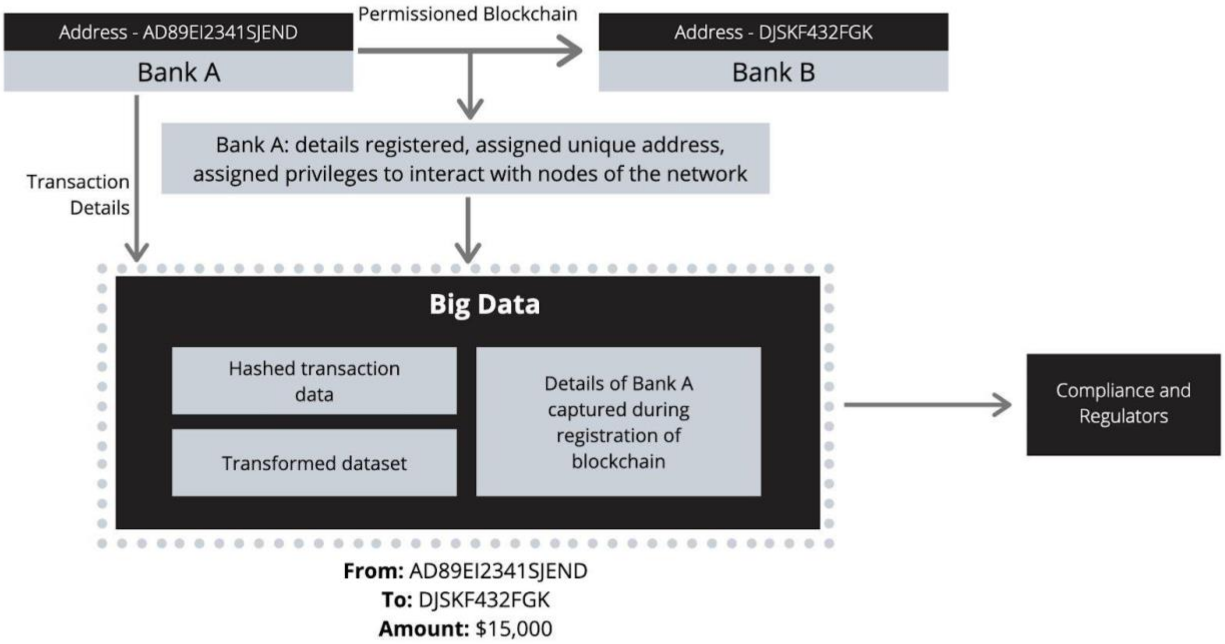

Permissioned Blockchain
Address - AD89EI2341SJEND
Bank A
Address - DJSKF432FGK
Bank B
Transaction Details
Bank A: details registered, assigned unique address, assigned privileges to interact with nodes of the network
Big Data
Hashed transaction data
Transformed dataset
Details of Bank A captured during registration of blockchain
Compliance and Regulators
From: AD89EI2341SJEND
To: DJSKF432FGK
Amount: $15,000

Fig. 6. Data layer ingested in big data environment.

The presence of a data layer is an invaluable source of information for regulatory and compliance purposes. It can increase transparency of the network, discouraging and preventing suspicious and high-risk transactions.[25]

However, Model 2 is still not feasible in the context of the current banking system. There is an inherent problem associated with both Model 1 and 2 – both require widened access to real time gross settlement (RTGS) systems, which settle payments in a continuous manner. Currently, only the central bank and a small number of domestic financial institutions who serve as intermediaries in cross-border transactions have direct access to RTGS systems in both foreign and domestic networks. Given the conservative nature of most central banks, it is unlikely that they would condone opening access to RTGS systems. Moreover, building extensive networks where banks have direct access to various foreign networks is a complex and expensive process.

[25] Achanta, “Cross-Border Money Transfer Using Blockchain – Enabled by Big Data.”

Blockchain can only be viable in a real-world context if central banks retain more control over international transactions and the networks become more scalable.

C. Model 3: Intermediary Approach

Model 3 explores the possibility of having no access to RTGS systems, which means that the sender and receiver will have to transact on different ledgers and networks.[26] In this case, intermediaries are needed to carry out international transactions involving different currencies as the sender and receiver can only operate in their own currency. The intermediary would hold wallets in both the domestic and foreign network and perform the conversion of currencies. They would also be able to conduct regulatory and compliance reporting on the transaction.

The HTLC sequence of Model 3 differs from both Model 1 and 2 because of the presence of intermediaries. Instead of being sent directly between the sender and receiver, the contract must traverse through an intermediary with a domestic and foreign counterpart.

[26] Bank of Canada and the Monetary Authority of Singapore, “Enabling Cross-Border High Value Transfer.”

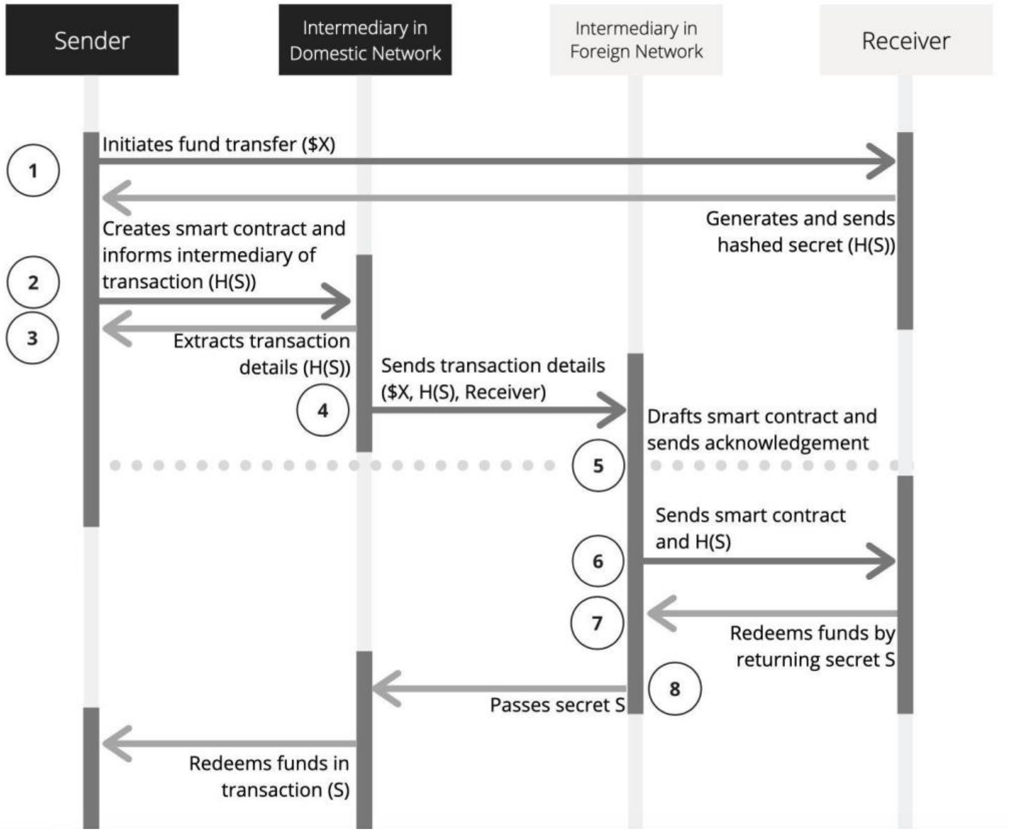

Sender
Intermediary in Domestic Network
Intermediary in Foreign Network
Receiver
1
Initiates fund transfer ($X)
Generates and sends hashed secret (H(S))
2
Creates smart contract and informs intermediary of transaction (H(S))
3
Extracts transaction details (H(S))
4
Sends transaction details ($X, H(S), Receiver)
5
Drafts smart contract and sends acknowledgement
6
Sends smart contract and H(S)
7
Redeems funds by returning secret S
8
Passes secret S
Redeems funds in transaction (S)

Fig. 7. HTLC sequence for transaction made via intermediary.

In this case, once the sender has created a smart contract encrypted by the receiver's secret, they will transmit the smart contract and the hashed secret to the intermediary. The intermediary in the domestic network would use the hashed secret to extract transaction details from the contract and send them to its counterpart in the foreign network. The intermediary in the foreign network would create a smart contract with the same receiver. Once the receiver obtains the contract, they can decrypt the transaction with the original secret. Through this process, the intermediary in the foreign network is made aware of the secret, and the intermediary in the domestic network can then use the secret to redeem the funds held by the sender's smart contract.

Although this model reintroduces an intermediary into cross-border payments, it is still more efficient and secure when compared to the current cross-border payment system. Model 3 seems to be the most plausible given the current banking situation, effectively maintaining regulatory reporting without requiring access to RTGS systems.[27]

Another variation of this model is to use a common currency backed up by a legal currency, such as Libra proposed by Facebook,[28] that would render the intermediary unnecessary. However, Libra has been heavily questioned and criticized by various governments as they are concerned with losing oversight on Libra transactions.

VIII. Conclusion

The implementation of blockchain technology can drastically improve the transparency of economic transactions and further strengthen the security of global financial systems[29] because of its ability to record, verify, and broadcast transactions in an efficient manner.

However, blockchain technology comes with certain risks that cannot be ignored. These risks relate to the issues associated with the lack of government-instituted intermediaries to monitor international transactions. On the other hand, many proponents of blockchain technology regard blockchain's ability to eliminate the need for financial intermediaries and the associated operational risks as one of its most important features.

Currently, the most plausible model of implementation is Model 3, which allows for atomic transactions between two banks operating on dissimilar blockchain networks. Model 3 has already been tested as a part of Project Jasper, initiated by the Bank of Canada, and Project

[27] Bank of Canada and the Monetary Authority of Singapore, "Enabling Cross-Border High Value Transfer."
[28] "Libra White Paper: Blockchain, Association, Reserve," Libra.org, accessed December 10, 2019.
[29] Maupin, "Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy."

Ubin, initiated by the Monetary Authority of Singapore.[30] Both PoCs aims to utilize distributed ledger technology to enable high value international transactions. The results of these projects demonstrate the technical viability of blockchain technology in a real-life scenario.

Although it is evident that more research and innovation is needed to effectively harness the key features of blockchain, the potential of blockchain technology to revolutionize the banking system and make cross-border transactions safer, faster, and more transparent should been recognized. Blockchain technology can also draw concentrated power away from large corporations and financial institutions by motivating individual banks and people to participate directly into the economy. Blockchain technology can serve as a crucial component in the effort to build a more inclusive and stronger global economy.[31]

[30] Bank of Canada and the Monetary Authority of Singapore, "Enabling Cross-Border High Value Transfer."

[31] Maupin, "Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy."

IX. Bibliography

Achanta, Ravishankar. “Cross-Border Money Transfer Using Blockchain – Enabled by Big Data.” Infosys, 2018. https://www.infosys.com/industries/cards-and-payments/resources/Documents/cross-bord er-money-transfer.pdf.

Antonopoulos, Andreas M. *Mastering Bitcoin: Programming the Open Blockchain*. Beijing: OReilly, 2018.

“Asymmetric Algorithms.” Asymmetric Algorithms - Cryptography 2.9.dev1 Documentation, 2017. Accessed December 1, 2019. https://cryptography.io/en/latest/hazmat/primitives/asymmetric/.

Bank of Canada, and the Monetary Authority of Singapore. “Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies.” Accenture. Accessed November 26, 2019. https://www.accenture.com/_acnmedia/pdf-99/accenture-cross-border-distributed-ledgertechnologies.pdf.

Bragg, Steven. “Ledger Account.” AccountingTools. Accessed November 14, 2019. https://www.accountingtools.com/articles/what-is-a-ledger-account.html.

“Bitcoin Transaction Fees.” Bitcoin Transaction Fees. Accessed November 27, 2019. https://bitcoinfees.info/.

Collomb, Alexis, and Klara Sok. “Blockchain/Distributed Ledger Technology (DLT): What Impact on the Financial Sector?” Digiworld Economic Journal 103 (2016). Accessed November 26, 2019. https://www.academia.edu/30192464/Blockchain_Distributed_Ledger_Technology_DLT_What_Impact_on_the_Financial_Sector.

“International Wire Transfer Fees.” Veem. Accessed November 14, 2019. https://www.veem.com/library/international-wire-transfer-fees-2/.

Kenton, Will. “What You Should Know About Correspondent Banks.” Investopedia. Accessed November 18, 2019. https://www.investopedia.com/terms/c/correspondent-bank.asp.

“Libra White Paper: Blockchain, Association, Reserve.” Libra.org. Accessed December 10, 2019. https://libra.org/en-US/white-paper/#introduction.

Maupin, Julie. “ Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy.” Centre for International Governance Innovation (2017). Accessed October 10th, 2019. www.jstor.org/stable/resrep05191.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” Bitcoin. Accessed November 26, 2019. https://bitcoin.org/bitcoin.pdf.

Nohe, Patrick. “What Is the Difference Between SHA-1, SHA-2 and SHA-256?” Hashed Out by The SSL Store™. Accessed November 26, 2019. https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/.

“Running A Full Node.” Bitcoin. Accessed November 27, 2019. https://bitcoin.org/en/full-node#what-is-a-full-node.

Shawkat, Shihab. “The RSA Algorithm.” ResearchGate. Accessed December 2, 2019. www.researchgate.net/figure/Figure-213-The-RSA-Algorithm_fig12_328828460.

“Transaction Rate.” Blockchain.com. Accessed December 2, 2019. www.blockchain.com/en/charts/transactions-per-second.

Zhao, Xiaohang, et al. “Cross-Border Settlement Systems: Blockchain Models Involving Central Bank Money.” R3. Accessed November 13, 2019. www.r3.com/wp-content/uploads/2018/05/CrossBorder_Settlement_Central_Bank_Mone y_R3-1.pdf.