Journal of
Risk and Financial Management

Technical Note

Implementing Triple Entry Accounting as an Audit Tool—An Extension to Modern Accounting Systems

Torje Vingen Sunde [1,*] and Craig S. Wright [2]

[1] Abendum AS, 0566 Oslo, Norway
[2] Computer Science Department, University of Exeter, Exeter EX4 4QJ, UK; craigwright@acm.org
* Correspondence: torje@abendum.com

Abstract: Despite the technological leaps modern accounting systems have brought about, fraud is still prevalent. This necessitates spending time and money on audits. Connecting modern accounting ledgers to a public blockchain would make accounting records easily verifiable, aiding the audit evidence gathering and analytics process. Continuous audits will be made viable by readily available audit evidence from the public blockchain. The proposed audit solution creates verifiable "Financial Fingerprints" (signed indexes) for every accounting entry. These Financial Fingerprints are then published to a certain range of addresses on the public blockchain. The objective is to help accounting ledgers be structured in a Triple Entry Accounting format. The third entry can be defined as publishing a notarized index of each accounting entry to the public blockchain. The crux of Triple Entry Accounting is atomicity, meaning there can only be one book. Trying to present an alternative set of books would still be possible, but it would be automatically detected. The method used to achieve the objective can be presented as two value propositions. The first value proposition of Triple Entry Accounting is to define a provable official true set of books. This is important because it is a door into the market without being dependent on network effects. The second value proposition of Triple Entry Accounting is to break down the data silos by using the blockchain as a shared ledger and thus help auditors immensely in their tedious work to gather sufficient and appropriate audit evidence. Because of value proposition number one, Triple Entry Accounting presents standalone value even before the network effect begins. The result of this is an open standardized protocol for implementing Triple Entry Accounting as an extension to modern accounting systems.

Keywords: triple entry accounting; continuous audit; public blockchain; shared ledger; financial fingerprint

check for updates

Citation: Sunde, Torje Vingen, and Craig S. Wright. 2023. Implementing Triple Entry Accounting as an Audit Tool—An Extension to Modern Accounting Systems. *Journal of Risk and Financial Management* 16: 478. https://doi.org/10.3390/jrfm16110478

Academic Editors: Khaled Hussainey and Thanasis Stengos

Received: 20 August 2023
Revised: 23 October 2023
Accepted: 2 November 2023
Published: 10 November 2023

1. Introduction and Literature Review

This paper claims four contributions.

Firstly, it explains how Triple Entry Accounting (TEA) can provide stand-alone value without the network effect of needing others to use it at the same time. The first value proposition of Triple Entry Accounting is to define a provable official true set of books. This is important because it is a door into the market for TEA. This paper contributes by outlining a protocol for the first value proposition ("Financial Fingerprint Type 1"), showing how it could be practically implemented and made compatible with current modern accounting systems. The technical mechanisms of how to achieve this are cited throughout the paper. In short, it is a two-party approach between the user and a public attestation of a ledger root using a public ledger (blockchain) (Wright and Savanah 2017a; Wright n.d.a, 2016b). This method builds on the foundations created by Dr. Craig S. Wright.

Secondly, as the network effect of Triple Entry Accounting grows, it will be easier for companies to agree, compare, and reconcile their sub-ledgers against each other, as the blockchain will be utilized as a shared ledger. The second value proposition of Triple Entry Accounting is therefore to break down data silos and thus help auditors immensely in their tedious and onerous work to gather sufficient and appropriate audit evidence (Wright 2016b) (para. 0064). This paper contributes by outlining a protocol ("Financial Fingerprint Type 2") that also is compatible with modern accounting systems. In short, it is a three-party approach between two users and a public attestation. This idea was pioneered by Ian Grigg in his 2005 paper, where "... the natural roles of a transaction are of three parties, leading to three by three entries." (Grigg 2005, p. 6), section "Triple Entry Accounting". Todd Boyle also had ideas regarding shared repositories (Boyle 2001), published on a webpage in 2001[1].

Third, and importantly, a central goal for practical implementation is reliable and straight forward onboarding and implementation from the current double-entry systems. This is achieved by connecting Triple Entry Accounting solutions to the API endpoints of current double-entry accounting systems. It must be emphasized that, in order to make onboarding practical and viral, the proposed solution allows for different users (trading partners) to be onboarded at different points in time and still be able to reconcile their accounting records.

Fourth, an objective of this paper is to first introduce developers and accounting professionals to the concept of Triple Entry Accounting and then outline how to implement a practical solution that businesses can use for Triple Entry Accounting and auditing.

Accounting may be regarded as one of the oldest and most important forms of information technology. Reliable accounting data can be valuable for decision making. However, there are shortcomings of accounting technologies in that they do not always blend well with human nature, perhaps partially explaining why the profession has been haunted with human mistakes and dishonesty for hundreds of years—including the most modern accounting and audit systems. The current state of the technology relies on annual audits and a double-entry solution. Advancing from parchment to databases has been a leap forward, but shortcomings such as the possibility of keeping multiple sets of books have been inherited by digital databases. Worse, digital solutions may even have made it easier to keep multiple sets of dishonest books. Another challenge that traditional databases have not yet solved is easing the process of gathering and reconciling accounting data between trading parties. This paper explores how that can be improved by indexing all general ledger entries on a public ledger. By the process of indexing, we mean (1) hashing each general ledger entry, (2) signing the hashes, and (3) writing the signed hashes to the blockchain using pre-defined range of keypairs (blockchain addresses).

To mitigate these failings, we propose the extension of modern accounting systems to use a shared public ledger, in practice implemented on a public blockchain. A blockchain can be thought of as an effective shared ledger with timestamping and immutability. Without these characteristics of timestamping and immutability, provided only by a blockchain, it would not be possible to implement Triple Entry Accounting.

The initiating spark for a practical implementation of Triple Entry Accounting can be said to originate with the paper by Ian Grigg on triple-entry accounting (Grigg 2005) and the Bitcoin Whitepaper (Wright 2008). Todd Boyle also conceptualized a shared transaction repository (Boyle 2001) as early as around 2000; however, it never really seemed to catch on and be implemented. Juan Ignacio Ibañez et al. have also been researching Triple Entry Accounting (Ibañez et al. 2022). Notably, Ibañez et al. have also studied other existing TEA use cases and projects (Ibañez et al. 2021). M. Maiti et al. have also been discussing the combination of TEA and blockchain technology (Maiti et al. 2021). Another study by Cai summarizes how far TEA using a blockchain has come (Cai 2019).

The reason we propose using a public blockchain arises from the security and sustainability it provides. It is more secure with respect to data integrity to have public witnesses to the activity on the blockchain. Furthermore, a public blockchain has the game theoretic incentives aligned so that the risk of a single point of failure is reduced substantially, making it more sustainable in the long term. Additionally, the most efficient transaction processor is rewarded, incentivizing efficiency and scalability and thus lowering the cost for users.

Using a public blockchain raises a confidentiality issue, as few companies will adopt a public display of their own private books. We propose that writing indexes of general ledger entries to a public blockchain does not mean public disclosure of the content of each general ledger entry. Privacy and confidentiality will be preserved because the index does not reveal the content (because a hash is a one-way function). This way, the record is private, but the announcement of its existence is public, as the first root master public key is made publicly known (Wright 2016b).

In Section 3.3, this paper proposes an audit solution using Triple Entry Accounting as a foundation. Since most accounting systems today use double-entry, this paper includes a suggestion on how to practically link a traditional double-entry accounting software to a Triple Entry Accounting protocol. In Section 2, we discuss the concept of Triple Entry Accounting. In Section 3, we point the discussion towards an audit solution that can be practically implemented and compatible with modern accounting systems. Section 4 discusses the regulatory environment for using the suggested solution auditors. Section 5 concludes the paper.

This paper draws on the foundations created by Dr. Craig S Wright, Ian Grigg, Todd Boyle, and Professor Yuji Ijiri.

1.1. From Single-Entry Accounting to Double-Entry Accounting

Professor Yuji Ijiri explains that accounting evolved from single entry to double entry by classifying the same entry twice (Ijiri 1982). Moreover, the two classifications have a logical relationship, illustrated by the accounting equation Assets = Liabilities + Equity. The left side of the equation represents the assets of a company, and the right side represents the claims on those assets. Since the two sides of the equation represent two ways to classify the same thing, the two sides must be equal. The double classification gives two dimensions in accounting; the first-dimension states *what* happened, the second dimension explains *why* it happened (Ijiri 1998). To avoid confusion for non-accountants, the terms "debit and credit" are avoided in this paper.

Classifying the same event twice can be illustrated by the case of taking a loan of 10 dollars.

A single-entry system would look like the familiar cash account in your mobile banking, only keeping track of how much cash you have, showing only one dimension: *what* happened. When receiving the loan in single-entry accounting, there would only be one entry that increases your cash account by 10, describing only *what* happened.

In a double-entry system, the first entry likewise shows *what* happened: an asset account (cash) increased by 10. However, a second entry to a liability account is made to show *why* it happened: liabilities increased by 10. As a control, the two entries must balance by being of equal amount.

1.2. Terms

Note that the term "double entry" refers to the fact that the same entry is posted twice to a set of accounts, once by classifying what happened, and once by classifying why it happened. You may think of it as a double classification or using two attributes to describe a posting.

The terms "posting" or "entry" to an accounting "ledger", "account" or "book" both have the same meaning. It is the same as adding an "item" to a "table" or "database".

The terms "ledger", "book", "account" mean the same thing, which is a collection of postings or entries relating to the same topic or thing.

The term "*set* of books" refers to all the accounting records, traditionally recorded in books, where the set of books is the one and only truthful version of the accounting records.

1.3. The Leap from Single Entry to Double Entry

The leap from single-entry to double-entry accounting meant that important data such as assets, liabilities, owners' equity, income and expense could be measured. Importantly, double-entry accounting also introduced a technique for checks and balances making it easier to detect errors or dishonesty.

Not only did double-entry accounting become the most advanced data management tool for measuring key decision-making data, but it also came with a balancing mechanism to detect errors. The balancing of the two dimensions, what happened and why it happened, was especially useful as an internal control to deal with the agency problem between managers and owners as the size and scope of businesses grew. Better internal controls mean errors and dishonest entries would be easier to detect, thus incentivizing honesty.

However, the added control mechanisms of double entry still have two major shortcomings.

Firstly, there could be multiple sets of books:

"Every good merchant kept two sets of books, with a libro segreto, a secret book for their eyes only, and plausible public books for state audits. . . . . . Even accountants often, and indeed systematically, kept secret books to hide their business tax from collectors and competitors. Datini did it, and so did Cosimo." Page 34, from "The Reckoning: Financial Accountability and the Rise and Fall of Nations" (2014), by Professor Jacob Soll (Soll 2014).

"Books" in plural is acceptable, as each account could be referred to as a book, or the amount of the account entries may require a whole set of books. However, "*multiple sets* of books" are associated with fraud, as multiple different sets of books can be used to pick and choose which numbers to present.

Secondly, the issue of data inaccessibility: Another shortcoming is that double-entry accounting records are stored in data silos, meaning the data is inaccessible to other departments or entities. The data are isolated in a private database or in paper form. This isolation makes it difficult to prove there is only one true book (or database). Furthermore, the data isolation makes reconciliation of postings between trading parties extra cumbersome. Double entry was a good system for data management and internal control hundreds of years ago, but not optimized for data flow and external verification in modern accounting systems. What is needed is an upgrade to Triple Entry Accounting.

2. Triple Entry Accounting

The double-entry method can be extended to a form of Triple Entry Accounting by adding a signed third entry to a public ledger. The third entry can be defined as publishing a notarized index of the double-entry accounting entry to the public blockchain. We will return to what is meant by notarized in the next Section 2.1.

Importantly, we propose public indexing by using a protocol called Financial Fingerprint Type 1 to let an entity prove there is one official true set of books. This is of help to auditors and stakeholders, because keeping multiple sets of books is the oldest form of financial fraud, still being used today. Unlike normal isolated accounting ledgers in use today, the public nature of a Triple Entry Accounting ledger can prove there is only one set of books. The third entry can provably be derived from a publicly pre-announced and attested "ledger root". The ledger root can be used to prove that an entry belongs to the one and only true version of the accounting records. Trying to present multiple sets of books is still theoretically possible, but it will be automatically detected. The rooting process is explained in Section 3.2.

Secondly, two parties can publish an entry reflecting the same event. The format must be reconcilable; thus, we are proposing a protocol called Financial Fingerprint Type 2. The parties can share selected relevant parts of their subledger with trading partners. If the entries or indexes (Fingerprint type 2) do not match, there is probably not an agreement. This helps auditors' jobs in gathering sufficient and appropriate audit evidence.

In addition to proving only one true set of books, Triple Entry Accounting on the public blockchain unlocks other novel functionalities such as inter-ledger reconciliations (audit), data flow (accounting), shared secret distribution, data integrity and availability (cyber security), data veracity (machine learning), supply chain analytics, customs, transparency, anti-money laundering, and more.

2.1. Identity

A solution for identity is needed to perform signing and attestation; however, this is out of scope for this paper. Identity is nonetheless mentioned because identity in Triple Entry Accounting is essential. It is a requirement that any use of signing or attestation needs sufficient and/or systematic identification of the parties, and of the meaning of any signature that relying parties can depend upon. Both the attestation of the ledger root and the third entries must be linked to identity through signing.

The timestamping properties of a public blockchain makes it a good shared ledger for the purpose of notarization. The public attestation or notarization of the ledger root may be performed at the Company House Register or another suitable authority.

Ian Grigg explains how the receipt is the transaction in his paper on Triple Entry Accounting (Grigg 2005): by creating a dominating record of the event. Identity matters because it is related to the signature on the receipt and possibilities for later verification by an auditor. Dr. Craig S. Wright explains that one true set of books can be proven by linking identity and publicly announcing and attesting the root of the ledger and linking it to the public blockchain (Wright 2016b), and using a ledger of ledgers or table (see Section 4, "Rooting the ledger") (Wright and Savanah 2017b) (para. 0158).

2.2. Defining the Third Dimension

Professor Yuji Ijiri reflects on what the third dimension could be in his monograph (Ijiri 1982). Although he did not go into the direction of using a shared public ledger, he did discuss the requirements for the third dimension. According to him, the three dimensions should have a relationship with each other, preferably a logical relationship, such as that which the two dimensions in double-entry accounting have through the accounting equation, Assets = Liabilities + Equity.

As discussed above, identity is needed to perform Triple Entry Accounting, so identity is a candidate to be defined as the third dimension. Alternatively, the shared public ledger itself could be the third dimension. However, it would be more descriptive to meld the two concepts into a dimension that can imply both identity and a shared public ledger. Using the shared public ledger in a notarization process that requires identity could be a better fit to describe the third dimension. Thus, the third dimension could be defined as "*notarization*" (see Section 3.2). Other alternatives could be authentication, attestation, event completion, fixation, time stamping, agreement, commitment, truth. We use the term notarization in this paper, but this can be discussed further in future studies. Figure 1 illustrates how the third entry can be an extension of current accounting systems, extending from a private double-entry accounting ledger, onto the public blockchain.

A Triple Entry Accounting format extends the double-entry accounting systems out of their isolation; hence, Triple Entry Accounting can repair the shortcomings of double-entry accounting discussed in Section 1.3 by introducing two new features:

(1) Proving there is only one set of books;
(2) Increasing verifiability, as the entries are indexed on a shared public ledger.

The scope of this paper is to point out how a Triple Entry Accounting protocol can be implemented from the current accounting platforms (Section 3), and to explore the use of verifiable accounting records or inter-ledger reconciliations as an audit tool built on top of Triple Entry Accounting (Section 3.3).

Figure 1 contrasts with the methods described by Grigg and Boyle, that Triple Entry Accounting was a shared entry between 3 parties. Our proposal is that Triple Entry Accounting can start out being performed with only two parties; one user and a notary, because proving one set of books provides value.

However, as more actors wish to do this, shared entries between trading parties (e.g., subledgers) suddenly become reconcilable, and we have grown into the concept of Triple Entry Accounting with shared entries between 3 parties; 2 trading partners and a notary.

Because this hybrid method provides value before the network effect emerges, it is a door to the markets and adoption of Triple Entry Accounting. This hybrid dynamic is an important contribution of how to practically implement Triple Entry Accounting from a business perspective rather than a technical perspective. It frees us from initially relying on network effects to provide value.

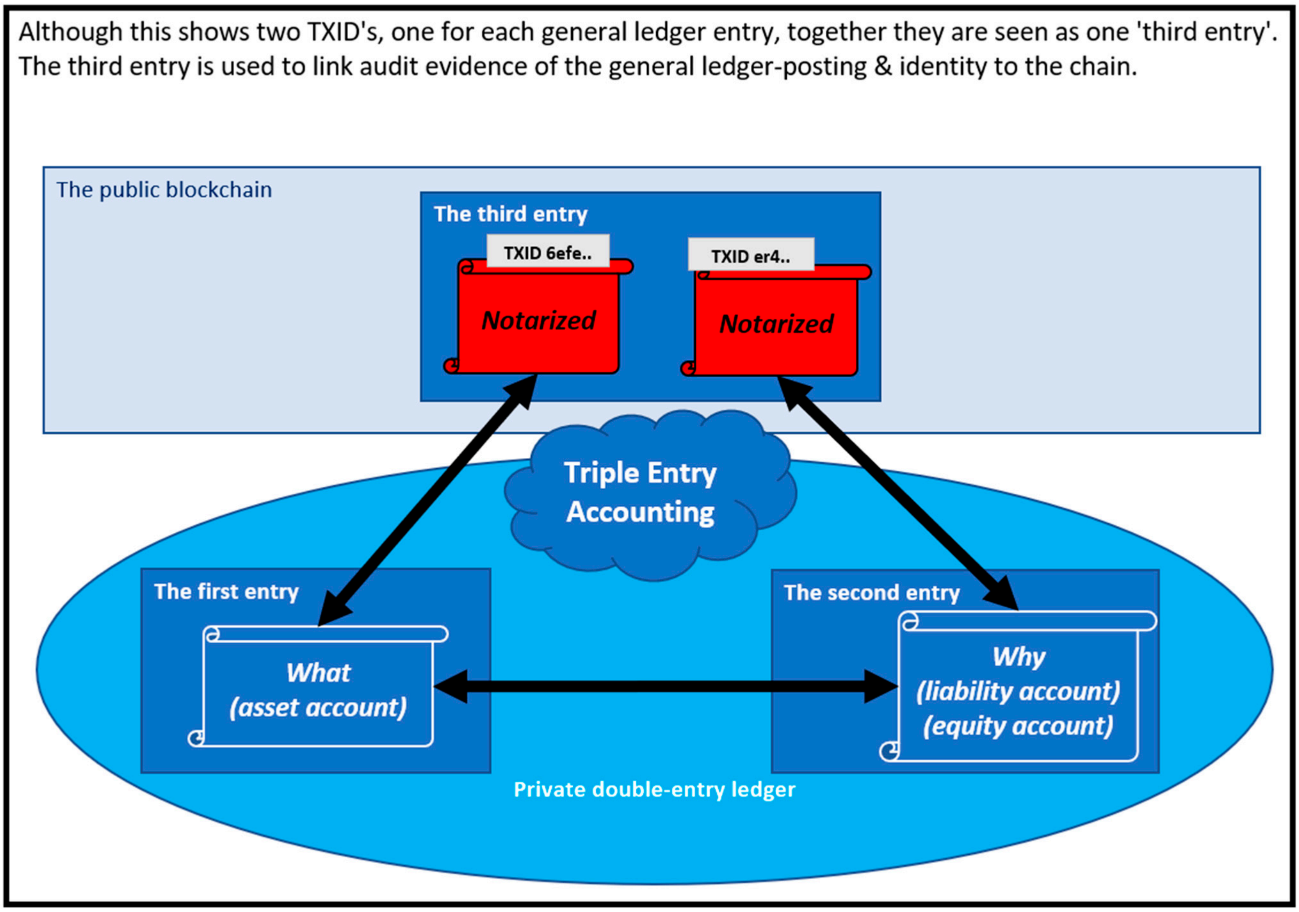

Although this shows two TXID's, one for each general ledger entry, together they are seen as one 'third entry'.
The third entry is used to link audit evidence of the general ledger-posting & identity to the chain.
The public blockchain
The third entry
TXID 6efe..
Notarized
TXID er4..
Notarized
Triple Entry Accounting
The first entry
What (asset account)
The second entry
Why (liability account) (equity account)
Private double-entry ledger

Figure 1. The third dimension as notarization.

3. Data and Methodology: Proposal for a Triple Entry Accounting (TEA) Protocol

A practical solution for Triple Entry Accounting and auditing faces many needs.

There is a need to ensure there is only one set of books, to prove the uniqueness of the accounting records, because keeping several sets of books is the oldest and yet unsolved problem in accounting. Despite the current state-of-the-art double-entry accounting practices and software, this has not been solved in double-entry accounting.

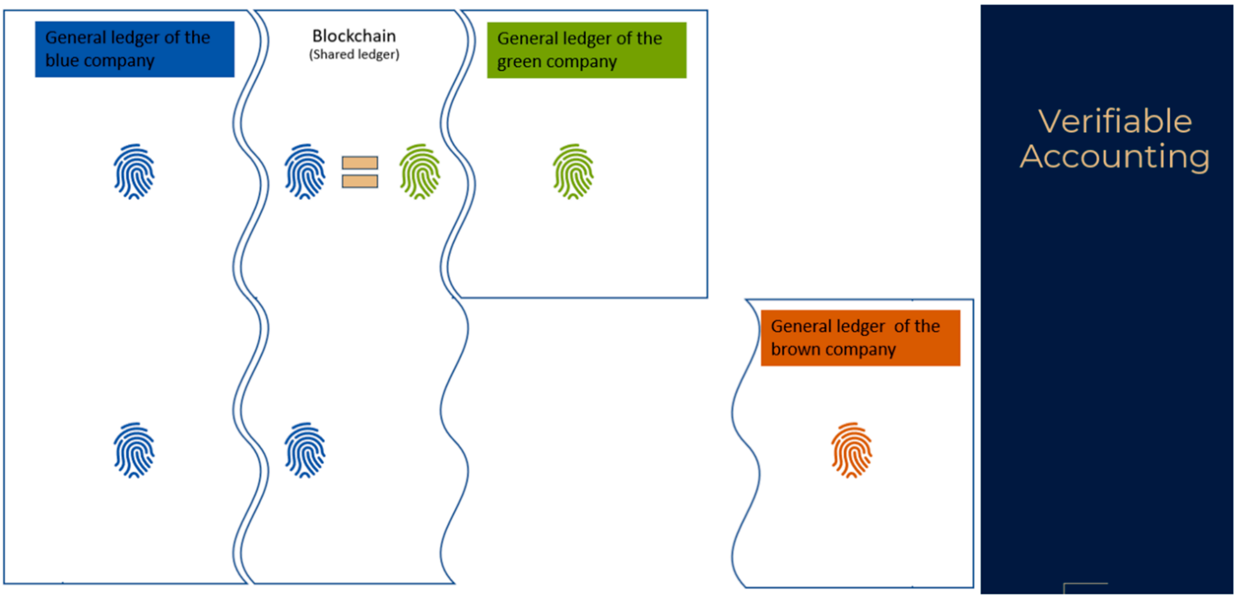
There is a need for better verifiability of accounting records. More specifically, there is a need for compatibility with a single open standard, being made of an open protocol for sharing records in an open format, and not locking users into walled gardens or single software solutions. This is important for several reasons, one being global compatibility for reconciliation. Secondly, it supports a vision of a world where users and organizations can control and own their own data. Third, it introduces competition for better services, because it is easier to move between solutions using the same protocol. Just like the email protocol, we have different email providers competing, using the same fixed protocol. We reap the benefits of that today, decades later, because emails are still portable, controlled and owned by the user, meaning that users have a choice of which service to use. This architecture preserves privacy, in contrast to other current big tech solutions whose business models include farming the user's data without valid consent.

Triple Entry Accounting needs to facilitate continuous audits, evidence gathering, and reconciliation. From The Financial Supervisory Authority of Norway annual report 2019 page 71: ". . . The most serious breaches were that the auditor had not obtained sufficient and appropriate audit evidence as a basis for the audit opinion." (Finanstilsynet 2019; Sunde et al. 2022b). The proposed solution helps auditors to gather sufficient evidence on a timely and efficient basis, thereby speeding up the annual audit process and improving the audit quality.

To make onboarding practical and viral, the proposed solution must allow for different users (trading partners) to be onboarded at different points in time, and still be able to reconcile their accounting records.

3.1. Financial Fingerprints: Recording an Index of All General Ledger Entries on a Public Ledger

Our design is such that the third entry is created by (a) taking a unique fingerprint of a double-entry accounting posting, and (b) writing it to a shared ledger (the public blockchain), as shown in Scheme 1, then (c) by some means notifying interested parties of that fingerprint. Notification can be performed from user to user, or via an oracle.


General ledger of the blue company
Blockchain
(Shared ledger)
General ledger of the green company
General ledger of the brown company
Verifiable Accounting

Scheme 1. Showing how accounting ledgers can become more easily verifiable between trading partners by using the public blockchain as a shared ledger.

We give a term to this third entry, naming it a "Financial Fingerprint". In its simplest form, the Financial Fingerprint is a digitally signed hash of a general ledger posting (XML or JSON format), published to the public blockchain. Identity is linked by including a public key certificate from a certificate body along with the signature, thus making the process similar to that of a notarization (see Sections 2.2 and 3.2). The fingerprints can later be reproduced from the local private general ledger and matched against the fingerprints written on the shared public ledger as audit evidence.

We define two types of Financial Fingerprints: Fingerprint Type 1 is used to prove one set of books. Type 2 is used for reconciliations between trading partners. Both are illustrated in Figure 2.

The Type 1 Financial Fingerprint is a digitally signed hash of a general ledger posting as described above and is produced for all general ledger entries and published in a deterministic way to a range of addresses (Wright and Savanah 2017a; Wright n.d.a, 2016b). The Fingerprint must be digitally signed because it must be demonstrated it belongs to a derived key from the notarized root keys, see Appendix A, following the committed procedure in order to prove it belongs to the official true set of books. Furthermore, introducing identity enhances accountability and auditability.

The benefit from Financial Fingerprint Type 1 is proving there is only one set of books.

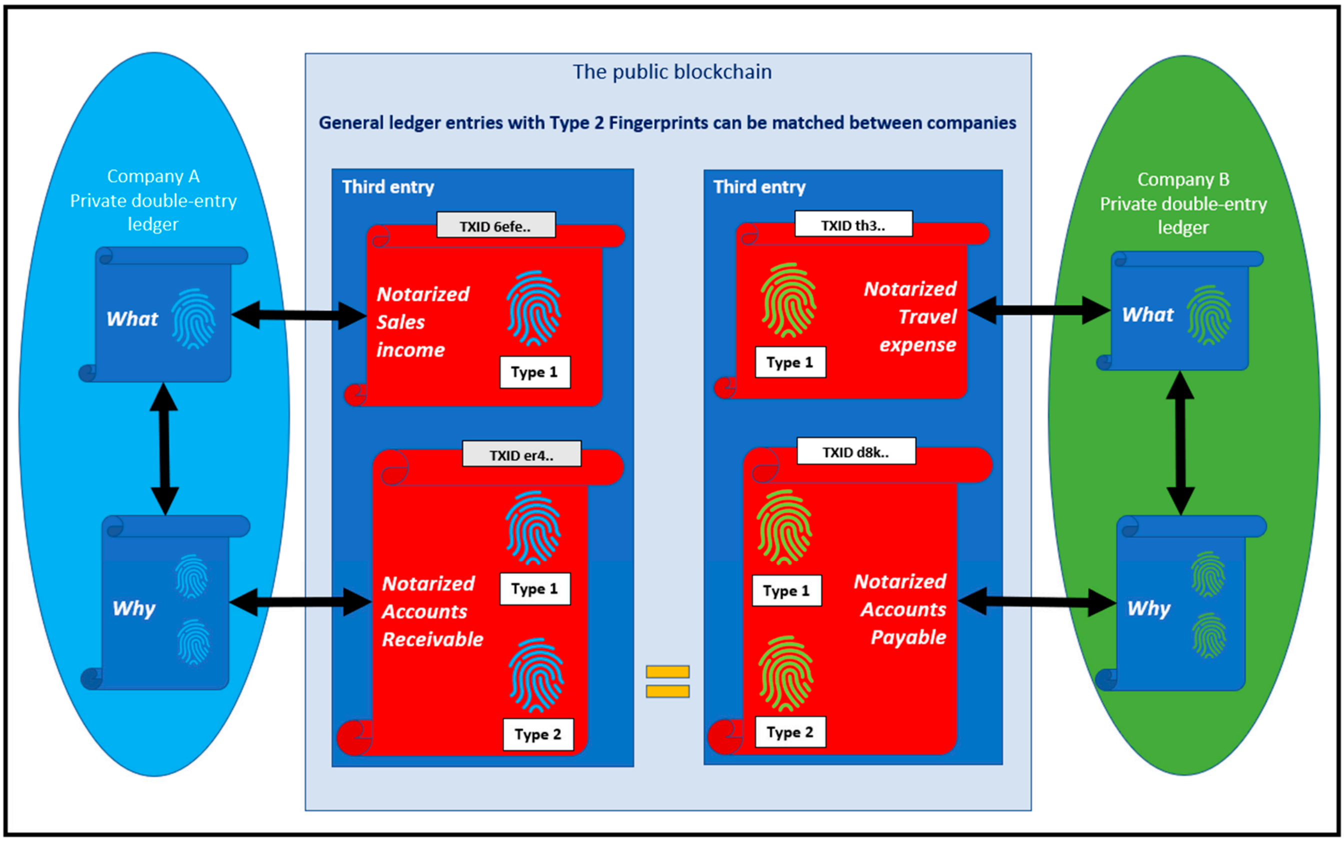


Figure 2. Showing how two trading parties, A and B, can reconcile their accounting ledgers using the public blockchain as a shared ledger by using Financial Fingerprint Type 2. Additionally, shows that the Type 1 Fingerprint is included in order to prove one book.

The Type 2 Financial Fingerprint needs to include a shared message with a trading party (Grigg 2005; Boyle 2001); this message can be determined based on an invoice number (Wright 2016a), message, or invoice (Wright and Savanah 2017b; Wright n.d.b).

The benefit from Financial Fingerprint Type 2 is that it increases the verifiability of accounting entries because the entries are indexed on a shared public ledger in a verifiable format.

The protocol design is meant to function as a hybrid implementation, because it ensures easier onboarding and provide value without the immediate network effect. In a hybrid implementation, when only one of the trading parties has implemented TEA, a shared “Message” is used instead of the shared secret. The message can be as simple as the invoice number. Shared secrets can be derived from the Message later, after the other trading party has onboarded to the TEA system. Shared secrets are important to mention, because it leaves the protocol compatible for future communications capabilities for the full implementation (Wright and Savanah 2017b) (paras. 0158 and 0172).

The Type 2 Fingerprint can be a hash of the combination of invoice amount, invoice (document) number, and the organization number of the invoice (document) issuer. Invoice number and organization number should be sufficient for establishing uniqueness of the index (Fingerprint Type 2). However, by including the invoice (document) amount in the hash pre-image, an auditor can know the counterparty certainly has booked the same amount by only comparing the signed hashes. If only invoice number and organization number made the preimage of the hash, the amount would not be part of the evidence hashes being reconciled.

Importantly, the proposed Triple Entry Accounting audit solution enables the two trading parties to generate the same Type 2 Fingerprint *independently of each other in time and place*, because the preimage of a Financial Fingerprint Type 2 consists of the concatenation of "invoice number | | organization number | | invoice amount". These data points are naturally already exchanged between trading parties and recorded in modern accounting systems today. This makes the onboarding process more viable, contributing to sowing the seeds of Triple Entry Accounting value proposition even before the network effect begins.

The Type 2 fingerprints help automate later evidence gathering and reconciliation in an audit process. They are also a step towards continuous audits when more trading parties use Triple Entry Accounting. A Protocol Type 2 fingerprint is generated in addition to a Type 1 fingerprint, but only for general ledger entries that have an external trading party. These kinds of ledger entries belong to account types such as accounts payable, accounts receivable, bank deposits, loans, equity, and other entries with a counterparty.

The difference between Type 1 and Type 2 stems from two different functional needs.

The first need is to prove one set of books. Here, a *two-party approach* between the user and a public attestation using a public ledger (blockchain) is used. For this, we use Financial Fingerprint Type 1. The functional value of the Type 1 Fingerprint is not dependent on other trading parties also using TEA, because it is not subject to reconciliation with external trading partners.

The second need is to make accounting entries reconcilable between trading parties. Here a *three-party approach* between two users and a public attestation on a public ledger (blockchain) is used. For this, we use Financial Fingerprint Type 2.

Transactions containing a Type 2 Financial Fingerprint can be exchanged between the relevant trading parties for reconciliation. The privately owned repository of these exchanged transactions will form a tamper-proof, verifiable shared ledger between the two parties.

Type 2 Financial Fingerprints can be exchanged in several ways, depending on whether a hybrid implementation is used where only one of the trading parties uses Triple Entry Accounting, or a full implementation is used, where both companies use Triple Entry Accounting. Referring to Figure 2, we see that Company A and B can create their Type 2 Fingerprint independently of each other in time and space. This means that it is possible for one of them to begin documenting their accounting entries in a TEA protocol format before the other party. This is an instance of a hybrid implementation. However, the functional value of having a Type 2 Fingerprint is derived only when both parties are onboarded and can reconcile their Type 2 Fingerprints, and this is an instance of a full implementation. In Figure 2, a full implementation is illustrated by the equality symbol, =, between the Type 2 Fingerprints.

In a hybrid implementation, the exchange of the signed Type 2 Fingerprints can happen through service providers or oracles, for example, if Abendum AS becomes a software provider for a Triple Entry Accounting platform.

In a full implementation, Type 2 Fingerprints can be exchanged directly in a peer-to-peer manner with a communication method of choice. A suggested method is illustrated in Appendix A. Given two trading parties use TEA, both parties have a preannounced pool of keys for invoice generation and for invoice repository. The key pool (address pool) is deterministic (Wright and Savanah 2017a; Wright n.d.a), meaning that it can be recreated as subkeys from the root key by following the pre-announced and attested procedures in the ledger of ledgers. Both parties can now know which addresses to monitor for incoming invoices; this could, for example, be a set of subkeys under the accounts receivable key or accounts payable key. Monitoring a set of addresses based on a deterministic path derived from shared secrets and a ledger of ledgers should be a viable way for data interchange for the full implementation (Wright and Savanah 2017b) (paras. 0158 and 0172).

To reduce one step, the sending party of an invoice can attach a signed Type 2 Fingerprint together with the invoice. The receiving party can only generate their Type 2 Fingerprint after having received the invoice.

For the exchange to be complete, the sending party must either (1) know about a repository to monitor like mentioned above or (2) receive it in a peer-to-peer manner using SPV as explained below or (3) make a request for the signed Fingerprint Type 2 from the receiving party.

By using SPV and Merkle paths, transactions containing the Financial Fingerprint(s) can easily be verified against the block header without having to search or look up the blockchain.

Only the hash needs to be published to the blockchain, meaning the transaction fee can be minimized and maintaining full privacy, *but still leaving a public record of the event or Fingerprint*.

By using OP_Pushdata, exchanging the transaction data in a peer-to-peer (business-to-business) manner and using Simplified Payment Verification (SPV) (Wright 2008) and Merkle paths, users neither need to depend on a single service provider or oracle to exchange fingerprints, nor need to search the blockchain to retrieve information or find their matching counterparty's fingerprint. The forementioned terms describe advanced blockchain-related techniques, out of scope to explain in this paper.

Along with the Financial Fingerprint, a signature and PKI-Certificates will be included with the blockchain transaction data. This way, identity can be verified without relying on a single oracle or intermediary.

In simple terms, the trading partners are exchanging notarized indexes of their supplier sub-ledger and customer sub-ledger on a continuous basis. The indexes containing Type 2 Financial Fingerprints can be automatically reconciled against a trading partner's Type 2 Fingerprint. The Type 1 Fingerprint can be trusted to belong to the official true set of books because it contains a deterministic derivation path from their trading partner's publicly announced and attested ledger root. The derivation path used for the posting must be verifiable to belong in their ledger of ledgers, so that any duplicates or alternative entries will be automatically detected.

3.2. Rooting the Ledger—Commitment to One Set of Books

In order to prove there is only one true set of books, we need to give accounting records the attribute of uniqueness. As discussed above, rooting the ledger is needed to create evidence that there is only one true set of accounting records, because any deviation from the pre-announced root and procedure would suggest that there are multiple sets of books. We propose to "root the ledger" in the following manner consisting of components (a–f).

(a) Posting the root master key somewhere;
(b) This place is "committal";
(c) There is an attestation stating that the fingerprints will be published according to a publicly preannounced schema;
(d) A ledger of ledgers will be kept;
(e) The previous steps must be performed before the posting of entries;
(f) The same steps must be performed upon onboarding and for each new accounting year.

Importantly, study Appendix A at the last page of this paper when reading this section.

The procedure of rooting the accounting ledger entails a public attestation and (a) posting of a master key as a "ledger root". As a (b) commitment, the public attestation of the ledger root may be performed at a government company's registrar such as the Company House Register in the UK or another suitable authority. The process may be similar to a notarization of the root key together with (c) pre-defined procedures of what is the true set of books. This way, the commitment to follow the procedure is notarized, which for each accounting entry indirectly notarizes the attribute of belonging or not belonging to the true set of books. The attestation can state that the Financial Fingerprints will be published to the public blockchain by the master key or derivatives of the key within a certain range of addresses, following a pre-determined algorithm that also must be attested at the same time of the root key (Wright and Savanah 2017a; Wright n.d.a, 2016b). The key pool (address pool) is deterministic, meaning that it can be recreated as subkeys from the root key by following the pre-announced and attested procedures in the (d) ledger of ledgers.

This is useful because (1) it helps prove only one set of books and can automatically detect attempts to keep multiple sets of books, and because (2) an auditor can recreate the public keys (because key generation follows a deterministic procedure from the root) used in the accounting and thus recreate addresses used in the accounting to test the completeness of both internal records (made by the company) and external records (made by the company's trading partners).

In order to prove only one set of books, keeping a "Ledger of Ledgers" or table is needed. The ledger of ledgers points to all the ledgers and accounts used in the accounting process, showing all the parts of the known ledger. Each ledger or account can be defined as a deterministically generated pool of addresses, where the next address is derived by using an algorithm that includes the previous address, forming a deterministic path of key pairs (addresses).

The rooting process must happen (e) *before* the Financial Fingerprints are published to the public blockchain. Rooting the ledger should be performed (f) before a new accounting year begins, or upon onboarding to the Triple Entry Accounting system. This way, the attribute of uniqueness can be assigned to accounting records. Uniqueness is usually associated with tangible things from the physical world. This method allows intangible digital records to be uniquely identified and leaves an audit trail that is derived from the root in a private, deterministic way.

3.3. Triple Entry Accounting as an Audit Tool

Triple Entry Accounting (TEA) can have many use cases; this paper outlines the use case of an audit tool. The first use case is to automate the gathering and reconciliation of large amounts of external confirmations. In steps 1–3, a double-entry system is onboarded to a Triple Entry Accounting format. In steps 4–7, the auditor can use Triple Entry Accounting as an audit tool.

- Step 1—Onboarding. Publicly attest the keys to be used to publish the Financial Fingerprints. Include a ledger of ledgers and key derivation procedures.
- Step 2—Creating Financial Fingerprints.
- Step 3—Publish the Financial Fingerprints to the blockchain.
- Step 4—Reconcile Fingerprints Type 1 with the General Ledger and analytics.
- Step 5—View a list of trade partners' Type 2 Fingerprints that already match.
- Step 6—Send a request for additional external confirmation of Type 2 Fingerprints if needed.
- Step 7—Reconcile Fingerprints Type 2 with trade partners.

In step 4, the auditing software can display which identities are related to the transactions, for example, by formatting the transaction data in a MetaNet format (nChain Limited 2019). The use of identity on a transaction level facilitates controls against management override of the accounts ref ISA 240. For example, if a COO or CEO makes an accounting entry, that might trigger a notice.

In step 5, an auditor can assess how much audit evidence may be readily available even before an audit begins during the planning stage. This can be used to assess how much resources are needed for the audit engagement.

In Step 6, the gathering of audit evidence may be more effective. A request for external confirmation can be sent, either the traditional way by email, or by the new Triple Entry way. The Triple Entry way requires the respondent to already have TEA or be asked to integrate the TEA API for free.

In step 7, the auditor can see all the entries that are reconciled by Triple Entry Accounting on an account and supplier level. This can be exported to a report that can be downloaded as a pdf and stored as audit evidence.

Auditors with minimal training should be able to walk through the data flow for the purpose of leaning on the process as audit evidence. This will require extra attention to simplicity, documentation, and user interface. However, the audit software will automate the verification of massive volumes of reconciliations.

3.4. Key Management

A solution for key management is needed for implementation of Triple Entry Accounting, however, a detailed description for this is out of scope for this paper. It is still worth mentioning for the sake of its importance and future development. Individual digital certificates can be created for each user and all tangible and intangible items, including each individual general ledger entry. It can be used for linking and managing identities, as identification is needed for accountability.

An example of other types of records can be non-fungible tokens (NFTs) associated with an item in an inventory or along a supply chain. Having individual NFTs for each inventory item recording individual history such as age, temperature exposure, expiration date, location, etc., gives new opportunities for both management and audit of inventory. Furthermore, ownership can be documented and transferred without moving the goods itself, by linking the items to contracts.

Key management on-chain is possible by using tokens and keeping a record on-chain of what has happened to the keys that have signed the digital certificates. For example, if a key or digital certificate has been compromised, it can be revoked by spending the token, and then reissued. The blockchain could help ensure that a timestamped history of key revocations, issuances, and other key management events can be kept as proof (Wright et al. 2020).

3.5. Using Triple Entry Accounting to Search for Unrecorded Liabilities

In an audit, the completeness assertion refers to the concept of whether all relevant entries have been included in the accounting. An example may be an entry about a liability that is missing, either by mistake or on purpose. There is a need to make the search for unrecorded liabilities easier.

There exists a method to create an on-chain repository that can be made by a pool or set of public keys that can be monitored on-chain, per Wright (Wright 2016a, 2016b). The keys can be mapped against the Chart of Accounts and allocation rules. By monitoring the set of keys, a transaction can trigger an automated entry from the blockchain to the general ledger. This is helpful in day-to-day accounting and for an auditor to assess the completeness assertion, for example, in the search for unrecorded liabilities.

However, the aforementioned method (Wright 2016a, 2016b) describes posting accounting entries in the direction sourcing from the blockchain to the general ledger, making an interesting use case for the completeness assertion.

It must be noted that the solution described in this paper is describing sourcing data in the opposite direction, from the general ledger to the blockchain.

The point of this section is to point out that by using a pool, set or range of addresses to monitor incoming invoices, we can help auditors in auditing the completeness assertion of the accounts, such as searching for unrecorded liabilities, for example, the executive who hid incoming invoices in a drawer.

4. Standards and Regulation

ISA 505 standardizes the external confirmation procedures of an external audit and requires that the auditor needs to be in control at key stages of the process. In building a Triple Entry Accounting system, it is important to both automate the procedures of the key stages and to keep the auditor in control of those stages.

In a financial audit, auditors need to gather sufficient and appropriate audit evidence to form an opinion about the financial statements. Usually, the best type of evidence is external, meaning that the evidence is provided by a third party, such as a trade partner or a bank. However, collecting external evidence on a large scale can be a time-consuming process. The understanding and definition of "Audit evidence" are regulated by the International Standard on Auditing 500[2] (ISA 500), stating that the reliability of audit evidence is influenced by its source and nature (ISA 500, paragraph A5).

In 2021, Abendum AS participated in the Financial Supervisory Authority of Norway's sandbox for fintech (Sunde et al. 2022a); there is also an English translation of this report[3] (Sunde et al. 2022b). The outcome provided regulatory clarity that a Triple Entry Accounting system is a viable method for the use of blockchain to obtain, store and provide audit evidence in the execution of an audit.

Just as the internet by itself does not solve accounting problems, blockchain by itself does not solve all accounting problems. When we use the internet today, the solutions on top need procedures for identity management, attestation, and law. Likewise, the procedure of publicly announcing the root-key and algorithms to prove there is only one ledger requires both identity and attestation; neither is something a blockchain can perform by itself. This requires people and law, in combination with blockchain technology.

5. Limitations, Discussion, and Future Issues

This research, however, is subject to several limitations to the depth and the width of the topics touched upon, such as accounting, auditing, cryptography, other TEA solutions, and blockchain technology. Furthermore, the suggested TEA protocol in this paper has not been implemented and tested in a commercial environment yet, which would give valuable insight into the workings of the suggested protocol and more access to data and input from professionals. Time and resource limitations have also made it difficult to draw on a wider diverse range of scientific resources.

There are several other projects and use cases for TEA (Ibañez et al. 2021; Cai 2019), and some have come further in development than others. As mentioned above, the method described in this paper have achieved a degree of regulatory clarity. The outcome of the fintech sandbox indicates that this kind of Triple Entry Accounting system is a viable method for using a blockchain to obtain, store, and provide audit evidence in the execution of an audit (Sunde et al. 2022a, 2022b). It would still be interesting to follow the regulatory developments regarding and auditors' willingness to use new technology for TEA.

To handle the throughput of all these accounting entries globally, we need to use a public blockchain that can scale. One such example is the original bitcoin blockchain (Wright 2008), today known as the BSV Blockchain, which has demonstrated 50,000 transactions per second (Coingeek.com 2021). We believe this sort of throughput is necessary for widespread adoption. It will be interesting to keep paying attention to how blockchain technology can scale in the future.

Looking further into the handling of identity, confidentiality, data silos and key management could be a topic for future research.

6. Conclusions and Summary

Triple Entry Accounting gives standalone value even before the network effect begins. Using a Type 1 Fingerprint, we can prove there is only one set of books, perform invoice organization number verification, analyze management override of accounts, and make simplified external requests. All the forementioned functionalities work without the network effects of trading parties also using TEA. As other trading partners of the audit client start using Triple Entry Accounting, audit quality and massive continuous reconciliation of accounts becomes possible by reconciling Type 2 Financial Fingerprints.

The proposed solution enables two trading parties to generate the same Type 2 Fingerprint *independently of each other in time and place*, because the required datapoints are naturally already exchanged between trading parties and recorded in modern accounting systems today. This makes the onboarding process more viable, contributing to sowing the seeds of Triple Entry Accounting reconciliation value proposition even before the network effect begins.

Regulatory clarity around the use of Triple Entry Accounting exists. Auditors can freely ask any entity to use Triple Entry Accounting and auditing tool without concern for their independence.

Importantly, a key goal for practical implementation is easy onboarding and implementation from the current double-entry systems. This is achieved by connecting Triple Entry Accounting solution to the API endpoints of current double-entry accounting systems.

It must be emphasized that in order to make onboarding practical and viral, the proposed solution allows for different users (trading partners) to be onboarded at different points in time and still be able to reconcile their accounting records.

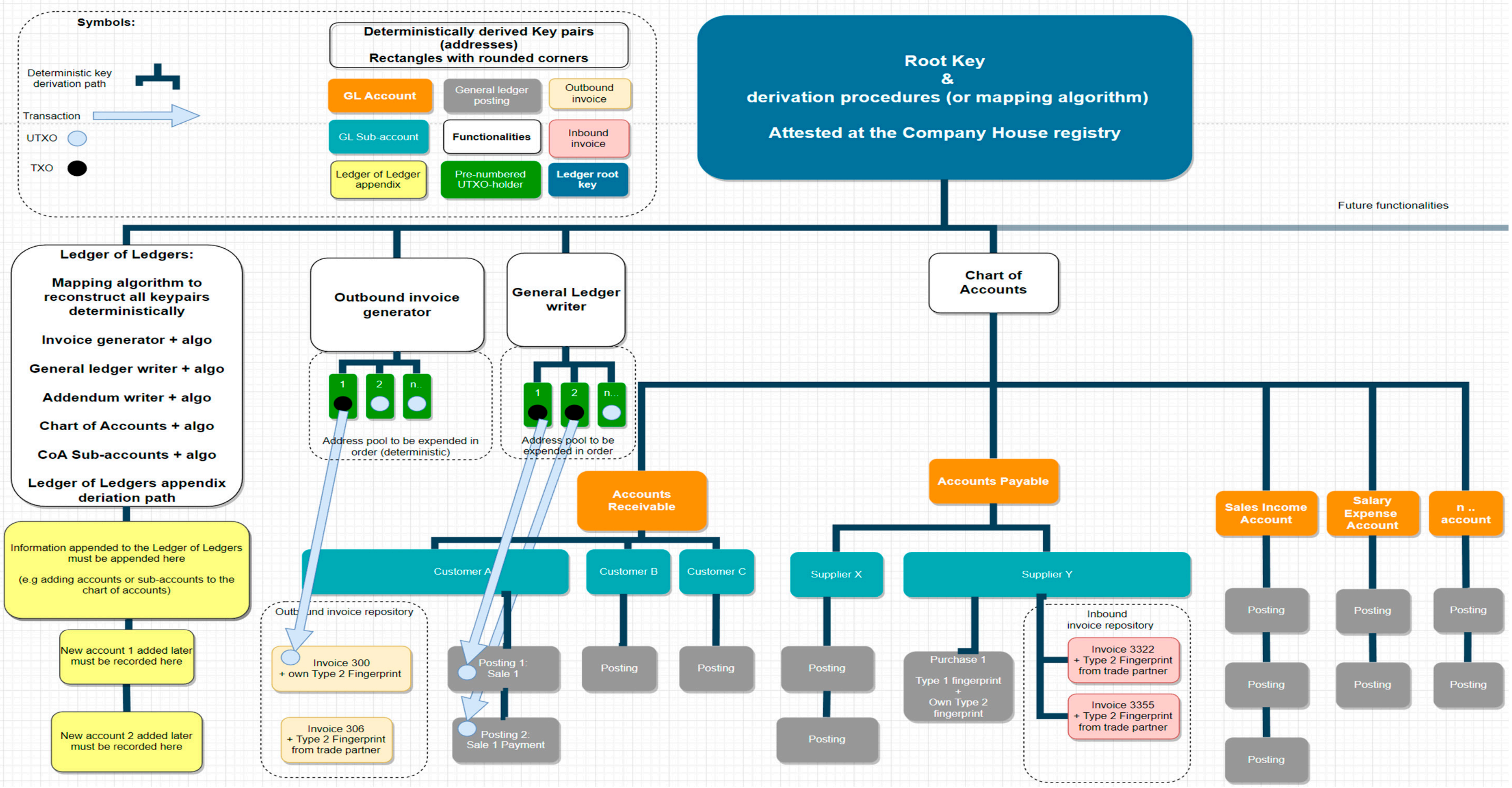
Author Contributions: Conceptualization, T.V.S. (the hybrid architecture of using two types of Financial Fingerprints) and C.S.W. (proving one true ledger, the use of cryptographic derivation methods and shared secrets); methodology, T.V.S.; software, T.V.S.; investigation, T.V.S.; resources, T.V.S. and C.S.W.; writing—original draft preparation, T.V.S.; writing—review and editing, T.V.S. and C.S.W.; visualization, T.V.S.; project administration, T.V.S.; funding acquisition, T.V.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by The Research Council of Norway grant project number 318045, Innovation Norway grant number 2021/584209, and the APC was funded by teaconf.org.

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

Conflicts of Interest: Author Torje Vingen Sunde was employed by the company Abendum. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A


Symbols:
Deterministic key derivation path
Transaction
UTXO
TXO
Deterministically derived Key pairs (addresses) Rectangles with rounded corners
GL Account
General ledger posting
Outbound invoice
GL Sub-account
Functionalities
Inbound invoice
Ledger of Ledger appendix
Pre-numbered UTXO-holder
Ledger root key
Root Key
&
derivation procedures (or mapping algorithm)
Attested at the Company House registry
Future functionalities
Ledger of Ledgers:
Mapping algorithm to reconstruct all keypairs deterministically
Invoice generator + algo
General ledger writer + algo
Addendum writer + algo
Chart of Accounts + algo
CoA Sub-accounts + algo
Ledger of Ledgers appendix deriation path
Information appended to the Ledger of Ledgers must be appended here
(e.g adding accounts or sub-accounts to the chart of accounts)
New account 1 added later must be recorded here
New account 2 added later must be recorded here
Outbound invoice generator
1
2
n..
Address pool to be expended in order (deterministic)
General Ledger writer
1
2
n...
Address pool to be expended in order
Chart of Accounts
Accounts Receivable
Accounts Payable
Sales Income Account
Salary Expense Account
n .. account
Customer A
Customer B
Customer C
Supplier X
Supplier Y
Outbound invoice repository
Invoice 300 + own Type 2 Fingerprint
Invoice 306 + Type 2 Fingerprint from trade partner
Posting 1: Sale 1
Posting 2: Sale 1 Payment
Posting
Posting
Posting
Posting
Purchase 1
Type 1 fingerprint + Own Type 2 fingerprint
Inbound invoice repository
Invoice 3322 + Type 2 Fingerprint from trade partner
Invoice 3355 + Type 2 Fingerprint from trade partner
Posting
Posting
Posting
Posting
Posting
Posting
Posting
Posting

Notes

[1] https://linas.org/mirrors/www.gldialtone.com/2001.07.14/ (accessed on 11 February 2021).

[2] https://www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf (accessed on 15 April 2021).

[3] https://abendum.com/wp-content/uploads/2023/07/Final-Report_26_01_2022-English.pdf (accessed on 17 July 2023).

References

Boyle, Todd. 2001. The Shared Transaction Repository (STR) ver. 0.60 Spec. Available online: https://linas.org/mirrors/www.gldialtone.com/2001.07.14/str.htm (accessed on 11 February 2021).

Cai, Cynthia Weiyi. 2019. Triple-entry Accounting with Blockchain: How Far Have We Come? *Accounting & Finance* 61: 71–93.

Coingeek.com. 2021. This Is What Teranode Is about (+50k TPS). Available online: https://coingeek.com/this-is-what-teranode-is-about-50k-tps/ (accessed on 8 August 2023).

Finanstilsynet (The Financial Supervisory Authority of Norway). 2019. Årsmelding 2019. Available online: https://www.finanstilsynet.no/contentassets/324174b9375c464f89a6ac15d94b50b7/finanstilsynets-arsmelding-2019.pdf (accessed on 2 October 2023).

Grigg, Ian. 2005. Available online: https://iang.org/papers/triple_entry.html (accessed on 27 February 2019).

Ibañez, Juan Ignacio, Chris N. Bayer, Paolo Tasca, and Jiahua Xu. 2021. The Efficiency of Single Truth: Triple-Entry Accounting. Available online: https://ssrn.com/abstract=3770034 (accessed on 12 April 2021).

Ibañez, Juan Ignacio, Chris N. Bayer, Paolo Tasca, and Jiahua Xu. 2022. REA, Triple-Entry Accounting and Blockchain: Converging Paths to Shared Ledger Systems. *Journal of Risk and Financial Management* 16: 382. [CrossRef]

Ijiri, Yuji. 1982. *Triple Entry Accounting and Income Momentum*. Sarasota: American Accounting Association.

Ijiri, Yuji. 1998. Available online: https://www.youtube.com/watch?v=7YE8lWl3tAA (accessed on 27 February 2023).

Maiti, Moinak, Ivan Kotliarov, and Vitalii Lipatnikov. 2021. A future triple entry accounting framework using blockchain technology. *Blockchain: Research and Applications* 2: 100037. [CrossRef]

nChain Limited. 2019. The Metanet A Blockchain-Based Internet Technical Summary. Available online: https://nchain.com/wp-content/uploads/2022/09/The-Metanet-Technical-Summary-v1.0.pdf (accessed on 10 October 2023).

Soll, Jacob. 2014. *The Reckoning Financial Accountability and the Rise and Fall of Nations*. New York: Basic Books, p. 34.

Sunde, Torje V., Stephan Nilsson, Vidar S. Nordtømme, and Olav B. Pettersen. 2022a. The Financial Supervisory Authority of Norway Regulatory Sandbox 2021—Use of Blockchain to Obtain, Store and Provide. Available online: https://www.finanstilsynet.no/tema/fintech/finanstilsynets-regulatoriske-sandkasse/pulje-2-informasjon-om-sandkasseprosjektene/ (accessed on 17 July 2023).

Sunde, Torje V., Stephan Nilsson, Vidar S. Nordtømme, and Olav B. Pettersen. 2022b. The Financial Supervisory Authority of Norway Regulatory Sandbox 2021—Use of Blockchain to Obtain, Store and Provide. [English translation]. Available online: https://abendum.com/wp-content/uploads/2023/07/Final-Report_26_01_2022-English.pdf (accessed on 17 July 2023).

Wright, Craig S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. August 21. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440802 (accessed on 9 May 2023).

Wright, Craig S. 2016a. Blockchain-Based Accounting: General-Ledger Posting (WP0001). Available online: https://craigwright.net/blog/bitcoin-blockchain-tech/blockchain-based-accounting/ (accessed on 9 May 2023).

Wright, Craig S. 2016b. Cryptographic Method and System for Secure Extraction of Data from a Blockchain. Europe Patent EP3420669A1, February 23.

Wright, Craig S. n.d.a. WP0060 Consolidated Accounting.

Wright, Craig S. n.d.b. White paper 0042 Secret Value Distribution.

Wright, Craig Steven, and Stephane Savanah. 2017a. Consolidated Blockchain-Based Data Transfer Control Method and System. U.S. Patent US20190073646A1, February 23.

Wright, Craig Steven, and Stephane Savanah. 2017b. Determining a Common Secret for the Secure Exchange of Information and Hierarchical, Deterministic Cryptographic Keys. WO Patent WO2017145016A1, February 16.

Wright, Craig Steven, Chloe Ceren Tartan, and Alexander Tennyson Mackay. 2020. Computer Implemented Method and System for Storing Certified Data on a Blockchain. U.S. Patent US 2022/0368539A1, September 14.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.