A Blockchain-Based Approach towards Overcoming Fraud in Issuing Letter of Credit

(Hadi Sepanloo, Tehran University, Department of Public Administration & Manager of Planning Affair, Bank Mellat, h.sepanloo@bankmellat.ir)
(Vahid Esmaeili, School of Industrial Engineering, West Tehran Branch, Islamic Azad University, Engineering Campus, Tehran & Yaas Industrial Engineering Company, esmaeili.v@wtiau.ac.ir)
(Maosud Narenji*, Iran University of Science and Technology & Yaas Industrial Engineering Company, narenji@yaasie.com)

Abstract

The best method for any organization to protect themselves against a possible fraud is to ensure that they have adequate fraud prevention and detection methods in place. Organizations need to realize the growing importance of addressing/controlling the risk of fraud in a comprehensive and integrated manner, which would in turn benefit them in a number of ways. Evaluating anti-fraud programs, controls, ethical conduct and compliance with policies and procedures in the business process by assessing its vulnerability to fraud is the foundation on which effective anti-fraud processes and tools are built. A fraud detection proprietary tool, can profile and analyze financial and non-financial data across various areas and disparate systems to find anomalous relationships, transactions or unusual patterns, such as, duplicate supplier invoicing, ghost employees, altered payees, etc. This rigorous analysis can help organizations identify fraudulent activity; prioritize case management and investigation; and improve the false positive rate of a detection and prevention strategies. Blockchain technology can and will help organizations to tackle fraud in this regard. Therefore, by the five years, we will see transaction volumes and the associated profit pools shifting from intermediaries toward the owners of new highly efficient blockchain platforms. These transactions could include transferring digital or physical assets, protecting intellectual property, and verifying the chain of custody. In an era of cyber-crime and stringent regulatory requirements, a highly fraud-resistant system for protecting and authenticating almost any kind of transaction could have a revolutionary impact on the financial services industry. Therefore, in this paper, we consider the design of a mix of private blockchain/public blockchain technology which can create various metadata components, used to create a unique series number. This number will be added to a precious asset as well as the blockchain. Once the database contains sufficient data, if one cannot provide encrypted proof that he/she owns the right to that precious asset, the asset will lose its substantial value. Such blockchain-based prototype system is aimed at eliminating this type of fraud in letters of Credit (LoC) and increasing transparency regarding their flow in the banking systems. While the prototype is based on the specific context of issuing letter of credit, we discuss how it can be generalized for tracking other banking transactions.

Keywords: Blockchain, Fraud Detection, Letter of Credit

[*] Corresponding Author: Tell: +989125596647

1- Introduction

Letter of Credit (LoC) are written commitments to pay to beneficiaries on the satisfactions of certain conditions (time, place, mode of shipment, and delivery). They are considered as common payment methods for participants in different countries under various laws engaging in the international trades in the globally interconnected financial markets.

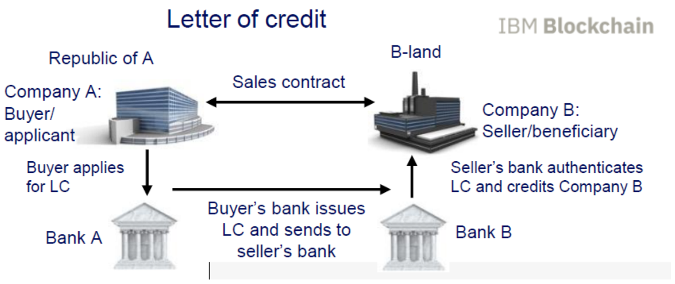

Letter of credit
IBM Blockchain
Republic of A
B-land
Sales contract
Company A: Buyer/ applicant
Company B: Seller/beneficiary
Buyer applies for LC
Seller's bank authenticates LC and credits Company B
Buyer's bank issues LC and sends to seller's bank
Bank A
Bank B

Figure ۱ - Graphical illustration of issuing LoC [17]

The applicant for the credit requests the issuing bank (usually a bank in the applicant's jurisdiction) to open a LoC in favor of the beneficiary of the credit during the trade operation. Often, the issuing bank also arranges with a confirming bank located in the jurisdiction of the seller to complete the payment to the seller. The payment is made upon the presentation by the seller to the confirming bank of certain documents identified in the LoC. They might include documents confirming title to the goods and bills of lading identifying the goods which have been transported or, in the case of a standby LoC, simply a written demand by the beneficiary without the need for any further documents. The confirming bank is itself entitled to compensation from the issuing bank upon presentation to it of the same documents. Figure 2 shows the flow of documents regarding LoCs which is an inconsistent or undocumented process, has unnecessary manual work, has limited ineffective automation of workflows and business policies, and has poor visibility of the end-to-end process.

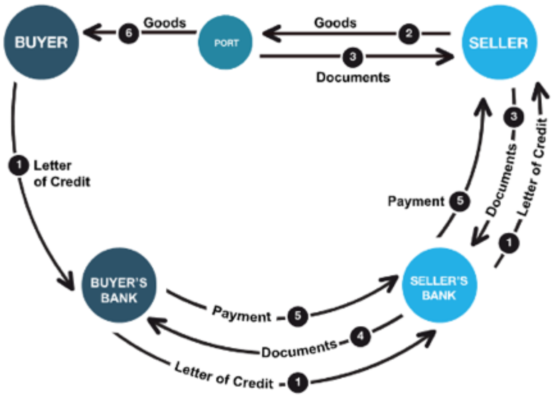


Figure 1- A Letter of Credit transaction

In this way, the obligation of both the issuing bank and confirming bank to pay is separate, and independent, from the beneficiary's obligations in its underlying contract with the seller. The banks pay strictly in accordance with the terms of the LoC and do not concern themselves with whether or not the buyer and seller have met their contractual obligations to each other. A dispute over the sale of the goods does not impinge on the effectiveness of the LoC and there are usually payment disagreements due to contractual ambiguities. Actually, according to Industry estimates, four out of five LoC documents contain inaccuracies, errors, and discrepancies. The payment are delayed mostly because of data errors in the Contract. Additionally, 70% of LC documents are rejected on their first presentation (iccwbo.org). LoC modifications increase costs and overhead and the average time for issuing LoCs is seven to ten days (letterofcredit.biz).

Consequently, LoCs in general have not been coupled with an infrastructure enabling the guarantee of the contractual terms between trade participants. As a result of this lack of systematic information ex- change, several banks have fallen victim to criminal actors submitting fraudulent LoC applications. One example is the fraud happened in LoCs issuing between Saderat bank and Melli bank (as the main confirming bank).

Therefore, LoCs in general have not been coupled with an infrastructure enabling the guarantee of the contractual terms between trade participants. As a result of this lack of systematic information ex- change, several banks have fallen victim to criminal actors submitting fraudulent LoC applications. One example is the fraud happened in LoCs issuing between Saderat bank and Melli bank (as the main confirming bank) which suffered an estimated loss of 1 billion USD in 2011-2012 in Iran. The loophole in the LoC approval process can arguably be characterized as a transparency problem, enabled by the sole reliance on local and stand-alone registry systems. In essence, it is a system that provides neither the transactional nor geographical proof required to make an informed decision on the applicant's entitlement to trade credits.

Currently there is no central information system dedicated to managing the flow of information between involved parties in order to reliably check an applicant's pledge to the LoC. Thus, in order to deal with the transparency problem, authorities could implement a new database that would offer support for managing international LoC tracking. In light of the blockchain applicability analysis framework [5], we assume this transparency problem presents a viable use case for a blockchain database. The current absence of an alternative system to track the questionable cross-border credit flow substantially increases the feasibility of a blockchain-based solution, because the common reservations regarding legacy systems (i.e., the trade-off between running outdated maintenance intensive systems and the expensive implementation of a new system) would not apply [10] in this case. Furthermore, its technologically open qualities and general pervasiveness (extending from backend database systems through business logic entities, up to organizational layers) [5], make blockchain technology well-suited as a comprehensive solution to transparency as well as building and integrating a traditional database system. Due to its immutable log of historical transactions, a private permissioned blockchain system as a distributed ledger technology could offer a viable solution for auditing purposes [5]. Furthermore, properly coded blockchain-based transactions on blockchain platforms have been shown to be potentially transparent. Finally, since smart contract execution reduces the required amount of external intervention (e.g., manually triggering token transfers along the credit dissemination process), blockchain could minimize expenses.

Thus, in this study we strive to investigate the suitability of using blockchain technology – as opposed to a traditional database system – for overcoming the loophole in issuing LoCs described above. Therefore, we follow a design science approach aimed at developing and evaluating a prototype for a blockchain-based solution that allows the LoC flow to be traced. The prototype is designed to assist in verifying the current practical approval deficiencies by also facilitating the informational exchange between banks and authorities. In general, this study investigates whether and how a blockchain-based system could improve the exchange of information in the banking sector for the purpose of eliminating fraud.

As such, we provide practical evidence for the potential of blockchain technology in overcoming current issues. Furthermore, this research also pertains to the more general context of banking industry systems. The remainder of the paper is structured as follows. In section 2, we briefly introduce the core blockchain features and related elements that are relevant to eliminating fraud in

LoCs issuance. In section 3, we discuss the application of blockchain in trade finance and LoC issuance. Section 4 explains the design science process and decisions as well as the artifact that we built. Finally, section 5 offers the conclusions reached by our study.

2- Related Blockchain Properties

We decided to use a blockchain-based approach, because blockchain offers several features that are particularly useful for overcoming the issue of LoCs described above.

Blockchain is an emerging technology which was originally used to implement cryptocurrencies (Nakamoto, 2008). While blockchain has become known as the technology behind Bitcoin, it is not limited to financial exchanges; rather, it can be used for transactions in general without involving an intermediary. Examples of potential application areas pertain to digital assets, marketplaces, notary services [9], supply chain information [9], and energy [14] and healthcare sectors [13]. While it is often claimed that it is a technology with substantial disruptive economic potential, the design science approach from [16] constitutes the first scientific approach modeling potential economic implications of these systems, and the case study by [15] is the first academically published analysis on how incumbent organizations such as banks deal with innovation related to blockchain.

Many blockchain systems support transferable tokens, either as an inherent feature or implementable in higher level scripting or programming languages [5]. In the original case, these tokens are treated as a coin to be transferred between nodes [8]. In the meantime tokens have expanded from being conceived of as a simple coin to becoming a representation of property, utility, or rewards
LeBeau, 2017). Tokens have distinct properties depending on their purposes. Therefore, different blockchain platforms host different tokens [4].

Smart contracts manage tokens that represent, for example, the account balance of a particular user address stored on the blockchain. When transferring tokens, smart contracts enter the appropriate number of tokens into a local database containing information on the amount and the user address [1]. This process is systematically equivalent to transferring funds into a bank account. Ultimately, these tokens can be maintained autonomously by the rules specified in the smart contract.

- **Blockchain is distributed**

A blockchain is a type of distributed digital ledger containing transaction data that is shared across a peer-to-peer network and continually reconciled. Each node in the network contributes to verifying the transactions and sends information about them to the other nodes via their public key. Nodes identify each other by the IP address, while users reference each other via their public keys [6].

In the context of this study, every acting unit (e.g. intermediary banking organization) is an individual user, and some users also act as nodes.

- **Blockchain is immutable**

Transactions recorded on blockchain are immutable because they cannot be deleted or changed. Before a “block” of transactions can be appended to the blockchain, network participants must agree the transaction is valid through a process called consensus. Rather than being stored in a database on a central server, a copy of the data exists on each node participating in the blockchain (Yli-Huumo et al., 2016). Each block in a blockchain contains a link to the previous block in the chain, a proof-of-work element, and a listing of one or more transactions. The link to the previous block is encrypted by using a hash function for the transaction part of the previous block [6]. So, by using blockchain you can see the provenance of an asset, including where it came from, where it’s been, and who’s had ownership of it.

When transactions are broadcast to the network of nodes, each node competes to try to complete the block containing the transactions. Once the node has solved the hash – i.e., found the proof-of-work

– it broadcasts the finished block to the other nodes, after which point that block cannot be changed without re-computing the proof-of-work for that block and for every successor.

Counterfeiting is a global problem that affects a wide range of industries such as luxury goods, clothing, food products, pharmaceuticals and more. Proving or disproving the authenticity and quality of an asset can be a challenge because traditional supply chains are long, complex and lack transparency. However, if a producer or manufacturer's goods are placed on blockchain, those goods will have provenance due to their immutable transaction history, and that will make it difficult to pass off fake products as real.

- **Blockchain can be permissioned**

Businesses deal with a lot of confidential data; they can't let just anyone have access to it. There must be some way to ensure outsiders can't get in to the network and insiders can't corrupt the records. This is where permissions come into play. But unlike the previous features previously discussed, not all blockchain networks are permissioned. However, permissioned networks can be great for fraud prevention because they restrict who is allowed to participate and in what capacity. Members of a permissioned network must be invited and validated before they can contribute.

- **Blockchain against fraud**

As one of the top operational risks of 2017, fraud isn't a problem organizations can ignore. In addition to being costly, it can decrease employee morale and create an unstable business environment as well as undermine the business and consumer relationships. Blockchain technology can be used to take a stand against fraud in banking industry and their business network.

There are several methods fraudsters use to conceal their criminal activities, including altering or deleting information in a company's accounting systems, changing electronic or paper documents and creating fraudulent files. Using a shared digital ledger can help reduce fraud because it increases the visibility and transparency of the transactions made throughout a supply chain and between members of a business network. Participants can see the history and transfer of assets, so fraudulent transactions are easier to identify. There is no central administrator or centralized version, so there is no single point of failure. Instead, management and authorization is spread across the network, so there is no obvious place for someone to instigate a fraud scheme. In the original conceptualization of blockchain (e.g., in Bitcoin), any transaction is visible to all participants, thus providing maximum transparency and replicability of transactions (Tschorsch & Scheuermann, 2015). Plus, to tamper with the transaction records on a blockchain, an individual or group of individuals in collusion would have to control a majority of the system.

According to a study by the Association of Certified Fraud Examiners, a typical organization loses five percent of revenues to fraud each year (acfe.com). Unfortunately, fraud in a business can go undetected for a long time and is often hard to uncover. The following three features of blockchain can help make business networks less susceptible to fraud.

3- Using blockchain for streamlining trade finance and issuing letter of credits

Trade finance is the process, by which importers and exporters mitigate trade risk through the use of financial institutions that serve as trusted intermediaries that provide assurance to sellers (in the event the buyer doesn't pay) and contract certainty to buyers (in the event that goods are not received). Conventional banking systems associated with cross-border trade are characterized by 'correspondent banking'; where a financial institution conducts business transactions, accepts deposits and gathers documents on behalf of another financial institution. Payment and delivery terms are documented in a letter of credit or open account contract vehicle, and the financial institutions receive fees for assuming risks, as well as for documentation and oversight of payment terms. About 80% of trade is supported by some sort of finance, with letters of credit facilitating 47% of global trade finance. This percentage adds up to $2.8 trillion per year worldwide. Yet, correspondent banking is a chain of links and, by its very nature, prone to some problems in completing transactions and lacks end-to-end visibility in a series of transactions. Banks have to pre-fund their accounts held at the correspondent banks; liquidity costs directly affects their working capital which represents their operating liquidity. In summary, multiple data formats, too many peer-to-peer interactions, absence of a messaging standard, and lack of real-time information makes it hard to approve these LoCs and many frauds can stem from these data challenges or result in error-prone or incomplete/inconsistent information, delays, and lack of visibility.

Having blockchain in the network makes a difference with key characteristics such as Consensus (all ledgers in the network are synchronized and all agree to the time and amount of a transaction), Provenance (there are records for the place of each asset), Immutability (anything written on the ledger cannot be undone, and finality (anything written in the blockchain cannot be disputed). The decentralized aspect of a blockchain also mitigates the potential of a monopoly. We are, nonetheless, a long way off solutions based on the blockchain technology being offered worldwide to disrupt the banking sector’s business model for trade finance. McKinsey & Company (2015) mentions: “it will take time for banks to achieve universal reach in destination and currencies, resolve compliance questions, and equip themselves to handle the high-volume payments required for international trade” [7] recognizes that “tokens of payment value” featured in the blockchain-based trade finance mechanism “enable real-time messaging and clearing within a cryptographically secure and resilient environment”; however, he asserts that bank-to-bank real-time settlement by means of the direct exchange of such tokens “remains a challenge, requiring commercial and central bank money to honor”.

In this regard, McKinsey & Company (2015) also points out that solutions leveraging the power of blockchain technology “still require banks to make correspondent-like agreements to define the right and obligations of participants” in the settlement systems, thus implying that “existing correspondent banking relationships” would remain in an era of blockchain technologies.

Blockchain would be the solution to the mentioned problems since such a system could enable the transfer of value without requiring that capital be placed into a corresponding bank. Banking institutions would bear no cost for transaction fee, transfer funds in seconds instead of days, and ensure the visibility of their all transaction processes.

Blockchain could eliminate inefficiencies that limit the value of the LoCs. This is where smart contract comes in to play as it “codifies the terms and conditions of trade by abstracting and expressing conditional clauses as separate, independent or interdependent functions that provide pass/fail outputs based on the [exporter/seller’s] input information” [18].

Blockchain introduces timely, accurate process performance. By using a distributed ledger as the underlying system of record, all participants can achieve significant business process improvements which is illustrated in Figure 3. All transactions are authorized, documents are sent and every action is visible through the blockchain technology. Participants retrieve documents and update information on the ledger, and react to events when others submit documents.

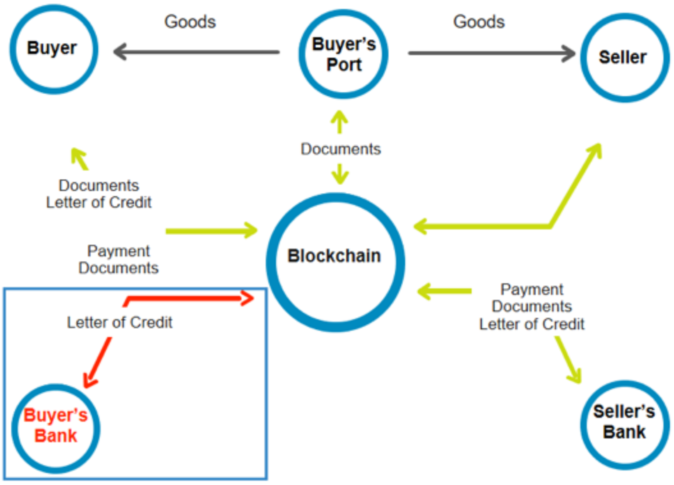


Figure 2- A Letter of Credit transaction by using blockchain technology

4- Fraud prevention using Blockchain in issuing letter of credits

The aforementioned blockchain properties assist in overcoming the problems in LoC issuance in several ways. The core capacity of blockchains to manage transactions is essential for our approach to preventing fraud. In the context of electronic payment systems regarding LoC issuance, fraud occurs when files are manipulated or account takeover happens. Since the earlier days of Bitcoin, several improvements have been implemented in blockchain systems to further ensure the transparency and publicity. In the case presented in this paper, the fraud problem arises from a lack of monitoring and information rather than a technical failure. Implementing the process on a blockchain would ensure that no such situations can occur, and that the smart contract is traceable according to the terms of trade. In order to conduct and track payments on the blockchain, tokens can be used to represent the value originally transferred from the buyer to the seller. Thus, the system tokens would receive official value backing comparable to traditional binding forms.

Managing this token dissemination process definitively necessitates trust in the token issuing (the buyer bank) and refunding institutions (the seller bank). The design solution that this paper seeks is a smart contract that maps payments due to automated execution of smart contract algorithms. Blockchain is often credited with the ability to decentralize control through its consensus mechanism between the participating nodes in the system [12]. While this holds true for the autonomously operating smart contract itself, the decentralization of control ends at the boundaries to the issuing bank system, which exchanges the system token into a valuable currency. While one could imagine a scenario in which an entire economic ecosystem being integrated into this blockchain system, the chances of such an evolution occurring seem unrealistic. Thus, while a smart contract is decentralized and autonomous, the integration into existing payment processes guarantees value only if trust exists among the involved institutions.

The cryptographically linked transaction log makes the blockchain resistant to manipulation [2]. This immutability of logs proposes a blockchain system as a paramount solution for auditing purposes, as is necessary in the case of LoC issuance. In blockchain-related environments particular measures often must be undertaken in order to guarantee data privacy of users [3]. Thus, this environment would require a permissioned blockchain, where only a specific set of permissioned users (according to figure 3) can see and validate transactions. In this case, privacy issues would not be a problem.

In sum, we assume that a blockchain-based solution is technically as well as legally feasible and offers some key advantages compared to a traditional central database system for solving LoC issues.

Technical feasibility becomes apparent in light of the blockchain applicability analysis framework (Glaser, 2017). Accordingly, a blockchain-based solution is applicable since the trade environment represents a collaborative market requiring commercial value to be linked through trusted interfaces to provide a service. Considering the aforementioned advances of blockchain, it seems that legal constraints regarding, for example, data privacy can be accommodated by blockchain systems. The pervasive structure of blockchain databases offers a comprehensive solution that is easily accessible for end users and can be rapidly integrated into existing banking systems. Moreover, smart contract execution requires very limited external and manual involvement, which suggests that a blockchain system may be more efficient compared to traditional database systems. Finally, the immutable log of past transactions constitutes an irrefutable advantage of blockchain databases over traditional counterparts for auditing purposes. It is important that the banking regulators have the ability to track value entitlements in order to prevent banks and individuals from paying or receiving fraudulent or otherwise erroneous claims. In a traditional database, banks can report having issued any amount of LoC at any point along the trade process with no simple way of formally real-time and online tracing whether it has actually been issued correctly and legally. In the case of discrepancies between issued LoC and the trade contract, it would require quite a lot of effort to retrace the global inter-organizational flow of payments in the case of fraudulent or erroneous reports in order to identify the source of the error, instantaneously. Blockchain, however, enables the transparency and traceability of transactions throughout the trade chain from the point of payment to the final recipient.

4-1- The Design Process

In terms of design science, the fraud that occurs when issuing LoC is a typical ”wicked problem” since (1) it may only be possible to find a solution to the problem that is ”good enough”, rather than solving it completely; (2) the solution to the problem will be good-or-bad rather than true-or-false; (3) testing the solution is complicated and depends on several contributing actors; (4) the possibility to learn by trial-and-error is limited as every attempt at testing the solution is complicated and resource intensive; and (5) the problem does not have an exhaustively describable set of potential solutions or a set of well-described permissible operations.
We therefore chose the ad hoc development approach by first learning about the problem and then designing a draft, which we concurrently and conclusively evaluated. Therefore, our design process follows the DSRM Process Model introduced by [11], see Figure 4.

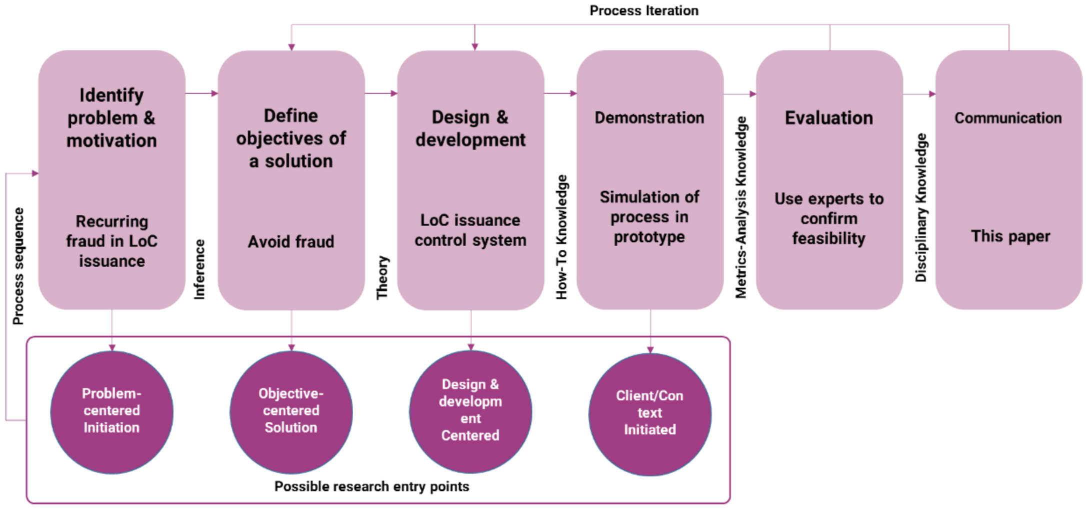

Process Iteration
Identify problem & motivation
Recurring fraud in LoC issuance
Define objectives of a solution
Avoid fraud
Design & development
LoC issuance control system
Demonstration
Simulation of process in prototype
Evaluation
Use experts to confirm feasibility
Communication
This paper
Process sequence
Inference
Theory
How-To Knowledge
Metrics-Analysis Knowledge
Disciplinary Knowledge
Problem-centered Initiation
Objective-centered Solution
Design & developm ent Centered
Client/Con text Initiated
Possible research entry points

Figure 3- The Design Science Research Process (Peffers et al., 2007)

In our case, the research entry point was problem-centered initiated; the aforementioned LoC fraud happened in Iran which could be avoided by designing an artifact to facilitate reliable tracking of LoC payments internal and international cross-institutional informational exchange. Based on the understanding of the problem, we considered the LoC issuance system described in section 3 which is not yet prototyped in the demonstration phase.

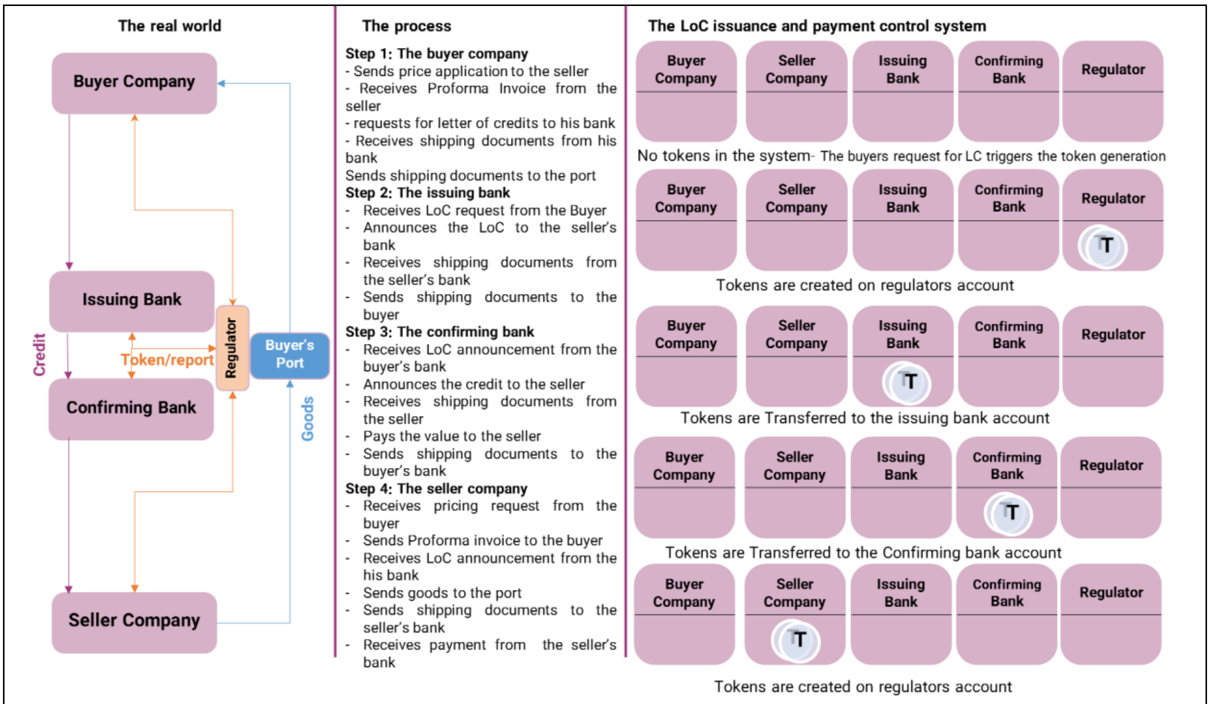
4-2- The Design Decisions

The first step in our design process was to establish the requirements for an improved LoC issuance system. The most important claim was to solve the fraud problem, which was one of the main reasons for the dissatisfactions with the current process. The other important requirements were related to ease of use by different actors involved with the process. The system should not introduce major changes in the roles traders, the financial institutions, or stockholders.

Blockchain was chosen as the underlying technology as it supports multiple information contributors, guarantees immutability of transaction records, and ensures the prevention of fraud. The smart contracts deploying on blockchain-based platforms enables us to implement a strongly automated token distributing system correspondent with the structure of the payments. Thereby, the system facilitates tracing the flow of value (tokens) and the exchange of supplementary documents.

Due to the exploratory nature of this project, we decided to focus on employing a functional payment representation on the blockchain that could subsequently be expanded to more elements and actors. For an ultimately comprehensive system, the foreign authorities would also be included on the blockchain as actors enabling them to confirm the LoC applicant and to access information regarding the applicant’s trade income for tax purposes. Thereby, the blockchain-based solution would facilitate the data exchange between authorities in order to improve the informational deficiencies occurring in the current system.

Our primary goal concerning the evaluation was to assess whether the artifact provides a feasible alternative to the current system by solving the LoC fraud problem. The evaluation therefore focuses on uncertainty and risk reduction from both a technical (i.e., is the solution feasible and reliable?) and social (i.e., will the system be convenient enough for the users?) standpoint. The properties our evaluation focuses on are actual effectiveness, actual efficiency, perceived usefulness and – to some extent – perceived ease of use.


The real world
Buyer Company
Issuing Bank
Credit
Token/report
Regulator
Buyer's Port
Goods
Confirming Bank
Seller Company
The LoC issuance and payment control system
Buyer Company
Seller Company
Issuing Bank
Confirming Bank
Regulator
No tokens in the system- The buyers request for LC triggers the token generation
T
Tokens are created on regulators account
Tokens are Transferred to the issuing bank account
Tokens are Transferred to the Confirming bank account
Tokens are created on regulators account

The process

Step 1: The buyer company

- Sends price application to the seller
- Receives Proforma Invoice from the seller
- requests for letter of credits to his bank
- Receives shipping documents from his bank

Sends shipping documents to the port

Step 2: The issuing bank

- Receives LoC request from the Buyer
- Announces the LoC to the seller's bank
- Receives shipping documents from the seller's bank
- Sends shipping documents to the buyer

Step 3: The confirming bank

- Receives LoC announcement from the buyer's bank
- Announces the credit to the seller
- Receives shipping documents from the seller
- Pays the value to the seller
- Sends shipping documents to the buyer's bank

Step 4: The seller company

- Receives pricing request from the buyer
- Sends Proforma invoice to the buyer
- Receives LoC announcement from the his bank
- Sends goods to the port
- Sends shipping documents to the seller's bank
- Receives payment from the seller's bank

Figure 4- The tokenized LoC issuance system

5- Conclusion

This study evaluates the feasibility of a blockchain-based solution to overcome LoC fraud as compared to traditional database systems. As such, we provide a blockchain-based design that enables tracking payments from the issuer to the final recipient in order to overcome the issue of fraud and the lack of transparency and information available to the authorities. Although the developed system is not designed to be rolled out across authorities in different countries, it demonstrates a feasible solution to LoC fraud, reduces the possibility of fraudulent contractual applications, and automatizes a great part of the work previously conducted manually. While the investigated use case is limited to credit and contractual fraud, we assume that an adapted solution of our designed system could also be useful for avoiding fraud in other intermediary banking systems (i.e., bank transaction and account managing systems) that companies utilize for various services. The designed system facilitates real-time fraud detection, whereby irregularities in transactions are captured on the corresponding transactions in the chain. It can simplify and improve efficiencies in the trade process and digitizes the workflow process across the transacting entities and increases transparency, and can reduce the effort required throughout the letter of credit lifecycle.

References

[1] Ahmed, K., Miller, A., Shi, E., & Wen, Z. (2016). The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts. *IEEE.*

[2] Arthur, G., Karame, G., & Wu, K. (2016). On the Security and Performance of Proof of Work Blockchains. . *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications.*

[3] Benjamin, F., Ermakova, T., & Sande, U. (2016). Anonymity in Bitcoin? The Users? Perspective. . *24th European Conference on Information Systems (ECIS 2016).* Istanbul, Turkey.

[4] Ethplorer. (2017). *Top 50 Ethereum Tokens for 90 Days*. Retrieved from https://ethplorer.io/top. Accessed 21-July- 2017

[5] Florian, G. (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Anal- ysis. . *In Proceedings of the 50th Hawaii Inter- national Conference on System Sciences (HICSS 2017).* Waikoloa Village.

[6] Florian, T., & Scheuermann, B. (2015). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials,, 18.*

[7] Higginson, M. (2016). *How Blockchain Could Disrupt Cross-Border Payments,* . McKinsey & Company.

[8] Jesse, Y.-H., Ko, D., & Choi, S. (2016). Where Is Current Research on Blockchain Technology? A Systematic Review. *PloS one, 11*(10).

[9] Kari, K., Hallikas, J., & Dahlberg, T. (2017). Digital Supply Chain Transformation toward Blockchain Integration. *50th Hawaii International Conference on System Sciences.*

[10] Keith, B. (1995). Legacy Systems: Coping with Success., 12(1):. *12*(1), 19–23.

[11] Ken, P., Tuunanen, T., & Rothen, M. (2007). A design science research methodology for information systems research. *Journal of management information systems, , 24*(3), 45–77.

[12] Marc, P. (2016). *Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations.*

[13] Matthias, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. In e-Health Networking, Applications and Services. *IEEE 18th International Conference.*

[14] Nurzhan Zhumabekuly, A., & Svetinovic, D. (2016). Security and Privacy in Decentral- ized Energy Trading Through Multi-signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing.*

[15] Roman, B., & Muller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. *50th Hawaii International Conference on System Sciences (HICSS 2017).* Waikoloa Village, Hawaii, USA.

[16] Roman, B., & Stenum Czepluch, J. (2016). Blockchain–The Gateway to Trust-free Cryptographic Transactions . *24th European Conference on Information Systems (ECIS 2016).* Istanbul, Turkey.

[17] Tennenbaum, J. (2016). *Blockchain Practical Usage around the World.* IBM Corporation.

[18] Varghese, L., & Goyal, R. (2017). *Blockchain for Trade Finance: Payment Method Automation.* Cognizant.