Journal of
Risk and Financial Management

MDPI

Article

A Private and Efficient Triple-Entry Accounting Protocol on Bitcoin

Liuxuan Pan *, Owen Vaughan and Craig Steven Wright

nChain Ltd., 30 Market Place, London W1W 8AP, UK; o.vaughan@nchain.com (O.V.); c.wright@nchain.com (C.S.W.)
* Correspondence: l.pan@nchain.com

Abstract: The 'Big Four' accountancy firms dominate the auditing market, auditing almost all the Financial Times Stock Exchange (FTSE) 100 companies. This leads to people having to accept auditing results even if they may be poor quality and/or for inadequate purposes. In addition, accountants may provide different auditing results with the same financial data. These issues are hard for regulators such as the Financial Reporting Council to identify because of insufficient resources or inconsistent compliance. In this paper, we proposed a triple-entry accounting protocol to allow users to report Bitcoin transactions to a third-party auditor to comply with regulations such as the travel rule. It allows the auditor to easily detect anomalies and identify the non-compliant parties, whilst the blockchain itself provides a transparent and immutable record of these anomalies. Despite building on a public ledger, our solution preserves privacy and offers an interoperability layer for information exchange. Merkle proofs were used to record non-compliant transactions whilst allowing compliant transactions to be pruned from an auditor's active database.

Keywords: triple entry accounting; bitcoin; blockchain; privacy; auditing

Citation: Pan, Liuxuan, Owen Vaughan, and Craig Steven Wright. 2023. A Private and Efficient Triple-Entry Accounting Protocol on Bitcoin. *Journal of Risk and Financial Management* 16: 400. https://doi.org/10.3390/jrfm16090400

Academic Editor: Eva R. Porras

Received: 18 July 2023
Revised: 25 August 2023
Accepted: 28 August 2023
Published: 7 September 2023

1. Introduction

Triple Entry Accounting (TEA) is an innovative discovery in the field of accounting and is considered as an extension of double-entry accounting (Grigg 2005). Between 1995 and 1997, Grigg introduced the concept of triple-entry accounting, which combined financial information from two companies into a single transaction receipt. This transaction receipt includes cryptographic signatures and constitutes the origin of triple entry (Ibañez et al. 2023). Independent in 1997, Boyle proposed the idea of shared ledger, which allowed two parties to communicate transactions in a single shared transaction repository. The two streams converged into TEA in 2005. In traditional double-entry accounting, a receipt for a financial transaction is issued by a central party, such as a bank, to commit the transaction between a payer and a payee. Grigg questioned this traditional accounting model, arguing that the central party has excessive power and this could result in the central party committing fraud using receipts (Simoyama et al. 2017). To mitigate this risk, the TEA model was proposed to ensure that all involved parties receive the same receipt for that financial transaction. Such a receipt includes all related parties' signatures to ensure data integrity of the receipt.

The concept of TEA is sometimes confused with triple-entry bookkeeping (TEB). Ibañez et al. classified the distinction as bookkeeping is simply recording transactions in sequence (Ibañez et al. 2021a) while accounting is the process of summarizing and analysing company information based on bookkeeping to help the company make decisions (Ibañez et al. 2021b). Thus, definitions of bookkeeping and accounting are inherited by TEA and TEB. TEB systems simply use the triple-entry method to record transactions, and TEA systems add an accounting layer on the top of TEB (Ibañez et al. 2021a). Additionally, in Grigg's TEA, 'entry' represents a signature record which is a signed message by a party, or simply a signature, and TEA is a 'signature gathering process' (Ibañez et al. 2023).

Grigg's TEA concept relies on a trusted third party with the shared ledger, and this makes it challenging to implement in the real accounting world (Singh et al. 2021). With the advent of Bitcoin (Nakamoto 2008), it becomes practicable as the Bitcoin blockchain can replace the role of the trusted third party, making TEA increasingly viable. In other words, Bitcoin simply uses the triple-entry method to record transactions. It is worth noting that Bitcoin is a TEB system, but it can become a TEA by adding an accounting layer on top (Ibañez et al. 2023). The accounting layer will record transactions in a systematic and controlled method to facilitate business events such as tax reporting and invoicing. In general, unspent transaction output (UTXO)-based blockchains can be regarded as TEA examples (Grigg 2011). The blockchain-integrated TEA solutions are used to improve the efficiency of processing data, reduce the risk of human error, enable fully automated auditing, and save time and costs in reporting, tax filing, payment, and compliance (Ibañez et al. 2021b; Faccia and Mosteanu 2019; Baba et al. 2021).

Not all blockchains can immediately enable TEA. Some of them need to run smart contracts to enable a TEA system, for instance, the account-based blockchains like Ethereum and managed ledgers such as Ripple (XRP ledger) (Grigg 2017). In addition, some existing blockchain-based TEA systems are facing a scalability issue. To resolve this issue, these systems propose a second layer or off-chain solution, e.g., the Request network (Request 2018), or to use a permissioned ledger, e.g., Hyperledger (Ibañez et al. 2021b). The Request TEA system (Request 2018), built on top of Ethereum blockchain, adopts an InterPlanetary File System to store data and partially use the blockchain for time stamping. These solutions can partially address the problem, but they still inherit the disadvantages of the adopted ledgers, such as the poor stability of Ethereum and the low transparency of Ripple and Hyperledger (Joseph et al. 2022).

Recent collapses of cryptocurrencies such as FTX collapse (Vidal-Tomás et al. 2023) and Terra luna crash (Liu et al. 2023) may affect people's perception of blockchain technology's capabilities and potential, especially when solutions are deployed on cryptocurrency-powered blockchains. While cryptocurrencies are the most well-known application of blockchain technology, cryptocurrency collapses will not end blockchain itself. Blockchain has proven valuable beyond cryptocurrencies and can continue to evolve in many industries even if specific cryptocurrencies face challenges and different types of attacks appear (Gountia 2019).

There are significant costs associated with auditing financial data. The UK publicly listed companies paid more than £1bn to audit firms in 2021 (Financial Reporting Council 2022). It is anticipated by the Financial Reporting Council (FRC) that new auditing solutions can reduce audit fees and improve the audit quality (Financial Reporting Council 2022). Although blockchains are decentralised, they are by no means exempt from auditing and the high associated costs. In fact, long-established regulations such as the *travel rule*, which stipulates that transactions over a certain value must be reported to a financial authority, are immediately applicable to Bitcoin and other decentralised cash systems, and, therefore, an auditing system is required.

It was the goal of this paper to allow users of Bitcoin to be audited in a manner that leverages the transparency and immutability of the blockchain whilst promoting on-chain privacy. We carried this out by developing a TEA protocol on Bitcoin that is efficient and practical. The starting point is to allow users to establish an off-chain link between invoices and identity information with on-chain transactions used for payments. Users then individually submit transactions to a third-party auditor and anomalies are detected if one user submits a transaction that their counterparty does not submit. In this case, the auditor can request the identity information of the non-compliant counterparty which is provably linked to the transaction.

The advantages of our scheme are as follows.

- All transactions are automatically audited in real-time. The blockchain provides transparency, immutability, and availability of transaction data.

- Our protocol is private in the sense that an adversary monitoring the blockchain will learn nothing about users' identities or the details of the invoices. This is because identity and invoice information are linked to on-chain public keys in a manner that cannot be inferred by inspecting public keys alone.
- Before a payment is made, the two transacting parties exchange identity information that will be linked to a single on-chain transaction. Once the transaction is published on the blockchain, a user can use the identity information and a Simplified Payment Verification (SPV) (Nakamoto 2008) proof to independently prove that their counterparty has taken part in the transaction.
- After a predefined time period, e.g., one day, each user makes a commitment to the third-party auditor of the transactions they have made. This commitment is stored on the blockchain and, so, cannot be changed retrospectively.
- A Merkle root is used for the commitment of a user's transactions to an auditor. This makes it efficient for a user to prove that they have included a specific transaction in the commitment when challenged. It is also private in the sense that the user does not need to give information about any other transactions during such a challenge.
- If all users are compliant, then they are never asked to provide identity information to the auditor. If one party is non-compliant, the compliant party can provide independent proof to the auditor of their own compliance and their counterparty's involvement in the transaction.

The paper is organized as follows: Section 2 provides an overview of Bitcoin as a TEB system, the travel rule, and how identity can be linked to a public key but still preserve privacy on the blockchain. In Section 3, we outline our invoice auditing protocol including the method of embedding the invoice into the blockchain and verifying it. The protocol also describes how the auditor can efficiently and automatically check the data integrity of all related invoices. We end with a conclusion in Section 4.

2. Preliminaries

In this section, we discuss how Bitcoin can be interpreted as a TEB system, the travel rule, and how identity can be linked to a public key (United States Department of the Treasury Financial Crimes Enforcement Network 1997).

2.1. Bitcoin and Triple Entry Bookkeeping

Bitcoin is the first and most well-known distributed ledger. The auditing solution in this paper is presented in terms of the original design of Bitcoin, which is currently embodied by the Bitcoin Satoshi Vision (BSV) protocol. This design offers scalability, data integrity, transparency, low cost, and high transaction throughput (Joseph et al. 2022). Grigg stated that a signed receipt or invoice can be considered as a transaction recorded on a shared transaction repository (Grigg 2005). Such an invoice transaction involves three entities' signatures and is used to refer to the payment event.

Figure 1 shows an example of Bitcoin performing as a TEB system. Suppose Alice and Bob are two parties, and their payments are recorded in the Bitcoin TEB system. Invoices are recorded in the form of Bitcoin transactions, and the associated debit and credit can be traced with the related transaction. For instance, Alice pays Bob for the invoice IV_1 and records this payment on the blockchain using the $TXID_1$. The transaction $TXID_1$ includes Alice's signature associated with her credit I_{A_1}, Alice's public key linked to the invoice IV_1 and her debit C_{A_1}, and Bob's public key associated with his Debit O_{B_1} and IV_1. All information from $TXID_1$ can be stored in Alice or Bob's off-chain ledger in a consistent manner. Notably, the auditor does not need to access their off-chain ledgers but can track all records from the Bitcoin blockchain.

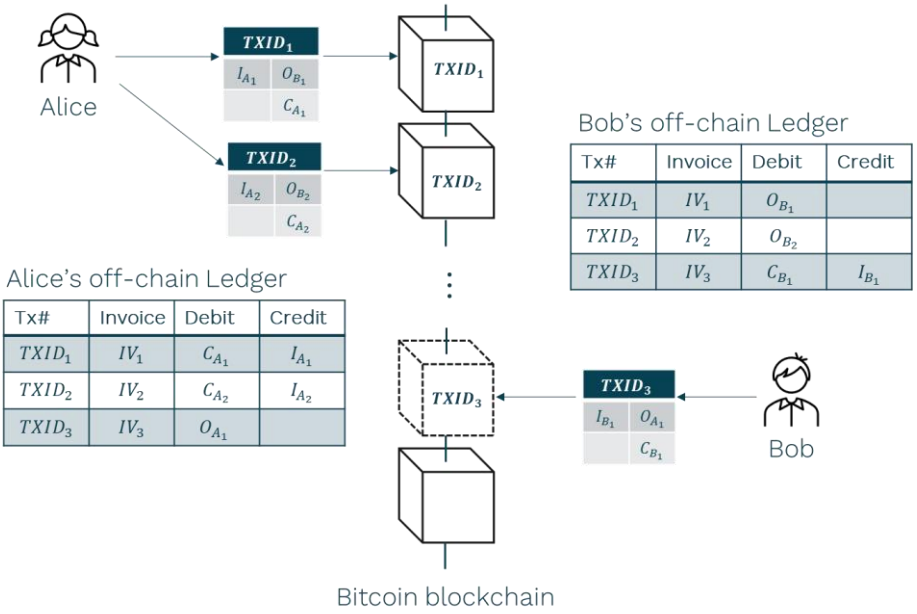

Figure 1. Bitcoin as a TEB system (processed by the authors with the help of PowerPoint, Tx# stands for the transaction number).

2.2. Travel Rule

The Travel Rule (United States Department of the Treasury Financial Crimes Enforcement Network 1997) requires financial institutions to send the originator and beneficiary information for each transaction over USD 3000 within the US, and over EUR 1000 in the EU (European Union 2023; United States Department of the Treasury Financial Crimes Enforcement Network 1997). It was extended by the Financial Action Task Force (FATF) in 2019 to include virtual assets (VA) and virtual asset service providers (VASP). FATF defines VA as 'the digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes', and VASP as 'a business conducting one or more of the following activities or operations for or on behalf of another natural or legal person' including 'exchange between virtual assets and fiat currencies', 'exchange between one or more forms of virtual assets', and 'transfer of virtual assets' (Financial Action Task Force 2019). Thus, we assume that Bitcoin transaction service providers such as wallets are virtual asset service providers and must comply with the Travel Rule and FATF obligations.

2.3. Identity-Linked Public Key

Suppose Alice owns a wallet with a master public key PK_{MA} associated with her identity. This can be achieved by obtaining a digital certificate on PK_{MA} from a Certificate Authority (CA). However, the public key that Alice uses in the transaction, e.g., $TXID_1$, is PK_A, which is different from her master key. PK_A is typically derived from PK_{MA} in a deterministic way. For example, we have Alice's master public key PK_{MA}, Bob's master public keys PK_{MB} and an additional data m such as an invoice or other metadata known to both Alice and Bob. Then, Alice's public key PK_A can be derived such that

$$PK_A = PK_{MA} + \text{HMAC-256}((V_{MA} \times PK_{MB}), m) \times G, \quad (1)$$

where HMAC refers to a Hash-based Message Authentication Code that is used to verify integrity and authenticity of messages, V_{MA} is the master private key with respect to PK_{MA} and G is the elliptic curve generator point. Note that $V_{MA} \times PK_{MB} = V_{MB} \times PK_{MA}$ is a shared secret between Alice and Bob. A similar key PK_B can also be derived for Bob.

This features both Alice and Bob to provide a provable link PK_A with PK_{MA}, PK_{MB} and m. However, without the knowledge of how the key is derived, someone looking at transaction $TXID_1$ could not link the key to Alice. According to the FATF, Alice's wallet

needs to provide the provable link of PK_A with PK_{MA} to Bob, and the same applies to Bob's wallet. There are alternative approaches of linking identity and invoice data to a public key which are explored in Section V of Benford's Wallet (Tartan et al. 2022).

3. Invoice Auditing Protocol

In the auditing process, it is necessary to verify the accuracy and completeness of invoices. However, invoice verification can be time-consuming, and it is not easy for auditors to detect all invoices and mistakes related to these invoices. The traditional way for the auditor is to randomly select a valid sample of invoices and detect the possible mistakes from this sample. One blockchain solution has been provided to solve this issue through publishing a blockchain transaction, which includes the hash values associated with invoices (Vincent et al. 2020). However, there is a problem with this solution that the invoices that are hashed directly on the blockchain can be easily traced if compromised. Our solution will solve this problem without including any hash values on the blockchain but still allowing stakeholders to verify the data integrity of the invoices.

We proposed an invoice-auditing protocol on top of Bitcoin, which allows entities to independently verify the invoices and auditors to efficiently match transactions associated with those invoices. This protocol can improve the auditing process and save time for auditors. Furthermore, this makes auditing automatic and checking all invoices possible (instead of a random selection). An invoice auditing overview is given in Figure 2.

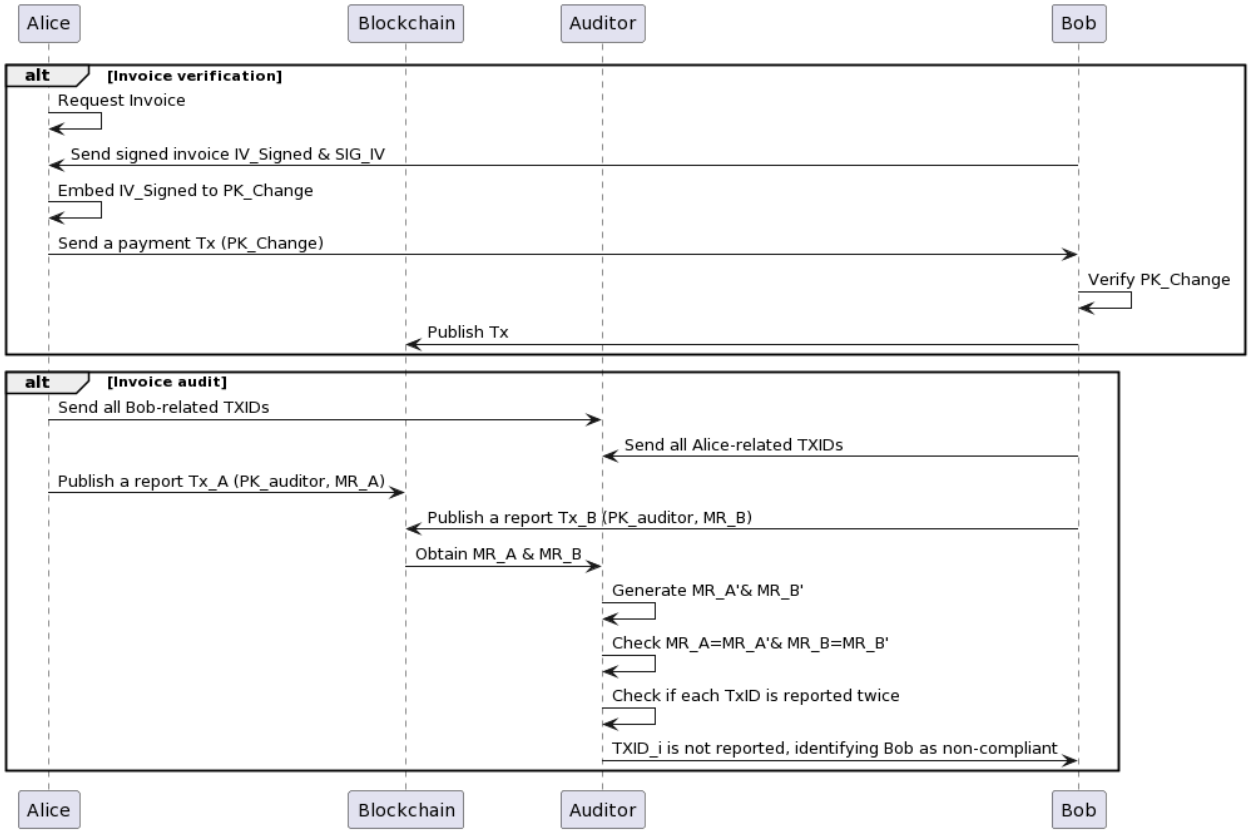

Figure 2. Bitcoin-based invoice-auditing protocol overview (processed by the authors with the help of the program PlantText UML).

It is implemented in two stages: invoice verification and transaction matching.

- Invoice verification—this makes the invoice verifiable by entities but without disclosing information of the invoice on the blockchain;
- Invoice audit—this allows the auditor to audit all invoices and the related payments in an efficient way.

3.1. Invoice Verification

Invoice verification refers to the process of reviewing and verifying invoices for accuracy, completeness, and valid authorization from each party. The auditor needs to check that invoices have been approved by appropriate parties and have not been tampered with.

In our auditing model, we assumed that the invoice is recorded in a Bitcoin transaction and is independently verifiable by entities. This section will introduce how an invoice is embedded in the Bitcoin transaction and can be mutually authenticated, and then describe how the auditor verifies the data integrity of the invoice based on the transaction.

Record and Sign Invoice

We suppose that Alice and Bob are the transaction-related parties. To comply with Travel Rule and FATF regulations (United States Department of the Treasury Financial Crimes Enforcement Network 1997; Financial Action Task Force 2019), they need to exchange information off-chain which provably links their identity to the transaction. For example, we assume that they have a well-known public key, denoted, respectively, as PK_{AC} and PK_{BC}, to identify each other and establish an authenticated and confidential communication channel to exchange the invoices. However, it is worth noting that these two public keys, PK_{AC} and PK_{BC}, are never used to send or receive any Bitcoin payments. In other words, they will not appear on the blockchain.

Bob generates an invoice (IV) and signs it with the private key related to PK_{BC}. Here, we assume the Elliptic Curve Digital Signature Algorithm (ECDSA) with secp256k1 is used to sign the invoice, and the signature is denoted as SIG_{IV}. The signed invoice indicates that Bob will provide the goods or services if Alice completes the payment to the invoice IV. Alice can verify SIG_{IV} with the given invoice and PK_B. If SIG_{IV} is not valid, Alice will not make the payment. If SIG_{IV} is invalid because the given invoice is not one signed by Bob, Alice can require Bob to resend SIG_{IV} that should be generated with the correct invoice.

If Alice requires amendments to the invoice, Bob updates the contents of the invoice and regenerates a digital signature of each new iteration of the invoice until both parties reach a final agreement. Having arrived at an agreement, Alice verifies the signature SIG_{IV}, to ensure that Bob signs the agreed invoice.

When Alice and Bob reach an agreement about the invoice, they create new public keys to be used in the transaction. These public keys should be related to their identity and the invoice in the manner given in Equation (1). Concretely, Bob creates a public key PK_B to receive funds and Alice creates a public key PK_{change} to be used as a change address. These keys are calculated as follows.

$$PK_B = PK_{BC} + \text{HMAC-256}((V_{BC} \times PK_{AC}), IV_{Signed}) \times G \tag{2}$$

$$PK_{change} = PK_{AC} + \text{HMAC-256}((V_{AC} \times PK_{BC}), IV_{Signed}) \times G \tag{3}$$

where $IV_{Signed} = \text{SHA-256}(IV||SIG_{IV})$, and SHA-256 is a cryptographic hash function that outputs a fixed-length 256-bit hash value.

Bob sends a payment transaction template containing PK_B to Alice. To complete the transaction, Alice adds her change address PK_{change} to the outputs and a funding UTXO in the input along with a valid signature. (Note that the public key used in the input UTXO may be linked to Alice's identity as well.)

The finalised transaction is displayed in Table 1. PK_A described in Section 2.3 is used by Alice to make the payment, and SIG_A is the associated signature. The value x is the payment amount that Alice agrees to pay to Bob, and y is the change that Alice will receive after completing the payment.

Note that the invoice is embedded within the public keys used in outputs of the above transaction, but it is not disclosed directly on the blockchain either in its raw form or a hash. Therefore, even if the invoice is leaked, it will be difficult to track the related transaction

without the invoice-signed signature SIG_{IV} and identity-related public keys. To ensure their relationship is untraceable, signatures and public keys are not stored along with the invoice.

Table 1. A payment transaction sent from Alice to Bob (processed by the authors with the help of Word).

$TXID_1$			
Inputs		**Outputs**	
Outpoint	**Unlocking Script**	**Value**	**Locking Script**
$UTXO_A$	$<SIG_A>$ $<PK_A>$	x	OP_DUP OP_HASH160 $<H(PK_B)>$ OP_EQUALVERIFY OP_CHECKSIG
		y	OP_DUP OP_HASH160 $<H\left(PK_{change}\right)>$ OP_EQUALVERIFY OP_CHECKSIG

3.2. Invoice Audit

The auditor requests Bob to provide the following information to check the accuracy and completeness of the invoices: the shared secret $V_{BC} \times PK_{AC}$, the invoice IV, SIG_{IV}, and $TXID_1$. The auditor can then verify SIG_{IV} against PK_{BC}. If SIG_{IV} is valid, the auditor generates the change public key using Equation (3) and compares it with PK_{change} in the locking script. If it matches, the auditor can confirm that the invoice embedded into the PK_{change} is the same as the invoice Bob provides to Alice. All invoices can be audited using this way and, more importantly, this can be carried out automatically. However, if checked only from Bob's side, the auditor cannot be sure that Bob has provided all transactions and invoices related to Alice. Therefore, the auditor also requires Alice to report all related transaction IDs.

Transaction Compliance

The first step is for the auditor to ask for a commitment from Alice and Bob as to the transactions they have reported. To make the process more efficient, the auditor can require, e.g., Bob to gather all his transactions in a regular period, e.g., one month, to construct a Merkle tree with Merkle root MR_B. That is, the auditor is checking the equality of transactions in batches. The auditor also requires Bob to report MR_B using a Bitcoin transaction. As shown in Table 2, the report transaction specifies the output to the auditor's public key $PK_{auditor}$ and embeds MR_B as an OP_RETURN data payload. The value z is the dust value, which is the minimum amount accepted by Bitcoin nodes. We assume that the $PK_{auditor}$ is certified and given to Alice and Bob beforehand.

Table 2. A report transaction sent from Bob to Auditor (processed by the authors with the help of Word).

$TXID_{report_B}$			
Inputs		**Outputs**	
Outpoint	**Unlocking Script**	**Value**	**Locking Script**
$UTXO_B$	$<SIG'_B>$ $<PK'_B>$	z	OP_DUP OP_HASH160 $<H(PK_{auditor})>$ OP_EQUALVERIFY OP_CHECKSIG
		0	OP_FALSE OP_RETURN $<MR_B>$

After receiving MR_B from $TXID_{report_B}$, the auditor calculates the Merkle root MR'_B of all $TXIDs$ that Bob has sent that month, and checks $MR_B = MR'_B$. If they are not equal, the auditor requires Bob to resubmit a new MR_B. The auditor also requires Alice to submit the similar report transaction including MR_A. We apply the same process to check $MR_A = MR'_A$.

The above step is intended for the audit to check that the auditor has accurately received all transactions that were reported individually by Alice and Bob. If this is the case,

the auditor can then check if the transactions match. Namely, the auditor should receive the same transaction ID twice, one from Alice and the other from Bob. If a transaction ID only appears once, then the auditor knows that someone has not reported their transaction. If this is the case, the auditor asks the party who reported the transaction for the identity and invoice information about the party who did not report the transaction. Recall that this identity and invoice information is provably linked to the transaction, and available to both parties.

For example, if there is a transaction reported by Alice and not by Bob, the auditor asks Alice for the transaction, Bob's identity information, and the invoice. The auditor can then contact Bob with evidence of non-compliance and ask him for an explanation. In our simple example, there are just two parties, Alice and Bob, and so, it is obvious who has not reported their transaction. But it easily extends to multiple parties where it becomes necessary for the auditor to specifically ask the compliant party who their non-compliant counterparty was in the transaction.

4. Conclusions

This paper introduced a Bitcoin-based TEA protocol that allows transaction-related parties to verify invoices and manage their off-chain ledger in a consistent manner. This can reduce the risk of running fraudulent invoices. It also provides transparency and data integrity of invoices to the auditor or tax regulator by embedding them into transactions but not disclosing any information on the blockchain. The protocol adopted the Merkle tree structure to consolidate related transactions from both parties. This enables auditors to efficiently identify the non-compliant party.

Our TEA protocol only introduced the example of one transaction per invoice and was mixed up with payment method. Parties willing to use this protocol need to pay with satoshis. To improve the protocol, future work includes allowing parties willing to use this TEA protocol to make payments in other ways and only use the blockchain for auditability; batching multiple invoices in a single transaction if payments are decoupled from the audit process.

Author Contributions: Conceptualization, L.P., O.V. and C.S.W.; methodology, L.P. and O.V.; software, L.P.; resources, L.P.; writing—original draft preparation, L.P.; writing—review and editing, O.V.; visualization, L.P.; supervision, O.V.; project administration, L.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

Baba, Asif Iqbal, Subash Neupane, Fan Wu, and Fanta F. Yaroh. 2021. Blockchain in Accounting: Challenges and Future Prospects. *International Journal of Blockchains and Cryptocurrencies* 2: 44–67. [CrossRef]

European Union. 2023. Official Journal L 150/2023. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2023:150:FULL (accessed on 26 June 2023).

Faccia, Alessio, and Narcisa Roxana Mosteanu. 2019. Accounting and Blockchain Technology: From Double-Entry to Triple-Entry. *The Business and Management Review* 10: 108–16.

Financial Action Task Force. 2019. Virtual Assets and Virtual Asset Service Providers. Available online: www.fatf-gafi.org (accessed on 27 June 2023).

Financial Reporting Council. 2022. Competition in the Audit Market—A Policy Paper. Available online: https://www.frc.org.uk/getattachment/83bb5ce5-891f-46b1-af84-799fd3d5ee39/Competition-in-the-audit-market-_-2022.pdf (accessed on 27 June 2023).

Gountia, Debasis. 2019. Towards Scalability Trade-off and Security Issues in State-of-the-Art Blockchain. *ICST Transactions on Security and Safety* 5: 157416. [CrossRef]

Grigg, Ian. 2005. *Triple Entry Accounting*. Itasca: Systemics Inc., pp. 1–10. [CrossRef]

Grigg, Ian. 2011. Is BitCoin a Triple Entry System? Available online: https://financialcryptography.com/mt/archives/001325.html (accessed on 27 August 2023).

Grigg, Ian. 2017. EOS: An Introduction. Available online: http://iang.org/ (accessed on 26 June 2023).
Ibañez, Juan Ignacio, Chris N. Bayer, Paolo Tasca, and Jiahua Xu. 2021a. Triple-Entry Accounting, Blockchain and next of Kin: Towards a Standardization of Ledger Terminology. Available online: https://ssrn.com/abstract=3760220 (accessed on 26 June 2023).
Ibañez, Juan Ignacio, Chris N. Bayer, Paolo Tasca, and Jiahua Xu. 2021b. The Efficiency of Single Truth: Triple-Entry Accounting. Available online: https://ssrn.com/abstract=3770034 (accessed on 26 June 2023).
Ibañez, Juan Ignacio, Chris N. Bayer, Paolo Tasca, and Jiahua Xu. 2023. REA, Triple-Entry Accounting and Blockchain: Converging Paths to Shared Ledger Systems. *Journal of Risk and Financial Management* 16: 382. [CrossRef]
Joseph, Daniel, Yuen Lo, Alessio Pagani, Liuxuan Pan, and Vlad Skovorodov. 2022. Chapter 1. Ledger Comparative Analysis. In *Blockchain Technology: Advances in Research and Applications*. Edited by Eva R. Porras. New York: Nova. [CrossRef]
Liu, Jiageng, Igor Makarov, and Antoinette Schoar. 2023. Anatomy of a Run: The Terra Luna Cras. Available online: http://www.nber.org/papers/w31160 (accessed on 27 August 2023).
Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. San Jose: Bitcoin.org.
Request. 2018. Whitepaper Request Network the Future of Commerce a Decentralized Network for Payment Requests. Available online: http://gavwood.com/paper.pdf (accessed on 27 June 2023).
Simoyama, Felipe de Oliveira, Ian Grigg, Ricardo Luiz Pereira Bueno, and Ludmila Cavarzere De Oliveira. 2017. Triple Entry Ledgers with Blockchain for Auditing. *International. Journal Auditing Technology* 3: 163–83. [CrossRef]
Singh, Kishore, Amlan Haque, Sabi Kaphle, and Janice Joowon Ban. 2021. Distributed Ledger Technology—Addressing the Challenges of Assurance in Accounting Systems: A Research Note. *Journal of Accounting and Management Information Systems* 20: 646–69. [CrossRef]
Tartan, Chloe Ceren, Wei Zhang, Owen Vaughan, and Craig Steven Wright. 2022. Benford's Wallet. Paper presented at 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), Irvine, CA, USA, November 7–11.
United States Department of the Treasury Financial Crimes Enforcement Network. 1997. Travel Rule. Available online: http://www.fincen.gov (accessed on 27 June 2023).
Vidal-Tomás, David, Antonio Briola, and Tomaso Aste. 2023. FTX's Downfall and Binance's Consolidation: The Fragility of Centralized Digital Finance, February. *arXiv* arXiv:2302.11371. [CrossRef]
Vincent, Nishani Edirisinghe, Anthony Skjellum, and Sai Medury. 2020. Blockchain Architecture: A Design That Helps CPA Firms Leverage the Technology. *International Journal of Accounting Information Systems* 38: 100466. [CrossRef]