Confidentiality-preserving Validation of Tax Documents on the Blockchain

Filip Fatz, Philip Hake, Peter Fettke

German Research Center for Artificial Intelligence, Institute for Information Systems, Saarbrücken, Germany
{filip.fatz, philip.hake, peter.fettke}@dfki.de

Abstract. Information exchange between tax administrations, businesses, and auditors is key to effective tax enforcement. Therefore, organizations proposed the application of blockchain technology to interconnect the different actors and increase tax transparency. However, the lack of confidentiality measures hampers further development. Especially, businesses are concerned about the disclosure of commercially sensitive information that might threaten their competitive advantage. In this paper, we investigate how the application of zero-knowledge-proofs can contribute to solving the dilemma between transparency and confidentiality in blockchain-based tax systems. To meet this end, we provide a conceptual design of a confidentiality-preserving distributed tax ledger. Moreover, we present a prototype addressing reporting obligations in the context of value-added tax. Our evaluation shows that zero-knowledge proofs are an effective measure to trade off transparency against confidentiality. Still, their application is challenging and future research must focus on better abstractions of proving statements.

Keywords: *blockchain, tax compliance, confidentiality, data protection*

1 Introduction

Taxes serve the financing of governmental tasks and public goods. They enable investments in public infrastructure, law enforcement as well as public safety, and thus the creation of attractive business locations. While businesses benefit from those investments, they have a natural incentive to minimize their tax burden in order to strengthen their competitiveness. Therefore, legislators have imposed a variety of regulations on companies to prevent tax evasion. These include, among others, reporting obligations and the implementation of organizational control measures. Non-compliance with regulations poses a significant risk to businesses and can result in fines, back taxes, and ultimately criminal penalties. Over the years, the complexity of tax systems has steadily increased and has become one of the main determinants of tax evasion [1]. The complexity not only makes identifying fraudulent behavior difficult but also disadvantages willingly compliant businesses. Moreover, administrative compliance costs can discourage companies from participating in a market [2]. The problems of the current tax system manifest themselves in tax gaps

15th International Conference on Wirtschaftsinformatik,
March 08-11, 2020, Potsdam, Germany

https://doi.org/10.30844/wi_2020_l1-fatz

such as those found for value-added tax (VAT) revenues in Europe. In particular, a recent report shows that the European Union lost 147.1 billion euros only in 2016 due to inadequate tax collection systems [3].

For administrations, the availability of detailed information is the key to effective tax enforcement. Hence, tax administrations require companies to report on their taxable transactions. In the past, reporting was primarily limited to aggregated data in the form of paper-based tax declarations. However, administrations are moving or have already moved to electronic information exchange to increase efficiency. In Germany, the Act on the Modernization of the Taxation Procedure [4] aims at the use of information technology to enable a more economic tax collection system. The establishment of digital interfaces (e.g., ELSTER) is supposed to simplify tax declaration for companies and partially automate tax determination on the part of the authorities [4]. Still, the reports are submitted in an aggregated manner. Italy's e-invoice system takes a step further by not only exchanging aggregated information (e.g., recapitulative statements or VAT declarations) electronically but also by recording individual invoices and checking compliance instantaneously [5].

Both solutions focus on individual national tax systems. In the absence of a global coherent tax information system, the flow of information between businesses and administrations is mostly point-to-point and does not provide an integrated view of the taxable transactions of a business. However, to prevent tax fraud and evasion on an international level, information about taxable transactions and the according administrative processes need to be integrated. The current lack of information flow across national borders is considered the main driver of tax losses [6].

The implementation of a global, centrally governed tax information system is challenging since national authorities may mutually distrust each other regarding how tax data is processed. Distributing tax data and the validation of tax information across different parties could establish the trust required in a global tax system. Recently, the shortcomings resulting from decentralized and individual tax and information systems have been addressed by blockchain solutions [7–15]. In the proposed applications [7–15], the blockchain technology provides an integrated and consistent view on taxable transactions. This is achieved by a combination of consensus mechanisms and smart contracts, leading to a decentralized validation and storage of information without requiring mutual trust between the participating actors.

Blockchain technology provides adequate protection for the basic IT security values of integrity (consensus) and availability (replication) [16, 17]. Since assessing the validity of data submitted to the blockchain requires data transparency among the validating actors, it is originally weak in ensuring confidentiality. However, the confidentiality of data is an essential requirement in business applications. Thus, this paper investigates the confidentiality issues of current blockchain-based tax compliance approaches. We aim at providing a solution to the dilemma between transparency and confidentiality in the context of tax reporting obligations by following a design science research approach [18]. We derive objectives of a solution, provide a conceptual design and a prototypical implementation. Finally, we evaluate our prototype and identify new research directions and implications for blockchain-based tax compliance.

https://doi.org/10.30844/wi_2020_l1-fatz

The remainder of the work is structured as follows. In Section 2, we describe the challenge of confidentiality in the context of blockchain and taxation. Moreover, we derive concrete design objectives from the outlined problems. Section 3 provides the conceptual design of our solution, including an architecture for the confidentiality-preserving exchange of tax documents. Section 4 describes our implementation and an exemplary use-case. Moreover, we evaluate the benefits and limitations of our approach. Section 5 discusses related work in the context of confidentiality, tax, and blockchain. Finally, we conclude our work in Section 6.

2 Problem Description and Objectives

Confidentiality, one of the basic characteristics of IT security [16], "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" [19]. Conversely, transparency entails the disclosure and communication of information for the purpose of understanding a fact. Both desirable characteristics are contradictory, leading to the dilemma between transparency and confidentiality.

Tax debates show that creating transparency may reduce conflicts between administrations and businesses and may increase efficiency based on cooperative compliance [20]. However, businesses consider the disclosure of commercially sensitive information (e.g., customer relations or custom discounts) a risk that might threaten their competitive advantage [21]. Therefore, a tax information system must integrate measures that provide confidentiality but also enable transparency concerning provided information and information processing for businesses and administrations alike. Existing tax information systems represent national solutions that operate independently. However, administrations require integrated systems and processes to combat tax fraud and evasion efficiently.

The original application of blockchain in Bitcoin was primarily driven by the requirement to create integrity and consistency of information through transparency [22]. The application enables users to unambiguously determine the coins that a user owns (transparency), thus allowing users to independently decide whether a coin transaction is valid or not. Nevertheless, the proposed approach lacks confidentiality since transactions and balances are publicly available and are replicated across arbitrary blockchain users [17].

Recently, blockchain technology has been employed to create decentralized applications that track taxable transactions of businesses [7–15]. However, the acceptance of blockchain-based business applications depends heavily on the creation of appropriate security measures to protect the business' data. Primarily, two approaches enabling confidentiality in blockchains can be distinguished. (1) Access control mechanisms restrict the retrieval of the information itself, e.g., users must authorize themselves before access is granted. In contrast, (2) encryption transforms information using a key into a ciphertext that cannot be deciphered without knowledge of the key. Ideally, the ciphertext does not reveal anything about the original data.

https://doi.org/10.30844/wi_2020_l1-fatz

Access control is the approach taken by private blockchains, i.e., blockchain networks to which only authorized users have access. Necessarily, private blockchains include an authority that controls access. As a result, trust assumptions are reintroduced and the entire system depends once again on a central authority, undermining the most important benefits of the technology – trustlessness and decentralization [23].

The encryption of transaction data creates confidentiality in public blockchains whose data is naturally accessible by anyone. However, the information encrypted can no longer be publicly validated, preventing transactions and the underlying processes from being auditable and verifiable during transaction validation [24].

In contrast, we seek for a solution that preserves transparency for validation purposes (O1). The compliance of tax documents should be assessable for a specified set of rules without the actual private document data being disclosed (O2). The desired transparency entails the availability of information and thus an electronic exchange of tax documents (O3). A centralized solution to the information exchange problem is unlikely. In particular, the large number of involved actors and jurisdictions represents a decentralized environment (O4). An overview of the objectives is given in Table 1.

Table 1. Objectives of a Solution

	Objective	**Description**
O1	Transparency	Compliance of documents with regulations should be publicly verifiable
O2	Confidentiality	The system should provide measures to protect tax documents from public disclosure
O3	Electronic information exchange	Tax documents should be exchanged electronically
O4	Decentralization	The document storage and validation should be decentralized

3 Conceptual Design

3.1 Overview

In the system to be developed, actors exchange tax information in the form of *documents*. *Document templates* define the structure of documents such as their attributes and the corresponding data domains. Attributes can either be *public* or *private*. Public attributes are stored unencrypted on the blockchain. In contrast, the blockchain does not directly record private attributes, but only a commitment to their value. We expect the participants to securely exchange private data off-chain, e.g., by using a decentralized file system [25]. By default, each document template includes meta attributes such as the public key of the document creator and the document

https://doi.org/10.30844/wi_2020_l1-fatz

creation time. The metadata attributes are automatically assigned a value when the document is created.

Document rules impose restrictions on the data and metadata of a document. After document creation, the compliance with document rules is checked as part of the transaction validation. Essentially, a document rule is a function that classifies a given document as either valid or invalid. If a document violates a rule, it is not added to the blockchain. We call the attributes required to evaluate a rule *constrained*. Public document rules, i.e., rules that only encompass public constrained attributes, are validated within the blockchain. For example, they are implemented by the smart contract function that handles the document creation. In contrast, smart contracts cannot evaluate rules posing constraints on private attributes since the data needed for the evaluation is not accessible on the blockchain.

Hence, we propose the use of non-interactive zero-knowledge proofs. For each new document, the creator attaches a proof attesting the document's compliance. Instead of evaluating a given document rule, the corresponding smart contract function only checks the validity of the proof. The zero-knowledge property of the proof ensures that the document's private data is not disclosed.

3.2 Building Blocks

In this section, we introduce the relevant concepts and cryptographic protocols used to build our solution.

Commitment schemes. To enable confidentiality in our system, the actors only publish hiding commitments that do not reveal any information about the committed transaction details [26]. In a second step, the commitment scheme enables the actor to proof to a verifier that the commitment belongs to a specific value. More importantly, the commitment is binding in the sense that once a commitment to a value v has been published, it is computationally infeasible for the committer to proof to a verifier that the commitment belongs to a different value v', i.e., $v \neq v'$. In order to commit to value v, the actor chooses a random blinding value r, deterministically computes the commitment $cm = COMM(v,r)$ and publishes cm on the blockchain. In a second step, the committer can proof to a verifier that the commitment cm belongs to v by revealing v and r to the verifier. The verifier recomputes $cm' = COMM(v,r)$ and checks if $cm = cm'$ [26].

Non-interactive zero-knowledge proof systems. Typically, proving the correctness of a statement reveals more information than the single bit as to whether the statement is true or false. For example, the naive proof that a number (e. g. 11639) is not prime reveals its factorization (e.g. 103 * 113 = 11639). To formalize this problem, Goldwasser et al. introduced the notion of zero-knowledge proofs (ZKPs) as "proofs that convey no additional knowledge other than the correctness of the proposition in question" [27]. A particular type of ZKPs are non-interactive zero-knowledge proofs (NIZKPs) that do not require any interaction between the prover and the validator. For example, the prover creates a proof, sends the proof to the validator that verifies

https://doi.org/10.30844/wi_2020_l1-fatz

the proof without further interaction. We propose the use of zero-knowledge succinct non-interactive argument of knowledge (zk-SNARKs) that satisfy an additional efficiency criterion. In summary, the following properties apply to zk-SNARKs:

- **Completeness.** If a statement is true, a prover can convince an honest verifier, i.e., a verifier that is following the protocol properly.
- **Soundness.** No dishonest prover can convince an honest verifier of a false statement.
- **Zero-Knowledge.** In the case of a true statement, a dishonest verifier learns nothing else than the fact that the statement is true, i.e., the proof does not leak any additional knowledge about the private input (the witness).
- **Efficiency.** The size of a proof is determined only by the security level given by the bit length of the verification and proving keys. A verifier can check the validity of a proof in polynomial time with respect to the number of public inputs.

In short, proving and validating a statement using zk-SNARKs encompasses three algorithms (see Figure 1):

- **Setup.** Zk-SNARKs require a trusted on-time setup to create a proving key (used to create proofs) and a verification key (used to verify proofs). The setup algorithm requires as input the statement to be proven. For simplicity, we use a zk-SNARK implementation that represents the statement using a domain-specific programming language (see Section 3.4).
- **Prover.** Given the proving key, the private input (the witness) as well as the public input, the proving algorithm creates a ZKP for the statement.
- **Verifier.** Given the verification key, the proof as well as the public input, the verification algorithm decides if the proof is valid (e.g., outputs true or false).

For a more formal definition of zk-SNARKs, we refer the extended version of [28].

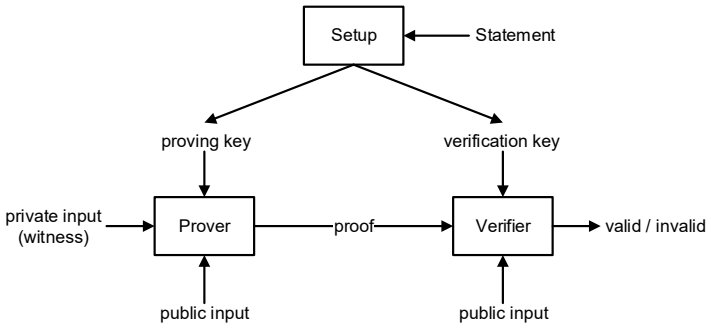

Figure 1. Zk-SNARK protocol overview

Blockchain. The term blockchain is inconsistently used in literature. In the following, we consider a blockchain to be a distributed append-only data store governed by a set of peer nodes. Each node keeps its replica of the ledger. Changes to the ledger are represented by transactions, which themselves are grouped into blocks. Each block

https://doi.org/10.30844/wi_2020_l1-fatz

refers to the data of the previous block by including its hash. Hence, blocks form a chain [29]. Whenever a new transaction is published within the peer-to-peer network, the participating nodes validate the transaction and run a consensus protocol to determine the order of transactions. The new transactions are embedded into a block which is finally appended to the blockchain. Blockchains can be further characterized by the freedom of actors to participate in the consensus-building. Private and permissioned blockchains limit the participation in the consensus-building to a single actor or consortium of parties. In contrast, in a public blockchain, any actor can participate and propose new blocks. The design of the blockchain affects the confidentiality, transparency, and performance of the system [30]. To enable automation, [31] introduces smart contracts to blockchains. Smart contracts are executable programs which are recorded on the blockchain. Their execution is triggered by submitting transactions to the blockchain. Determining the program state is part of the consensus and validation mechanism. The consensus participants ensure a consistent program state by executing the program and verifying the new state.

3.3 Private Document Rule Validation

Transaction validation is commonly understood as the mechanism that determines whether a blockchain transaction conforms to a set of predefined rules. Invalid transactions are discarded and not included in the blockchain. Having a clear set of rules and distributing the validation across different organizations translates into transparency and trust. However, the validation concept has a significant limitation: (1) the validation can only rely on data available on the blockchain and (2) at least the validators must access the data. As a result, the blockchain cannot validate confidential data. This subsection discusses how zk-SNARKs enable the validation of data that is (1) only recorded on the blockchain in the form of binding commitments and is therefore (2) not accessible by the validators.

Essentially, the main idea is to replace the direct validation of transaction data by the validation of a ZKP that the committed data conforms with the corresponding rule. Whenever a new document is created, the proof is attached to the document creation transaction and is checked by a smart contract. The zero-knowledge property ensures that the proof does not disclose any information other than the validity of the corresponding rule. The commitment stored for each private attribute binds the document creator to a particular value. More specifically, the statement gets as *private input* (1) the private attribute values and (2) the corresponding binding values and as *public input* (3) the public attribute values as well as (4) the commitments to the private attribute values. The statement states that (a) the commitments can be recomputed from the private attribute values and the corresponding blinding values and (b) the document rule is fulfilled, i.e., evaluates to true.

3.4 Document Rule Specification

We use ZoKrates' [32] domain-specific language (DSL) to specify private document rules, i.e., rules including constrained private attributes. The language has been

https://doi.org/10.30844/wi_2020_l1-fatz

designed to compile into arithmetic circuits over finite fields, a model of computation commonly used by NIZKP systems. Due to the underlying model, all variables in ZoKrates represent finite field values and operations use modular field arithmetic.

In the following, ZoKrates programs implement document rules. The entry point of any ZoKrates program is its *main* function which can receive *private* and *public* parameters. Private parameters represent the constrained private attributes of a document, while public inputs represent constrained public attributes. Listing 1 shows an example of a simple invoice document rule. The rule has the tax rate and the total net amount as private inputs (line 1). This implicitly includes the corresponding blinding values (line 2) and the public commitments to the values (line 3). The document rule checks if the public commitments match the private data by using the predefined commitment function *comm* (line 5-6). In line 8-10, the rule enforces the tax rate to be either 19 or 7. Moreover, the depicted rule considers constrains documents to include a total net amount of less than 1000 (line 12-13).

```
1  def main(private field taxRate, private field netTotal
2     private field bTaxRate, private field bNetTotal,
3     field cTaxRate, field cNetTotal)->(field):
4
5     cTaxRate == comm(taxRate, bTaxRate)
6     cNetTotal == comm(netTotal, bNetTotal)
7
8     field testTaxRate = if taxRate == 19 || taxRate == 7
9       then 1 else 0 fi
10    testTaxRate == 1
11
12    field testLimit = if netTotal < 1000 then 1 else 0
13    testLimit == 1
```

Listing 1. Extract of a document rule implementation in ZoKrates DSL

3.5 Document Smart Contracts

The proposed blockchain includes a document smart contract for each document template. The tax authorities create and set up the smart contracts, i.e., by initializing them with a proving and verification key needed to generate and verify proofs. A document contract allows the creation of new documents by calling its *createDocument* function. Whenever the function is called, the attached proof is checked for validity and finally the new document (including the public attribute values as well as commitments to the private attribute values) is stored (see Figure 2). The random binding values used to create the commitments are considered private and thus stored off-chain by the document creator.

https://doi.org/10.30844/wi_2020_l1-fatz

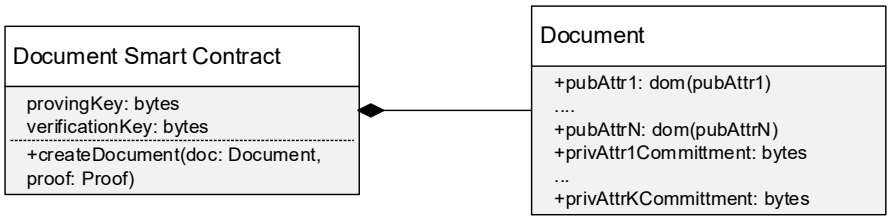

Figure 2. The structure of the document smart contract

3.6 Platform Architecture

The architecture for the blockchain-based document exchange consists of an on-chain and an off-chain environment, as shown in Figure 3. Smart contracts store the data and implement all logic of the on-chain environment. In contrast, the off-chain environment is the local runtime of each actor participating in the system. Both environments are interconnected by the interface layer, which handles the connection to the blockchain and provides a dedicated API for the document exchange. For example, the interface layer provides functionalities to listen for events, to create new documents, and to query information from the blockchain.

The on-chain environment consists of three different smart contract types. The identity management contract provides logic to administrate the participating actors such as tax authorities, businesses, and auditors. Its authentication logic can be used throughout the whole on-chain environment to authenticate participants. The document management allows the registration of new document templates as well as administrate (e.g., updating) existing document templates. Each document template has a unique identifier which refers to the corresponding document contract bundling all document data (compare Section 3.5).

The off-chain environment maintains all private data (including the binding values) as well as the private keys to authenticate new document transactions. Moreover, it contains a compiler that translates document template specifications into smart contract and ZKP specifications. The proof generator provides the tools needed to create a proof for a given document.

https://doi.org/10.30844/wi_2020_l1-fatz

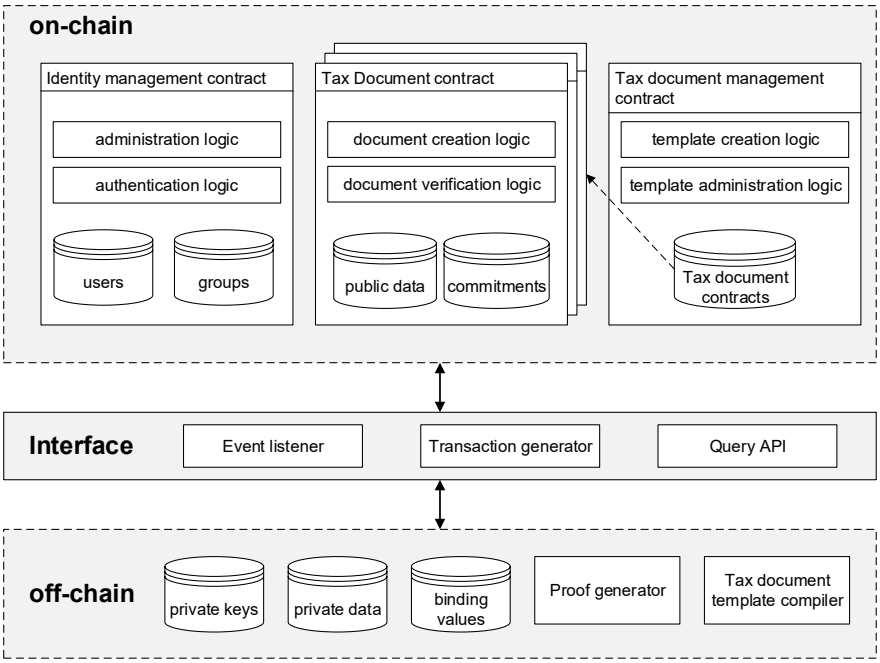

Figure 3. System architecture

4 Implementation and Evaluation

The described design has been prototypically implemented to enhance compliance with VAT invoicing rules. We used the Ethereum framework [31] and Truffle [33] to accelerate the development process. For the zk-SNARKs, we adopted ZoKrates [32] to specify the statements to be proven as well as to validate proofs within Ethereum. We use Pedersen commitments [34] since they are perfectly hiding and can be efficiently computed over the elliptic curve implemented by ZoKrates.

4.1 Invoice Verification Use Case

Invoices are the most important tax documents. According to the German VAT act (Section 14 UStG), an invoice is any document used to settle a delivery or other service. In the context of VAT, invoices serve the purpose of determining VAT duties and as proof for claiming VAT deduction. Therefore, checking invoices for compliance is a crucial step towards fraud prevention.
In the following, we demonstrate how our solution supports the immutable storage of invoices for VAT determination. In this context, we show the application of document rules to invoice validation. For simplicity, our prototype only covers the essential invoice attributes such as the item description, a quantity, the unit net price, and the VAT rate applied. While the former attributes are considered private, our invoice

https://doi.org/10.30844/wi_2020_l1-fatz

document includes the VAT id of the seller and receiver as public attributes. Although this decision undermines transactional privacy, it is necessary to establish clear responsibilities for taxation.

Our prototype implements several structural rules such as "VAT rate is either 0%, 7% or 19%", "the item description may not be empty" and "the quantity must be larger than 1". Moreover, we implement a fictional rule that requires invoices exceeding a certain total amount to be flagged. The flagged invoices are subject to further inspection by the tax administration.

Besides the structural compliance rules, we implement an audit mechanism that enables the comprehensible reporting of aggregate information about the individual invoices. We allow businesses to report periodically (e.g., monthly) aggregated data (e.g., the total turnover) without disclosing the individual invoice information. Our prototype ensures that the reported amount is the sum of the committed individual amounts. More specifically, we exploit that Pedersen commitments are additively homomorphic, e.g. $COMM(v_1, r_1) * COMM(v_2, r_2) = COMM(v_1 + v_2, r_1 + r_2)$. Thus, the business may use a zk-SNARK to prove the correctness of the sum as follows:

- Given as public inputs the sum of the total amounts of all invoices in the report period (the last n invoices): $amount_{sum} = \sum_{i=1}^{n} amount_i$,
- the product of the commitments to the amounts $comm_{mul} = \prod_{i=1}^{n} comm_i$,
- and as private input the sum of the corresponding blinding values $r_{sum} = \sum_{i=1}^{n} r_i$,

the business provides a proof that $comm_{mul} == \mathrm{COMM}(amount_{sum}, r_{sum})$ and publishes $amount_{sum}$ along with the proof.

4.2 Evaluation

We evaluate our solution by revisiting the predefined objectives. Unlike many other approaches to tax compliance (see Section 5), our solution enables the public to verify adherence to document rules (O1). The increased transparency is a significant improvement compared to the traditional encryption or access control approaches. By relying on the zero-knowledge property of zk-SNARKs and the perfect hiding property of the commitment scheme, the presented system does not explicitly disclose any information about private attribute values (O2). Document rules provide a powerful measure to tradeoff between transparency and confidentiality. While a valid proof attests compliance with a document rule, the private data that led to compliance may not be disclosed. However, the degree of disclosure highly depends on the underlying document rule. For instance, if a document rule investigates whether an invoice amount exceeds a certain value, the information that the invoice exceeds this value is available to the public. Still in comparison to public blockchains, the exact invoice amount remains hidden.

Furthermore, document templates define a standard for the tax documents, enabling an electronic information exchange (O3). The interface layer of our architecture provides functionalities to automatically serve the blockchain interface as

https://doi.org/10.30844/wi_2020_l1-fatz

well as the off-chain private data exchange interface connected to a decentralized file system. Our solution takes care about the heterogenous tax environment by being fully decentralized (O4). This design decision facilitates the integration of new actors.

However, we still consider a couple of steps necessary for the practical adoption of the proposed solution. First, better abstractions of tax documents and document rules need to be developed or integrated into our solution. A compiler might automatically translate the higher-level document and rule specifications into ZoKrates DSL and Solidity code. Moreover, in its current state, our system assumes a trusted setup of the proof parameters such as the proving and verification key. Otherwise, the randomness required in the setup phase could be used to forge proofs [35]. Decentralization of the parameter generation [35] would relax this trust assumption.

The introduced system is a single point of truth for determining tax liabilities. Therefore, companies should not be completely anonymous within the system. As previously mentioned, each transaction can be linked to an actor by using the attached signature. Unfortunately, this enables the public to derive usage statistics, possibly implicitly leaking private information. This loss of confidentiality must be considered the cost of transparency.

5 Related Work

Blockchain and Taxation. Several authors proposed the use of blockchain technology to increase tax compliance. For example, Wijaya et al. [7] present a blockchain-based VAT system that technically binds invoicing to the successful payment of the included tax. The system relies on a private distributed ledger maintained by the tax administration and thus achieves a high level of confidentiality. However, the design restricts transparency concerning the processing of tax transactions. In contrast, Hoffmann [8] argues that efficient taxation requires a trade-off between privacy and transparency. Therefore, the sketched solution includes a permissioned blockchain that enables the implementation of access control policies. Hyvärinen et al. [9] present a blockchain solution to combat fraud caused by forged refund applications in the context of dividend taxes. The authors state that transparency in blockchains must be restricted when dealing with sensitive tax data. Furthermore, there exist several concepts on establishing a blockchain-based VAT system [10, 14, 15]. These concepts rely on private distributed ledgers and encryption to ensure confidentiality of VAT data.

The described private and permissioned blockchain solutions reintroduce trust assumptions and restrict verifiability to the participants of a transaction. This approach decreases transparency and prevents the public from verifying transactions. Consequently, the adoption of public unpermissioned blockchains has been proposed. In [11] the authors state that increased transparency reduces compliance costs and makes tax evasion more difficult. The authors argue that ZKPs allow controlling the degree of transparency [11]. In a previous work [12, 13], we rely on a public blockchain to enable compliance with documentation obligations related to VAT.

https://doi.org/10.30844/wi_2020_l1-fatz

Confidentiality is guaranteed by partially encrypting tax data, while smart contracts enable a transparent processing of VAT-related transactions.

Confidentiality-preserving Blockchains. Many authors address the challenge of providing confidentiality in blockchain-based systems. Zerocash [36] utilizes ZKPs to prevent the tracking of cryptocurrency coins and enable anonymous payments. The concepts of Zerocash laid the foundation for the cryptocurrency Zcash[1]. Kosba et al. [37] present the concept of privacy-preserving smart contracts. Similar to Zerocash, the authors use ZKPs to provide validation and computation on sensitive data while preserving confidentiality. The framework includes a compiler that automatically translates smart contracts into a corresponding cryptographic protocol. Enigma [38] adopts another technology by relying on multi-party computation. The protocol distributes the validation of private data among several parties so that only the final result is revealed. Narula et al. [39] propose the use of ZKPs to support third-party auditing. In the proposed architecture, properties of the ledger can be proven without revealing individual transactions. In the context of automatic transaction processing, Wang and Kogan [40] conduct a similar approach. The processing system validates transactions based on the attached ZKP.

6 Conclusion

The main contribution of our work is the conceptual design of a decentralized and confidentiality-preserving tax document exchange system. The system enables transparency by implementing publicly verifiable compliance checks.

Investigating current challenges in taxation and blockchain technology revealed a major conflict between the two opposing objectives of transparency and confidentiality. While a certain degree of transparency increases trust into the tax system, obliging organizations to disclose sensitive business information might harm the relationship between businesses, tax administrations, and the public [20]. In this context, the proposed application of ZKPs solves the dilemma by balancing the transparency benefits against the disadvantages of confidentiality losses. Research in the field of cryptography has led to many sophisticated protocols, which still must be transferred into the application. The present work takes a first step in this direction by using zk-SNARKs to enforce tax compliance. Notably, the approach taken is fundamentally different from other blockchain-based systems in this field. By relying on a public blockchain, we build a fully decentralized environment in which tax administrations and businesses exchange and validate information. The presented approach contributes to reducing reporting obligations while maintaining a high level of tax compliance. However, ongoing research on the performance of public blockchains and ZKPs is vital to the success of the outlined solution.

[1] http://www.z.cash

https://doi.org/10.30844/wi_2020_l1-fatz

Acknowledgments. This work was conducted within a project partly sponsored by the German Ministry for Education and Research (BMBF), project name ProcessChain, support code 01IS17086B.

References

1. Richardson, G.: Determinants of tax evasion: A cross-country investigation. Journal of International Accounting, Auditing and Taxation 15, 150–169 (2006).
2. World Bank Group: Doing Business 2017: Equal Opportunity for All. (2016).
3. Center for Social and Economic Research (CASE), Institute for Advanced Studies: Study and Reports on the VAT Gap in the EU-28 Member States: 2018 Final Report: TAXUD/2015/CC/131.
4. Bundesministerium der Finanzen: Gesetz zur Modernisierung des Besteuerungsverfahrens.
5. Putz, R.: Italien als digitaler Vorreiter: Flächendeckende Verpflichtung zur E-Rechnung B2B und B2C eingeführt. Rethinking Tax 1, 62–67 (2019).
6. Owens, J.: Tax Transparency and BEPS. Journal of Tax Administration 1, 5–14 (2015).
7. Wijaya, D. A., Liu, J. K., Suwarsono, D. A., Zhang, P.: A New Blockchain-Based Value-Added Tax System. In: International Conference on Provable Security (ProvSec), pp. 471–486 (2017).
8. Hoffman, M.: Can Blockchains and Linked Data Advance Taxation. In: Companion Proceedings of the The Web Conference (WWW), pp. 1179–1182 (2018).
9. Hyvärinen, H., Risius, M., Friis, G.: A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. Business & Information Systems Engineering 59, 441–456 (2017).
10. Ainsworth, R. T., Shact, A.: Blockchain (Distributed Ledger Technology) Solves VAT Fraud. SSRN Electronic Journal (2016).
11. Lyons, T., Courcelas, L., Timsit, K.: Blockchain for Government and Public Services. (2018).
12. Fatz, F., Fettke, P., Hake, P., Risse, R.: Potenziale von Blockchain-Anwendungen im Steuerbereich. HMD Praxis der Wirtschaftsinformatik 55, 1231–1243 (2018).
13. Fatz, F., Hake, P., Fettke, P.: Towards Tax Compliance by Design: A Decentralized Validation of Tax Processes Using Blockchain Technology. In: Proceedings of the IEEE Conference on Business Informatics (CBI), pp. 559-568 (2019).
14. Ainsworth, R. T., Alwohaibi, M., Cheetham, M.: VATCoin: The GCC's Cryptotaxcurrency. SSRN Electronic Journal (2017).
15. Ainsworth, R. T., Alwohaibi, M.: Blockchain, Bitcoin, and VAT in the GCC: The Missing Trader Example. SSRN Electronic Journal (2017).
16. German Federal Office for Information Security: BSI-Standard 100-2: IT-Grundschutz Methodology. (2008).
17. Mendling, J., Weber, I., van der Aalst, W. M. P., vom Brocke, J., Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., Gal, A., García-Bañuelos, L., Governatori, G., Hull, R., La Rosa, M., Leopold, H., Leymann, F., Recker, J., Reichert, M., Reijers, H. A., Rinderle-Ma, S., Solti, A., Rosemann, M., Schulte, S., Singh, M. P., Slaats, T., Staples, M., Weber, B., Weidlich, M., Weske, M., Xu, X., Zhu, L.: Blockchains for Business Process Management - Challenges and Opportunities. ACM Transactions on Management Information Systems 9, 4:1–4:16 (2018).

https://doi.org/10.30844/wi_2020_l1-fatz

18. Peffers, K., Tuunanen, T., Rothenberger, M. A., Chatterjee, S.: A design science research methodology for Information Systems Research. Journal of Management Information Systems 24, 45–77 (2007).
19. International Organization for Standardization (ISO) and International Electrotechnical Commission: ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements (2005).
20. Owens, J.: Tax Transparency: The „Full Monty“. Bulletin for International Taxation 68 (2014).
21. Karajovic, M., Kim, H. M., Laskowski, M.: Thinking Outside the Block: Projected Phases of Blockchain Integration in the Accounting Industry. Australian Accounting Review 29, 319–330 (2019).
22. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, http://www.bitcoin.org/bitcoin.pdf [Accessed: 29.10.2019] (2009).
23. Yu, T., Lin, Z., Tang, Q.: Blockchain: The Introduction and Its Application in Financial Accounting. Journal of Corporate Accounting & Financ 29, 37–47 (2018).
24. Viriyasitavat, W., Hoonsopon, D.: Blockchain characteristics and consensus in modern business processes. Journal of Industrial Information Integration 13, 32–39 (2019).
25. Benet, J.: IPFS - Content Addressed, Versioned, P2P File System. arXiv:1407.3561 (2014).
26. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman & Hall/CRC (2014).
27. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM Journal on Computing 18, 186–208 (1989).
28. Bitansky, N., Chiesa, A., Ishai, Y., Paneth, O., Ostrovsky, R.: Succinct Non-interactive Arguments via Linear Interactive Proofs. In: Proceedings of the Theory of Cryptography Conference (TCC), pp. 315–333 (2013).
29. Beck, R., Avital, M., Rossi, M., Thatcher, J. B.: Blockchain Technology in Business and Information Systems Research. Business & Information Systems Engineering 59, 381–384 (2017).
30. Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., Tan, K.-L.: BLOCKBENCH: A Framework for Analyzing Private Blockchains. In: Proceedings of the ACM International Conference on Management of Data (SIGMOD), pp. 1085–1100 (2017).
31. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014).
32. Eberhardt, J., Tai, S.: ZoKrates - Scalable Privacy-Preserving Off-Chain Computations. In: Proceedings of the IEEE International Conference on Blockchain (2018).
33. Truffle, https://truffleframework.com [Accessed: 24.10.2019].
34. Pedersen, T. P.: Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: Proceedings of the Annual International Cryptology Conference (CRYPTO), pp. 129–140 (1992).
35. Bowe, S., Gabizon, A., Green, M. D.: A Multi-party Protocol for Constructing the Public Parameters of the Pinocchio zk-SNARK. In: Proceedings of the International Conference on Financial Cryptography and Data Security (FC), pp. 64–77 (2019).
36. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: Proceedings of the IEEE Symposium on Security and Privacy (SP) (2014).
37. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In: Proceedings of the IEEE Symposium on Security and Privacy (SP), pp. 839–858 (2016).

https://doi.org/10.30844/wi_2020_l1-fatz

38. Zyskind, G., Nathan, O., Pentland, A.: Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv:1506.03471 (2015).
39. Narula, N., Vasquez, W., Virza, M.: zkLedger: Privacy-Preserving Auditing for Distributed Ledgers. In: Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI), pp. 65–80 (2018).
40. Wang, Y., Kogan, A.: Designing confidentiality-preserving Blockchain-based transaction processing systems. International Journal of Accounting Information Systems 30, 1–18 (2018).

https://doi.org/10.30844/wi_2020_l1-fatz