Social Economic Debates
Volume 13, Issue 1, 2024
ISSN 2360-1973; ISSN-L 2248-3837

EMERGING SOLUTIONS FOR INTEGRATING BLOCKCHAIN TECHNOLOGY INTO THE FINANCIAL-ACCOUNTING INFORMATION FLOW

Lucian Gheorghe NĂSTASE
Valahia University, Targoviste, Romania,
Email: nastase@gmail.com
Dumitru BEJINARIU
Valahia University of Târgoviște, România,
dumitrubejinariu@yahoo.com
Florin RADU
Valahia University, Targoviste, Romania,
Email: florinuniv@yahoo.fr

Abstract: In the era of accelerated digitalization, blockchain technology is becoming a promising solution for optimizing financial and accounting information flows, bringing transparency, security and efficiency in transaction management. The implementation of blockchain in a Billing Data and Payments/Receipts (CDFPI) confirmation system, highlights how smart contracts and security protocols can reduce the risk of errors and fraud, while ensuring voluntary tax compliance. By integrating the public blockchain, the proposed system offers a robust architecture that guarantees both the confidentiality and verifiability of transactions, contributing to the modernization and security of accounting processes.

Key words: blockchain technology, smart contract, financial-accounting information flow, eInvoice

JEL Classification: F52, L81, M41, F32

Introduction

In the current context of digitalization, blockchain technology represents an innovative solution with significant potential for transforming and optimizing financial and accounting information flows. In an increasingly complex economic world, where the speed and security of financial transactions are essential, blockchain offers a transparent, decentralized and secure infrastructure capable of responding to the current challenges related to the validation and verification of transactions.

Integrating blockchain into financial and accounting systems can address a number of pressing issues, such as the risk of fraud, errors in data processing, and lack of transparency in financial reporting. For example, confirming billing and payment/receipt data (CDFPI) is a crucial process that can benefit significantly from blockchain technology. This technology can ensure an immutable and verifiable record of transactions, thus reducing the risk of errors and fraud, as well as ensuring that VAT on invoices is correctly deducted and reported.

Social Economic Debates
Volume 13, Issue 1, 2024
ISSN 2360-1973; ISSN-L 2248-3837

Emerging solution for improving ANAF eInvoice system and pre-filled VAT statement using blockchain technology

Confirmation of Invoicing and Payments/Receipts (CDFPI) is a popular way to provide extra security in front of the default state bodies, and offers the possibility to confirm the veracity and authenticity of the transactions made. This will reduce the risk that the VAT related to some invoices will become non-deductible and not only. The primary function of an Invoice and Payment/Receipt Confirmation Accounting System (SCCFPI) is to prevent an invoice from failing to meet the deductibility conditions and thus generating undue costs for the entity. To prevent non-deductibility, many accounting ecosystems use one or more centralized entities to verify the fulfillment of the deductibility conditions. However, this puts a lot of power in the hands of these entities and makes it difficult for users to challenge situations where irregularities are found, information is wrongly recorded, or manipulated negligently or intentionally.

There are several problems and challenges in the CDFPI process. For example, it often requires several manual steps. In addition, information is dispersed between different systems and databases. There are also trust issues related to the confirmation of billing data and payments/receipts. The seller and the buyer must trust that both will quickly operate the information necessary to confirm the payments in time for ANAF to generate the eAccount. The seller at the time of confirmation of payment by the buyer must verify that this transaction has been carried out successfully, as the buyer can confirm the payment without making it. This is the main problem that a CDFPI system must prevent in order to avoid VAT tax fraud. Usually, we can assume that both the seller and the buyer can be considered trustworthy entities only when they both confirm the payment related to the transaction, since both entities have economic benefits in the CDFPI process, one deducts VAT and the other has to pay it.

In this context, a public blockchain seems like a natural tool for solving these problems, as it can keep track of CDFPI processes, but it can also prevent possible fraud. A distributed ledger can make the database distributed and highly available, as well as logically unique and safe against tampering. In this way, CDFPIs can be concluded faster, with fewer errors and still carry the authenticity and credibility of manual contracts. Concretely, the registry-based CDFPI system should operate with no errors, provide confidentiality and protection of personally identifiable information and business information, provide non-repudiation for dispute management, be decentralized and secure against corruption, comply with KYC, be cost-effective, and provide easy user integration.

The eInvoice system and the VAT return pre-filled by ANAF raise problems regarding the security of the information transmitted and the confirmation of its veracity between the entities participating in the process (ANAF, customer, supplier) in order to solve them, we proposed an emerging solution that uses blockchain technology. A public blockchain can keep a permanent, secure, orderly, and transparent record of transactions, which is then available to everyone at any time to view and verify.

In the underlying protocol, an architecture for confirming records based on a general blockchain is proposed. The blockchain platform builds trust between parties through the correct execution of transactions. A smart contract

is used to complete the process of confirming invoices, payments/receipts and to prevent situations that could lead to VAT non-deductibility. The smart contract provides for auditing and dispute resolution so that confidentiality is protected and relevant information is always available.

In the second protocol, a relayer is added to our architecture for easier integration. Improved identity management and authentication using the concept of verifiable credentials (VC) to better comply with the Know-Your-Customer (KYC) regulation. In fact, in this architecture, participants use their decentralized identifiers (DIDs) and the DIDComm protocol for asynchronous and secure off-chain interactions.

In business-to-business financial relationships, it is common practice to pay for some services or products with a certain delay, for example, a few months later. In this situation, the provider (i.e. the seller) if he uses the VAT collection system will be able to benefit from the deferral of the VAT chargeability until the invoice is collected. The VAT collection system is a popular way to provide cash flow for small entities.

In order to create the system for confirming the billing data, the payments/receipts related to them, a server will be used on which blockchain technology will be integrated and several procedures will be carried out to achieve the proposed objectives: the payment confirmation procedure, the term payment procedure and the ANAF notification procedure. These procedures have a well-defined role and will help in the smooth running of the confirmation of billing data, payments, receipts.

The payment confirmation procedure is a procedure that has the role of notifying the partners about the payment of an invoice issued. At the end of this procedure, the ANAF notification procedure will also be carried out. Thus, if one or both entities involved in the transaction are subject to VAT on collection, ANAF, through the eDecont system, will have the necessary information for the correct pre-completion of the information related to these payments, the VAT becoming payable.

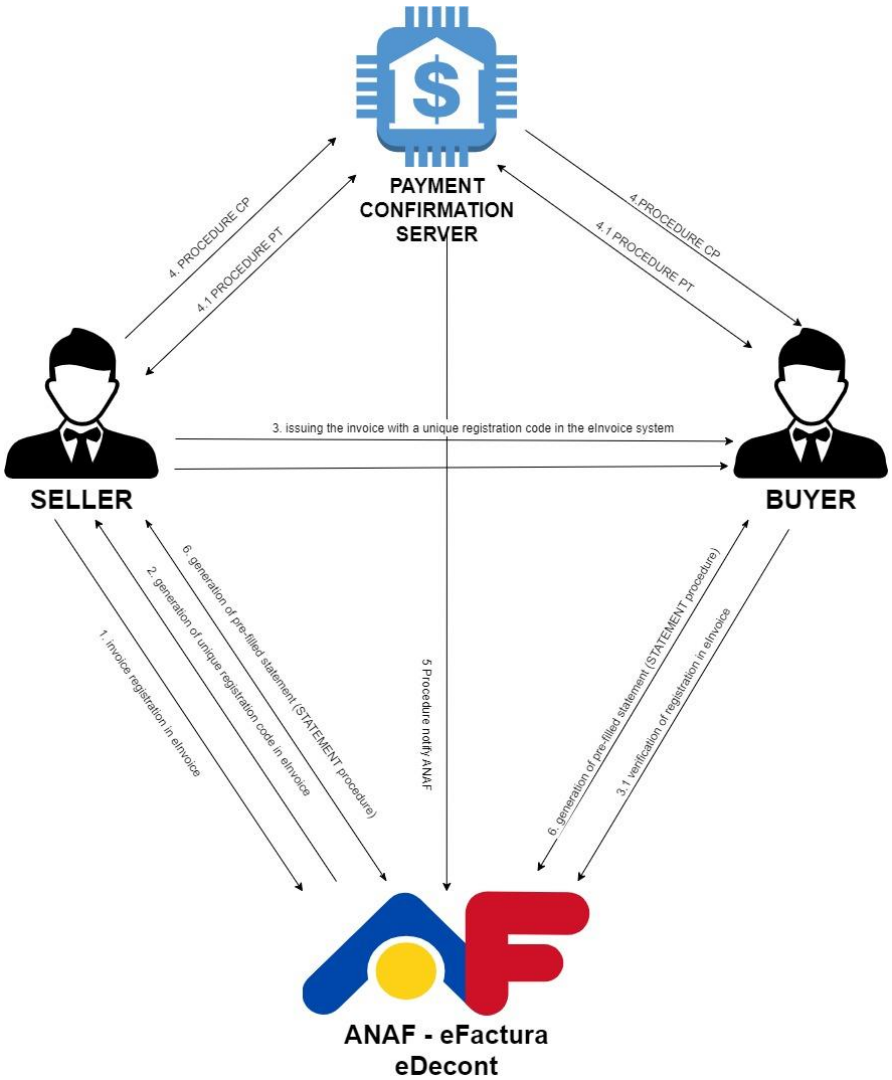
The term payment procedure has the role of establishing a confirmation between the partners making the transaction and confirming each other's payment in order to establish the state of affairs of VAT (the moment when it becomes chargeable for entities using the VAT collection system. At the end of the procedure, the payment confirmation procedure will be resumed in order to subsequently notify ANAF about the VAT chargeability related to the transaction made.

The ANAF notification procedure has the role of confirming to the body that pre-fills the eDecant VAT return regarding the VAT chargeability related to the completed and paid transaction.

All these procedures will be carried out with the help of a smart contract. The data recorded by the smart contract will provide high availability for the relevant data that the buyer needs to know, such as payment terms. Because it will contain sensitive data, we encrypt this data before storing it on-chain. In addition, we store a proof of the summary of the payment confirmation agreement between the two partners in the form of a cryptographic commitment. The storage of the CDFPI contract summary on the chain can be used to manage any future disputes

between the seller, the buyer and ANAF. This summary of the agreement must be signed by both the seller and the buyer.

As mentioned, a CDFPI relationship involves three parties: a buyer, which is a natural person or an economic entity to whom the goods or services are supplied with cash or forward payment (on credit), a seller, which is an economic entity that provides the goods or provides the services in cash or on credit, and a CDFPI server, which can be a professional accounting association or a state institution (MFP).



CDFPI System

The typical interactions between the participants in the CDFPI system are detailed in the figure above and are as follows: 1 – registration of the invoice in the eInvoice system, 2 – receipt from the ANAF server of the validation code of the invoice upload in the eInvoice system, 3 – the seller sells a service or product to the buyer and issues an invoice containing the unique registration code in the eInvoice system, 3.1 – the buyer verifies the registration of the invoice in the eInvoice system, 4 – if the payment is made instantly, the CP Procedure (payment confirmation) will be activated, which will confirm to the partners the payment related to the transaction and will activate the ANAF Notification Procedure, 4.1 – if the payment will be made later, it will activate the PT Procedure (payment on time) at the time of payment, the CP Procedure will be resumed, 5 – at the time of payment, the ANAF Notification Procedure is activated, which has the role of confirming to the body that pre-fills the VAT return eDec regarding the VAT due date related to the transaction completed and paid, 6 – ANAF will generate the pre-filled return

Proposed architecture

In our architecture, we have the three classic entities of the eDecont scenario – namely provider, customer and ANAF, a new entity Payment Confirmation Server – as well as smart contracts implemented on a public blockchain. Below, we present a detailed explanation of our proposal and a logical scheme.

In our architecture, after verifying the invoice declaration to ANAF through the eInvoice system, we assume that the customer is trusted for the payment confirmation process. We also assume a public blockchain for our architecture, but we should note that we don't use blockchain cryptocurrencies for payments. Our architecture is a system of record, and actual payments are made off-chain using fiat transfers between bank accounts.

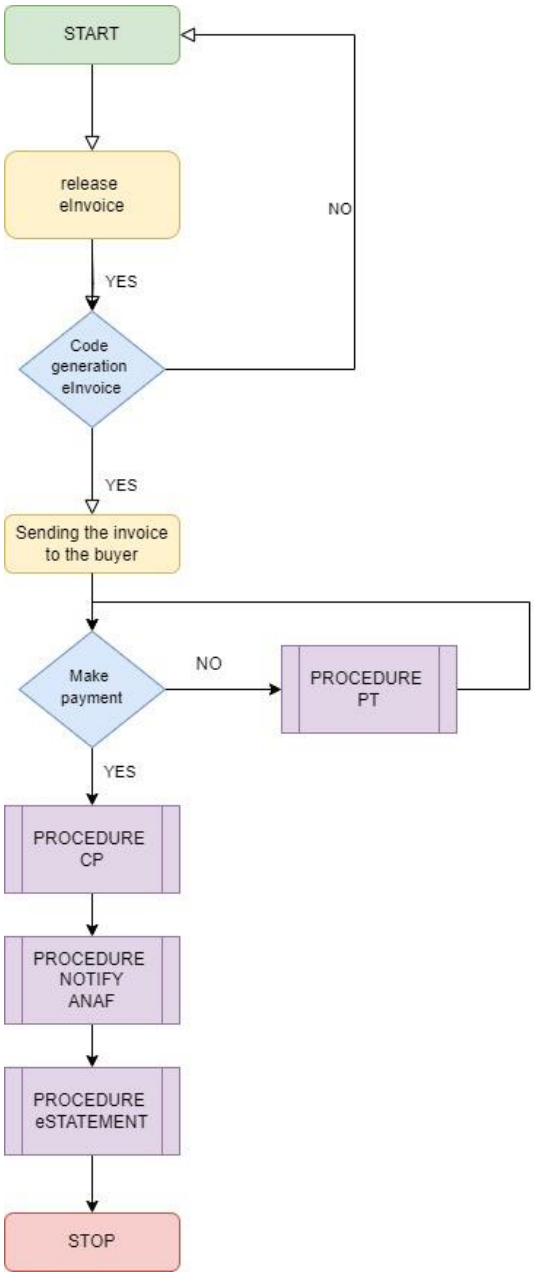
All interactions for completing the CDFPI will be managed through a smart contract. All parties can trust the correct execution of transactions managed by the smart contract, as the blockchain platform guarantees this execution. If the invoice has been taken into account, the customer must pay the invoice to the bank account of the entity registered through the smart contract. Therefore, all parties involved must review the smart contract code and ensure its correctness. The smart contract address is also part of the negotiation between the supplier and the customer.

Since every transaction that changes the state of a public blockchain has a cost, one of our main design goals is to have a minimum possible number of transactions for confirming billing data and payments/receipts. A large part of the communications between the different parties are outside the chain of trust (off-chain).

As a general rule, in our design, the CDFPI is as complex as possible and resource-consuming for ANAF. In particular, in our architecture, ANAF will not need specific digital certificates for confirming billing data and payments/receipts and will not perform digital signatures related to this process. Instead, the payment confirmation server will offer a simple web service to provide access to some minimal information about invoices and related payments, so that ANAF can verify the information provided by the supplier/customer in the submitted statements.

Social Economic Debates
Volume 13, Issue 1, 2024
ISSN 2360-1973; ISSN-L 2248-3837

Since every transaction that changes the state of a public blockchain has a cost, one of our main design goals is to have a minimum possible number of transactions for confirming billing data and payments/receipts. A large part of the communications between the different parties are outside the chain of trust (off-chain).



CDFPI System Logic Diagram

At a high level, our protocol works as follows:

1. The supplier sends the invoice to the customer through the eInvoice platform

2. The supplier sends a request to the customer to confirm the collection of the receivable or to confirm that it will be collected later.

3. The customer publishes a cryptographic summary of the payment in a web service.

4. The supplier is waiting for the payment confirmation by the customer

5. At the time of payment, the customer and the supplier certify through a smart contract that it has been made

6. The server sends the confirmation to ANAF for pre-filling the data related to this transaction

As a general rule, in our design, the CDFPI is as complex as possible and resource-consuming for ANAF. In particular, in our architecture, ANAF will not need specific digital certificates for confirming billing data and payments/receipts and will not perform digital signatures related to this process. Instead, the payment confirmation server will offer a simple web service to provide access to some minimal information about invoices and related payments, so that ANAF can verify the information provided by the supplier/customer in the submitted statements.

When we use a public ledger, we gain transparency, but at the same time, everyone has access to the stored data. In the process of confirming billing data and payments/receipts, there is sensitive business information that needs to be properly protected. For privacy protection, we do not store sensitive data directly on the blockchain. Instead, some of the data is symmetrically encrypted before being stored on-chain, another part of the data is stored off-chain, and we use cryptographic pledges to provide proof of existence.

Once an invoice and payment confirmation are registered, it is guaranteed that: it has been declared to ANAF and is deductible, it is accepted by both the customer and the supplier, the relevant parties have access to the relevant data and proof of its existence, there is no way to challenge the CDFPI once the smart contract has registered it. In addition, to carry out the registration process, all parties will have real identities (e.g. CUI), and the supplier and customer will also have blockchain accounts (which are pseudo-anonymous identifiers).

Finally, we assume that an invoice contains the following information: the identity of the supplier and the customer, the invoice number, the date of issue, the due payment term, the total amount, and other details about the services/goods provided by the seller to the buyer. We assume that the identity of the supplier and the invoice number are sufficient to uniquely identify the invoice, therefore the use of unique invoice numbers should be applied. In addition, the customer's identifier, the due payment term and the total amount are required for ANAF to pre-fill the eSettlement. Other information can be added to the invoice without affecting the way our architecture works.

Our architecture is framed in a financial context and therefore strict regulatory restrictions apply to it. In particular, according to the Know-Your-Customer (KYC) regulation, the parties involved must be well identified with each other, and their agreements must be maintained for further audits and law enforcement. To comply with the KYC regulation, the provider and customer will record the correspondence between their real identity (IDA) and their pseudonymous identifier in the blockchain (@A). We use the term Blockchain Certificate to refer to these links between real identities and pseudo-identities. In our architecture, we rely on the customer and supplier to create these links, as both would have to pay/deduct VAT, therefore we can assume that they have an interest in certifying transactions.

On the other hand, by design, our protocol avoids ANAF from digitally signing Blockchain certificates or any other data. Our Blockchain certificates are used privately and are exchanged between a provider and a customer only after they intend to conclude an agreement. In addition, an entity can have multiple Blockchain certificates with different blockchain addresses to have additional protections against link attacks.

Our protocol is built around a smart contract, which is implemented on a public blockchain. The smart contract will contain registration data for a set of invoices. No one (including the one who carries it out) will have special powers over the contract. In particular, no one will be able to interfere with the operation of the smart contract or change the data of the set of invoices and payment terms.

Social Economic Debates
Volume 13, Issue 1, 2024
ISSN 2360-1973; ISSN-L 2248-3837

Our architecture is designed to work on a public blockchain. Public blockchains have costs, so our protocol needs to be cost-effective. Generally, there are three different places where data is stored on the blockchain: transaction input data, key value storage, and transaction output logs. Each of these places has a different purpose and a different cost.

Summary of smart contract storage possibilities.

The transaction input data is the transaction data that provides the inputs to execute the smart contract logic for the current transaction. The transaction input data is very cheap compared to key-value storage, which is by far the most expensive storage. Key-value storage provides storage to the smart contract that persists between transactions. The storage of the key value is part of the current global state of the blockchain, and as such, it can be used by the logic of the smart contract for the execution of future transactions. Finally, transaction output logs are data produced after a transaction is executed.

Transaction input data and transaction output logs are part of blockchain data, and as such, are highly available and immutable. However, this data is not part of the current global state of the blockchain, which means that blockchain nodes do not need to keep this data in its current state once the transaction has been executed. This is why this data is cheap to store, and also why a log data from a previous transaction is not available to logic that executes a subsequent transaction.

In our protocol, we use a combination of the previous three storage locations to provide an efficient deployment while preserving the privacy and security of the architecture. In particular, we use a single persistent key-value slot to prevent fraud. CDFPI data is recorded using a transaction output log. It should be noted that data in transaction output logs typically has indexed fields that allow external entities to perform quick searches based on these index fields. In our protocol, we use a pseudo-anonymous identifier for the invoice as an indexed journal field to speed up the data search.

Finally, we would like to mention that our smart contract stores the blockchain addresses of the on-chain provider and customer as part of the transaction record. In our protocol, as we will show, we use transactions that include signatures using blockchain identities of both the provider and the customer, and we will retrieve their blockchain addresses from these signatures.

The complete CDFPI process using the above detailed protocol are:

Phase 1: eInvoice Registration – The CDFPI process of a specific invoice begins with the registration phase and is followed by the payment confirmation phases. Each phase consists of several stages. At the beginning of the CDFPI phase, the provider requires the customer to publish the billing information through its Web service. The publication is quite similar to how Blockchain certificates are published, except that additional information related to the CDFPI process is required.

Phase 2: Confirmation of billing data and payments/receipts – This phase begins with the supplier contacting the customer to confirm the payment or confirm the payment term. The supplier should naturally provide the invoice details, including the invoice number, the total invoice amount, and the due payment term to the customer. Finally, we need the invoice registration data to be available to the parties: the customer for VAT deduction, the supplier for VAT payment and ANAF for pre-filling the eSettlement, so that the 3 parties have evidence in case of litigation. To make this efficient, we store this data as a smart contract exit transaction log.

Phase 3: Payment – In the third phase, after verifying the information recorded by the smart contract, the customer pays the provider. Subsequently, the customer and the supplier will confirm the payment on time and will be informed to ANAF through the notification procedure. If one of the customers or suppliers is the beneficiary of VAT on collection, ANAF will use the data to pre-fill the eStatement.

We must note that our registration protocol is not secure against malicious customers, because if the customer and the supplier publish false information, this can only be challenged by ANAF following thorough analysis. As a result, ANAF must trust the customer and supplier that they will voluntarily comply. A malicious customer, for example, may not pay the vendor but confirm the payment. A malicious customer can also deceive ANAF by creating a fake supplier and a large amount of non-existent invoices. Then, the fake supplier receives the payment confirmations, but the corresponding payments are not made by the malicious customer, and the customeruk commits VAT tax fraud. If the clientuk is not trustworthy, a mechanism must be used to enforce good behavior (such as a reputation system that is public).

Conclusion

The integration of blockchain technology into the financial-accounting information flow, especially in the systems for confirming invoicing data and payments/receipts (CDFPI), represents a promising emerging solution

that addresses multiple existing challenges in the field. By using a distributed ledger, blockchain provides a secure, transparent, and efficient platform for managing transactions, reducing the risk of errors and fraud, as well as the costs associated with verifying and auditing these transactions.

The proposed smart contract-based architecture not only improves data integrity and privacy, but also facilitates compliance with tax and audit regulations such as KYC. The proposed solution stands out for its efficiency, minimizing complexity and resource consumption, and offers a reliable way to ensure VAT deductibility and improve the cash flow of economic entities.

Thus, the integration of blockchain into financial-accounting flows promises to radically transform the way invoicing and payment data are managed, contributing to greater transparency and security in business relationships. This not only modernizes existing processes, but opens up new perspectives for more efficient accounting and more secure management of financial data.

References

1. De Filippi, P., & Wright, A. (2020). Blockchain and the Law: The Rule of Code. Harvard University Press

2. Dietrich, J. C. G., & Grüninger, S. (2019). Blockchain Technology in Accounting: Opportunities and Challenges. Journal of Accounting and Public Policy

3. Kanaparthi, V., (2024), January. Exploring the Impact of Blockchain, AI, and ML on Financial Accounting Efficiency and Transformation. In International Conference on Multi-Strategy Learning Environment. Singapore: Springer Nature Singapore

4. Zubareva, E.A., Basantsov, I.V. and Byelov, S.V., (2020). Financial e-control: modernization of the state financial control system in the conditions of digital economy. Journal of Automation and Information Sciences