Blockchain-based Risk Mitigation for Invoice Financing

Meriem Guerar, Luca Verderame, Alessio Merlo
DIBRIS - University of Genoa
Genoa, Italy
name.surname@unige.it

Mauro Migliardi
DEI - University of Padua
Padua, Italy
mauro.migliardi@unipd.it

ABSTRACT

The market for *invoice financing* has been steadily growing in the last few years and has been the third financing market in size in 2016. Most solutions in this field are based on private platforms and even the new proposals based on blockchain are mostly adopting a private, permissioned blockchain. In this paper, we propose an idea based on a public blockchain that allows both fully open and group-restricted auctioning of invoices. Furthermore, our proposal introduces a reputation system that is based on the past behavior of entities, as it is photographed by the public blockchain, to allow insurance companies modulate the cost of the insurance contracts they offer. This combination guarantees the complete transparency and tamperproof-ness of a public blockchain, while it allows reducing insurance costs and fraud possibilities.

CCS CONCEPTS

• **Security and privacy → Database and storage security**; **Database activity monitoring**.

KEYWORDS

Blockchain, Ethereum, Smart contract, Auction, Invoice factoring, IPFS

ACM Reference Format:
Meriem Guerar, Luca Verderame, Alessio Merlo and Mauro Migliardi. 2019. Blockchain-based Risk Mitigation for Invoice Financing. In *23rd International Database Engineering & Applications Symposium (IDEAS'19), June 10–12, 2019, Athens, Greece.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3331076.3331093

1 INTRODUCTION

Companies work hard to ensure economic liquidity and maintain steady cash-flow, that said, those important factors are seriously affected by the long invoicing due dates which represent a big challenge, especially for small to medium enterprises (SMEs). In order to overcome this issue companies make use of different forms of invoice financing such as factoring. This type of financing enables businesses to cash-in invoices before their due date. The process of factoring can be described as follows: an SME sells the invoice to a factoring company which is often a financial institution for a pre-agreed percentage of the invoice amount, the buyer then pays the factoring company the full invoice amount on the due date. While this helps the SME solve the cash-flow issues, it exposes the factoring companies to serious fraud risks mainly because of the lack of communication among themselves. In fact, a well known fraud risk in factoring is double financing, where the SME sells the same invoice to more than one financial institution. The buyer will naturally pay the invoice once, paying only one institution and leaving the rest unpaid. Another considerable risk is represented by a situation where the buyer refuses to pay as agreed on the due date of the invoice. One of the main reasons that leads to this is the fact that a financial institution does not have a direct relationship with the buyer and relies only on the information provided by the seller, in our example the SME.

One potential solution to the double financing problem is an invoice financing platform hosted on a centralized database where all the potential invoice-buyers can verify whether the invoice has been already funded or is still available. However, centralized systems can be expensive, they are a single point of failure, and they are prone to privacy infringement, data manipulation and attacks which may make them unreliable and untrustworthy. Luckily, with the emergence of blockchain technology and smart contracts, we no longer have to rely on centralized systems. Blockchain may be used to implement an immutable, trusted, and decentralized ledger [6] that relies on a consensus algorithm to decide which data is appended [13].

In this paper, we propose an invoice financing solution through auctioning based on InterPlanetary File System (IPFS) [2] and Ethereum blockchain [16]. The invoice data is stored on the IPFS while its corresponding IPFS hash is stored into a blockchain smart contract in order to ensure integrity, traceability and authenticity of the invoice. Moreover, the proposed solution uses a reputation system which contributes to reduce the fraud risks. The rest of this paper is structured as follows: In Section 2 we introduce the invoice financing solution; in Section 3 we describe the frauds scenario and countermeasures; in Section 4 we present related work. Finally, Section 5 concludes this paper.

2 THE PROPOSED INVOICE FINANCING SOLUTION

2.1 System overview

In this paper, we propose a prototype of an invoice financing platform for SME based on InterPlanary File System (i.e., IPFS), reputation profiles, and smart contracts hosted on Ethereum blockchain. Every function call that modifies the blockchain state or smart contract executed on the Ethereum blockchain requires Gas [1]. Gas is a unit that is used to calculate the amount of fees that need to be paid to the network in order to execute an operation. Since the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
IDEAS'19, June 10–12, 2019, Athens, Greece
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6249-8/19/06…$15.00
https://doi.org/10.1145/3331076.3331093

invoice data are very sensitive and storing this data directly in the blockchain is very expensive, we do not plan to store the whole invoice inside the blockchain. On the contrary, we propose to use IPFS to store these data in a decentralized, distributed manner that is publicly and globally accessible through the use of IPFS hashes. At the same time, to control access to the data, we encrypt the IPFS hash with the authorized investors public keys and store only these into a smart contract. Thus, any modification of the invoice content would change the IPFS hash, and would then not match the hash stored within the smart contract. The confidentiality of invoice data is ensured because only the authorized investors will be able to access it using their private keys.

The main components of our platform are:

- a smart contract hosted on the Ethereum blockchain,
- the Ethereum client,
- IPFS,
- a web app.

The web app provides a graphical user interface for the Ethereum client, which in turn interacts with the smart contract on the Ethereum blockchain. The roles of the participants can be summarized as follows:

Seller: is a company that has the goods to be packaged and transferred to the buyer and it is looking to improve its cash flow by creating a smart contract capable of selling the invoice to one of the investors enrolled in the platform through an auction. This kind of company is usually an SME.

Buyer: is a company that would like to purchase the goods from the seller by paying the shipping amount on delivery and benefits from the delayed payment of the full invoice amount (i.e., the price of goods plus taxes).

Authorized investor: is a person or a financial institution that is allowed to participate in the auction to buy the invoice at a price lower than its real value to gain a profit.

Insurance: is responsible to reimburse the authorized investor in case the buyer refuses to pay.

Unlike the traditional financing model, our platform does not limit the factoring service to banks and financial companies. Any investor can subscribe to the web app and make an offer to participate in the auction of an invoice. The highest offer made by an authorized investor that satisfies the minimum requested amount wins the auction once the bidding time has expired. This enables the SMEs to invite a large number of investors around the world and get the best financing offer in short time and with less effort to get funding.

At the same time, the buyer will benefit from the delayed invoice payment to optimize the use of their working capital.

2.2 Challenges

Since the investors do not have any direct knowledge of either the seller or the buyer, they are exposed to a considerable amount of risk. As an example, there is the risk of the invoice not being paid as agreed by the buyer; another significant risk is the seller knowingly submitting false, modified or duplicate invoices with the intent to commit a fraud, either acting alone or in collusion with the buyer. A solution might be to add risk insurance to refund the investor; however, in the absence of significant countermeasures aiming at reducing the fraud opportunity, the cost of such an insurance will make the whole operation economically unfeasible. Hence, the simple addition of an insurance is not considered a viable solution.

2.3 System design

The proposed platform mitigates these risks by adding transporter entity and reputation profile. The former provides information about shipping status while the latter shows the list of invoices that has been paid or unpaid by the buyer on the due date without showing the confidential data. This can help investors in the selection of trustworthy counterparts while pushing malicious buyers off the system.

The platform allows the seller and their counterparts to register by selecting the account type (e.g., seller account, investor account, etc) and providing an identity certificate which is unique to make sure that they can not create another account with a clean reputation profile in case of fraud. The services are provided according to the type of the account and every time the contract data changes, a notification is sent to the counterpart.

As shown in Figure 1, the seller writes the invoice data into IPFS and creates a smart contract that specifies the minimum amount required to participate in the auction and the hash to retrieve the invoice from IPFS. Then, he deploys it into the Ethereum blockchain. If the invoice is genuine, the buyer accepts the invoice and pays the shipping amount. When he accepts the invoice the buyer states that he verified all the information mentioned in the invoice and he agreed to pay the shipping amount immediately and the entire amount on the due date as specified in the invoice. Afterward, the investors can participate in the auction and thus read the invoice data and make an offer after checking the following conditions:

- the invoice has been accepted by the buyer;
- the "invoice ID" has not been submitted before;
- the buyer confirmed the delivery in order;
- the reputation profiles of both the seller and the buyer show that they are trustworthy.

If the reputation profile shows that one of them is untrustworthy or the invoice does not meet one of the above mentioned requirements, then it will not be funded by the investors. An investor that decides to finance an invoice in spite of the above mentioned problems is fully responsible of his decision and knows that, in case of fraud, his request of refund will be rejected by the insurance. Beside protection against double financing and submitting false or modified invoice, our platform mitigates the risk of a buyer that does not pay as agreed. In fact, in our platform the reputation profile will show that a buyer is untrustworthy and investor may freely take a fully informed decision if they want to run the risk. Thus, our platform facilitates the invoice financing for SME and reduces the risk of frauds.

2.4 The proposed invoice financing workflow

Figure 2 illustrates the message sequence diagram of selling the invoice through an auction with two possible scenarios. In the first scenario the buyer pays on due date of the invoice while in the second the buyer refuses to pay. The interactions between the different entities with the smart contract are as follows:

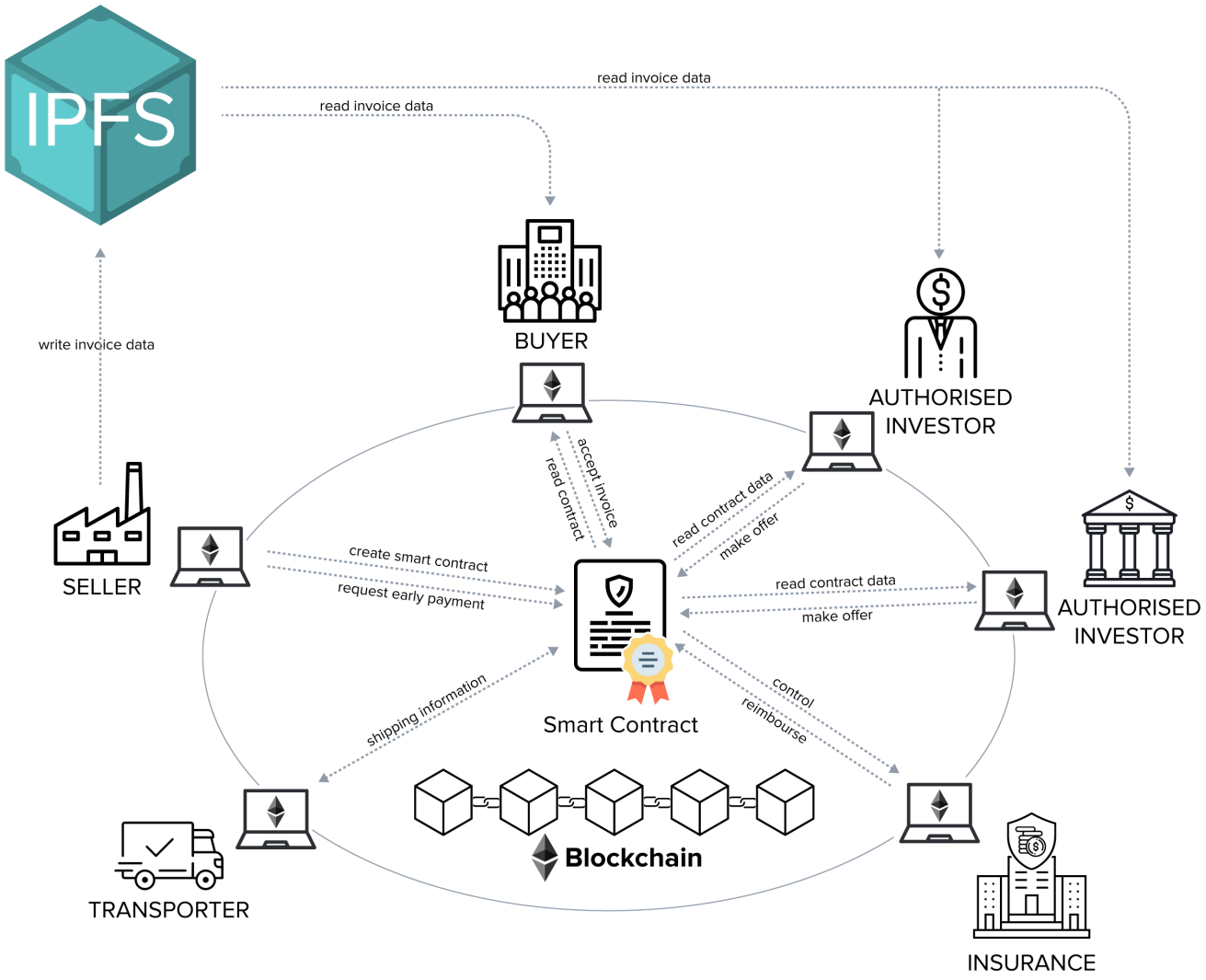

Figure 1: Invoice financing solution based on blockchain and IPFS.

(1) The seller creates a smart contract and deploys it in the Ethereum blockchain. The seller can choose to open the auction to all the investors in the platform or only to some predefined investors. In case of two authorized investors, the main contents of the smart contract are: hash (Invoice ID), shipping amount, the minimum bid requested, the highest bid, offers, auction deadline, shipment status and IPFS hash encrypted with public key of investor 1, 2 and the buyer.
(2) The buyer decrypts the IPFS hash using his private key and verifies the invoice data. If the invoice is genuine the buyer accepts the invoice and performs a safe payment of the shipping price. The smart contract holds this amount of Ether until the delivery.
(3) The transporter verifies if the invoice has been accepted by the buyer then, updates the shipment status on the smart contract to "in transit" upon receiving the goods.
(4) The buyer verifies if the shipment status on the smart contract is "in transit" then, updates it to "delivered" once the goods are received. The smart contract payout the transporter for the shipment.
(5) The investors verify the participation conditions mentioned above in order to decide whether to bid on this invoice or not.
(6) In case all the conditions are met, the first investor places his bid which should be higher than the minimum bid requested by the seller.
(7) The second investor places his bid which should be higher than the highest bid (i.e., bid 1). The highest bidder become the owner of the invoice when the auction ended.
(8) The seller asks for an early payment when the auction ended. The smart contract transfers the highest bid to the seller.

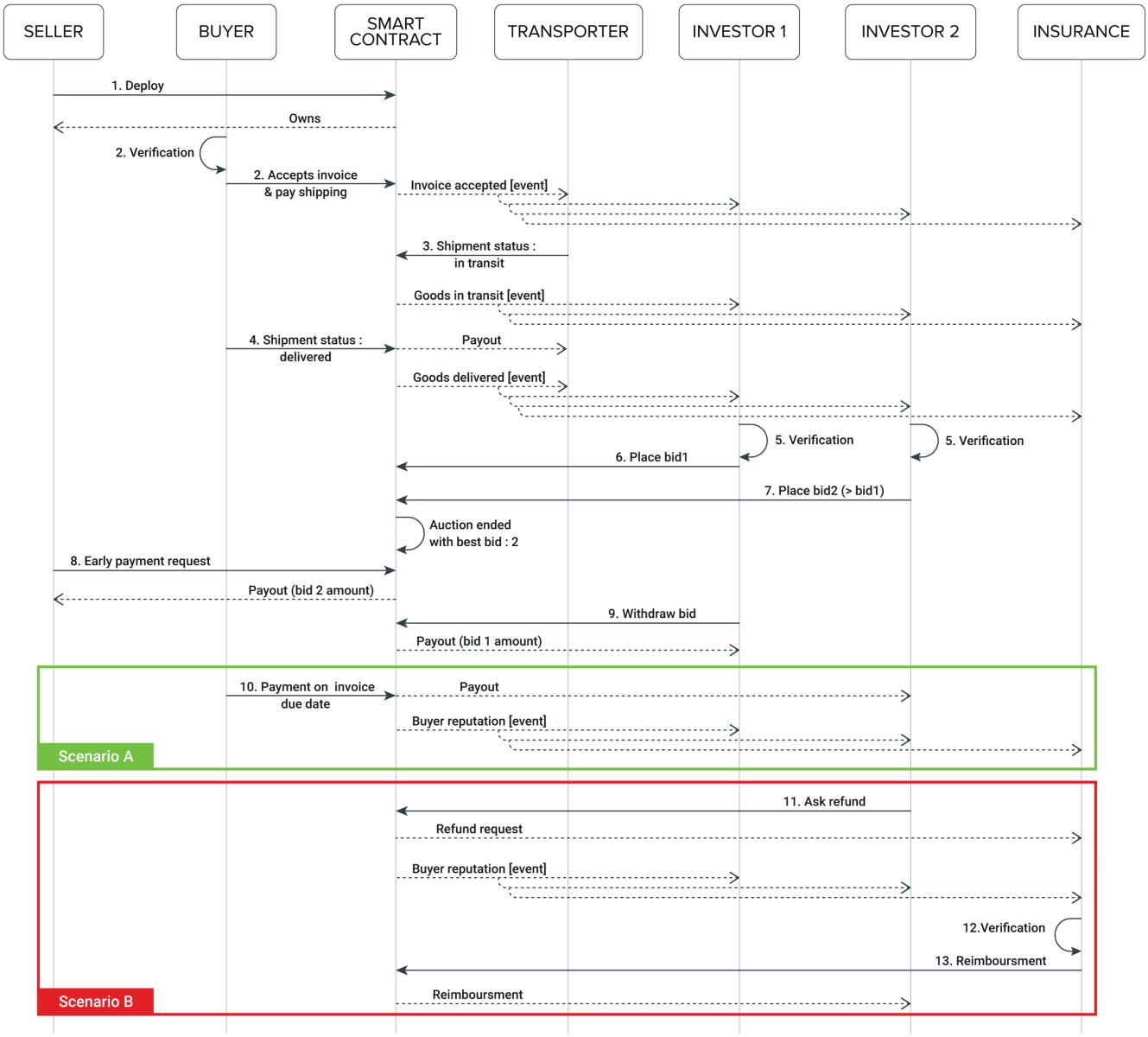

Figure 2: Sequence diagram of the proposed invoice financing workflow.

(9) When the auction ends, the investor 1 asks to withdraw his funds because he did not win the auction. The smart contract sends to the investor 1 his corresponding bid amount.

(10) **In scenario A**, the buyer pays the entire amount on due date of the invoice to investor 2 through the smart contract. An event ***BuyerReputation(BuyerAddress,"invoice paid on due date")*** will be triggered to help in tracing the buyer reputation and in notifying all parties.

(11) **In scenario B**, the buyer did not pay on due date of the invoice as agreed and thus investor 2 sends a refund request. Two events will be triggered ***RefundRequest(msg.sender, "Refund request")*** to notify the insurance and ***BuyerReputation(BuyerAddress, "Unpaid invoice on due date")*** to create notification and save a log about the buyer reputation. In this scenario, the buyer profile will show that this buyer is untrustworthy.

(12) The insurance verifies if the investor 2 did not ask refund before and he made the necessary verification before participating in the auction.

(13) The insurance refunds the investor 2 through the smart contract.

It is important to mention that in step 8, the seller manually invokes the smart contract when the auction ends to receive his money because the contract cannot activate itself; however, automating the reimbursement for investors that did not win the auction is possible by relying on step 9 on step 8. Nevertheless, we added step 9 to let the investors withdraw their funds rather than push funds to them automatically for the following security reasons: i) Sending ether back to all the investors that did not win auction could run out of gas. ii) Sending ether to unknown addresses could lead to security vulnerabilities [5].

3 FRAUD SCENARIOS AND COUNTERMEASURES

In this section, we present the possible fraud scenarios and we explain how the proposed solution, without relying on trusted third parties and just leveraging smart contracts and public blockchain technology, reduces the possibility of frauds in invoice financing between mutually untrusted entities.

All involved entities will be able to share and monitor the information related to invoice, auction, shipping and payment in a transparent manner. In addition, these information are immutable and cannot be changed. Therefore, the information that is used to build reputation profile is reliable.

Scenario 1: The seller knowingly submits a false or modified invoice. Our solution prevents this fraud because the invoice will not be funded by the investor if it has not been already accepted by the buyer. The buyer will be interested into accepting the invoice only if it is genuine because his reputation is at stake and he could lose the shipping amount.

Scenario 2: The buyer colludes with the seller, he accepts the false invoice submitted by the seller to commit a fraud and split with the seller the amount of Ether received from the investor. In this case, the buyer will be identified as untrustworthy. Furthermore, this is not enough to get funding, because the investor verifies also if the transporter receives the goods before deciding to finance the invoice.

Scenario 3: The seller submits a duplicate invoice in order to have double financing. Our platform enables both the buyer and the investor to verify that the invoice has not been submitted before because of the unique "Invoice ID" and the transparency guaranteed by the public blockchain.

Scenario 4: The buyer refuses to pay the investor in due time as stated on the invoice because he did not receive the goods. Our platform enables the investor to check if the goods has been delivered with a confirmation from the buyer before participating in the auction. The transporter will be interested into having the delivery confirmed by the buyer because his payment depends on the shipment status. Otherwise, the transporter will not accept to deliver the goods.

Scenario 5: The buyer receives the goods but refuse to pay on due date of the invoice. In this case, the investor will be refunded by the insurance and this buyer will be easily identified as malicious and untrustworthy through his reputation profile.

4 RELATED WORK

Most researchers, when proposing blockchain based solutions for invoice financing focus mostly on the issue of double financing.

Nijeholt et al. [9] proposed DecReg, a framework based on blockchain technology to address the "double-financing" issue in factoring. The framework has been implemented on a private blockchain. The access to the blockchain is controlled by a central authority (CA). Authors pointed out that the only feasible attack would be a collusion between the seller and the CA, where the CA prevents the financial institution from accessing the network which makes it vulnerable to double-financing. Hence, the financial institution should halt invoice financing until it regains access to the blockchain network.

Hofmann et al. [7] stated that the registration of invoice on the blockchain provides the opportunity to prevent fraud and double-financing issues in invoice discounting and factoring. Each invoice distributed across the network is hashed, timestamped, and given a unique identifier to prevent multiple financing on that particular invoice. However, authors did not provide implementation details such as whether the invoice is registered in public or private blockchain and how the different parties interact with each other.

Similarly, Nicoletti et al. [14] stated that blockchain can play an important role in preventing fraud during procurement finance solution implementation and notably reverse factoring. Blockchain provides complete traceability and real-time visibility on invoices status which prevent the fraudulent organizations from extracting funds from multiple financial institutions by using the same invoice.

In [15], authors proposed a conceptual framework based on blockchain technology for reverse factoring and dynamic discounting. Efficiency, transparency, and autonomy were identified as blockchain value drivers that will improve supply chain finance solutions.

Bogucharskov et al. [3] presented possible interaction between supplier, customer and factor in blockchain-based factoring application. In their interaction model, the factor provides funding to the supplier upon the confirmation of the customer that he received the goods. However, authors did not take in consideration the fraud risks if the supplier or costumer are untrustworthy or malicious. In addition to that storing invoice in the public blockchain is very expensive both from the storage and from the computational point of view.

Kayal et al. [8] stated that blockchain technology can be a powerful tool to tackle the financing problems of SMEs. In addition, they conducted an exploratory research into the appetite of the stakeholders involved in invoice factoring and inventory finance for adopting the blockchain technology.

5 CONCLUSION

In this paper we have put forward an idea for the invoice factoring and financing problem that is based on the IPFS, the Ethereum blockchain, smart contracts and reputation profiles. Our proposal is expected to provide a higher level of transparency than most solutions previously proposed, as it uses a public blockchain instead of a private one. Besides, the use of a proof-of-work based public blockchain also guarantees a better resilience to tampering and collusion. Finally, as we showed in this paper, our solution is capable

of preventing most practical cases of frauds and, by providing better guarantees, it allows lowering the costs of insurance that is needed to protect the involved parties from residual fraud cases.

As a future extension, it is worth pointing out that, in principle, the adoption of a public blockchain based on proof-of-work may lead to energy wasting, as each fraud attempt carried out by any of the involved parties is expected to lead to some form of energy loss. To this aim, we argue that the energy impact of the adoption of a public blockchain in actual invoice financing scenarios should be investigated in future works, as well as energy-wasting related attack that malicious parties can willingly attempt. We plan to model the energy consumption of a public by leveraging models previously adopted in other contexts (like, e.g., [4, 10–12]).

REFERENCES

[1] [n. d.]. What is Gas? https://kb.myetherwallet.com/posts/transactions/what-is-gas/ Accessed: 2019-05-20.

[2] Juan Benet. 2014. IPFS - Content Addressed, Versioned, P2P File System. *CoRR* abs/1407.3561 (2014). arXiv:1407.3561 http://arxiv.org/abs/1407.3561

[3] A.V. Bogucharskov, I.E. Pokamestov, K.R. Adamova, and Zh.N. Tropina. 2018. Adoption of Blockchain Technology in Trade Finance Process. *Journal of Reviews on Global Economics* 7, 7 (nov 2018), 510–515. https://doi.org/10.6000/1929-7092.2018.07.47

[4] N. Gobbo, A. Merlo, and M. Migliardi. [n. d.]. A denial of service attack to GSM networks via attach procedure. 8128 LNCS ([n. d.]), 361–376. https://doi.org/10.1007/978-3-642-40588-4_25

[5] Neville Grech, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. 2018. MadMax: Surviving Out-of-gas Conditions in Ethereum Smart Contracts. *Proc. ACM Program. Lang.* 2, OOPSLA, Article 116 (Oct. 2018), 27 pages. https://doi.org/10.1145/3276486

[6] H. R. Hasan and K. Salah. 2018. Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters. *IEEE Access* 6 (2018), 46781–46793. https://doi.org/10.1109/ACCESS.2018.2866512

[7] Erik Hofmann, Urs Magnus Strewe, and Nicola Bosia. 2018. *Discussion—How Does the Full Potential of Blockchain Technology in Supply Chain Finance Look Like?* Springer International Publishing, Cham, 77–87. https://doi.org/10.1007/978-3-319-62371-9_6

[8] Alex Kayal, Jingwen Yao, Judith Redi, and Erich C.G. Schnoeckel. [n. d.]. *Financing Small & Medium Enterprises with Blockchain: An Exploratory Research of Stakeholders Attitudes.* Chapter Chapter 4, 65–83. https://doi.org/10.1142/97817863463910004 arXiv:https://www.worldscientific.com/doi/pdf/10.1142/9781786346391_0004

[9] Hidde Lycklama à Nijeholt, Joris Oudejans, and Zekeriya Erkin. 2017. DecReg: A Framework for Preventing Double-Financing Using Blockchain Technology. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC '17)*. ACM, New York, NY, USA, 29–34. https://doi.org/10.1145/3055518.3055529

[10] A. Merlo, M. Migliardi, and P. Fontanelli. [n. d.]. Measuring and estimating power consumption in Android to support energy-based intrusion detection. 23, 5 ([n. d.]), 611–637. https://doi.org/10.3233/JCS-150530

[11] M. Migliardi and A. Merlo. [n. d.]. Energy consumption simulation of different distributed intrusion detection approaches. 1547–1552. https://doi.org/10.1109/WAINA.2013.214

[12] M. Migliardi and A. Merlo. [n. d.]. Modeling the energy consumption of distributed IDS: A step towards Green security. 1452–1457.

[13] Satoshi Nakamoto. 2009. Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf

[14] Bernardo Nicoletti. 2018. *Fintech and Procurement Finance 4.0.* Springer International Publishing, Cham, 155–248. https://doi.org/10.1007/978-3-030-02140-5_6

[15] Yaghoob Omran, Michael Henke, Roger Heines, and Erik Hofmann. 2017. Blockchain-driven supply chain finance: Towards a conceptual framework from a buyer perspective. In *IPSERA 2017*. Budapest - Balatonfüred, 1–15. https://www.alexandria.unisg.ch/251095/

[16] Gavin Wood. 2017. Ethereum: A secure decentralised generalised transaction ledger EIP-150 REVISION (759dccd - 2017-08-07). https://ethereum.github.io/yellowpaper/paper.pdf Accessed: 2018-01-03.