Triple Entry Accounting

We all know how insubstantial internal ledger entries are, and how we can only rely on them to the extent that we trust our internal processes (e.g. who can forget the Enron events of 2007 leading to a popular view that accounting and audit have failed us).

On the other hand, we also see how solid payment systems are. Whether bank- or Government- or private-run, payments generally work. When these multi-party activities do not work, all hell breaks loose, and people run, sometimes quite literally, to other systems.

When accounting ledgers break, we sigh and move on. Triple entry accounting, via Block Chain Ledgers, takes us from the unreliable fantasy of the accounting entry to the hard concrete reality of the RTGS payment: the secure Block Chain Ledger is as solid as a bitcoin payment, but without the technobabble (mining etc.).

Quite simply, the basics of accounting have not changed for hundreds of years.

Today, the many well-known issues are trying to be addressed by formulating new rules, employing more auditors and investing in more IT infrastructure. This I believe is the wrong approach.

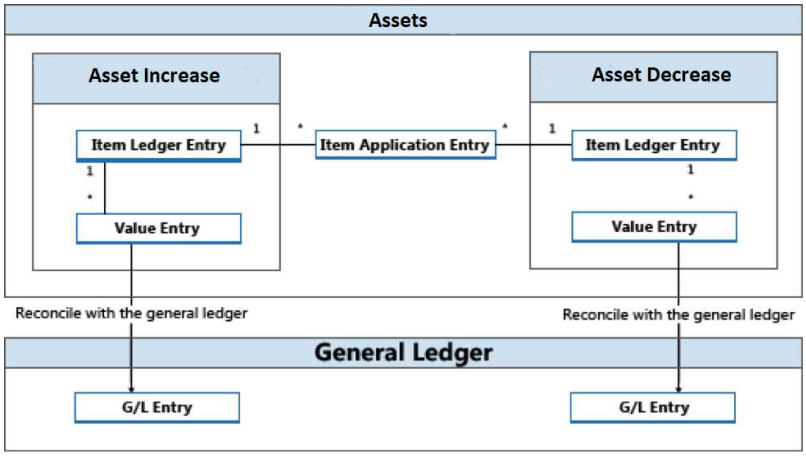
I believe most of the above are solvable by doing four things;

1. Make the accounting of a business activity an integral part of that activity. Instead of treating it as a many separate process. What if the invoice was the journal?
2. Sharing data between transacting entities. Any business transaction involves an agreement of value by one or more parties. Privacy is not a problem as all parties must record the same data.
3. Securing each ledger, with immutable write once block chains, brings existing accounting systems into today's digital world, without throwing away everything.

Block Chain Ledgers achieve the first two things by creating and signing inter-ledger transactions, via the generation of a cryptographic proof that the transaction happened and the two transacting parties had the rights & obligations to the unspent ledger values referenced by the transaction.

The Asset Ledger View

If we consider the transfer of assets via a set of ledger entries between two transiting parties (an inventory system) via traditional double entry accounting systems below.



If Alice Ltd wants to pay Bob Ltd, Alice will no longer rely on its accounting systems alone to describe this situation, and neither will Bob. Both of these parties will share a “receipt” that is cryptographically signed by some party that has mediated it (could be an existing bank such as ANZ, the Reserve Bank of Australia, or any mutually agreed third party with appropriate legal capability to demonstrate legal finality to the transaction.

Item Ledger Entries

We can see that purchases increase assets while sales decrease assets, and that within each ledger entry the quantity of the asset increases must equal the quantity of the asset decrease between the two systems.

Posting Date	Entry Type	Document Type	Document No.	Item No.	Quantity	Invoiced Quantity	Remaining Quantity
1/26/2017	Purchase	Purchase Re...	107039	1150	1	1	1

We can see the Asset Block Chain Ledger augments the traditional accounting system ledger by providing a way for parties to share asset transactions as if they were as solid as payments. To differentiate between traditional account systems and this new form of secure inter-ledger based double-entry accounting system solutions within this article, we will refer to a triple entry accounting system as **The Block Chain Ledger**.

Triple Entry Accounting

Triple entry accounting is very simple, as shown above, there are three parties, each holding a copy of the same receipt, hence the label "triple-entry". In the Block Chain Ledger world, that middle inter-mediator is the public ledger block chain and the two other parties are the Private Ledger Block Chains, all are just secure double-entry ledgers, nothing more from an accounting perspective.

The receipt or public ledger journal above, itself is secure, as it is cryptographically co-signed and hence authorised by the payer, the recipient and cryptographically signed off by a mediator (as a

minimum). It represents solid evidence that it is practically irrefutable in terms of the facts on record, and it is trivially automated in audit terms.

Holding this entry is far more flexible than Alice and Bob relying solely on their double-entry systems. Because one can build the double-entry systems out of the collection of receipts any time you need them, and secondly, it is so strong that it can be used as evidence to create derivative claims. E.g. it's a set-up for securitisation or loaning contracts or other more advanced uses. And, it's a lot easier to audit because it is such non-repudiable evidence.

The Block Chain Ledger from 2004 was the first at-scale experiment in a large scale triple entry issuance. In part, seeing what happens on the blockchain generates excitement because we perceive an ability for any company to turn its stalled internal assets into contracts that are then dynamically mediated through cryptographic receipts.

Once one can issue all the accounted assets into a triple entry arrangement that others will instantly respect, finance will democratise Savings for every Accounting Ledger entry.

So where are we at today?

With the release in 2015 of the first commercial Block Chain Ledgers the double-entry accounting of each transaction between any two parties, Alice and Bob can now be secured and audited via their individual "Private" Block Chain Ledgers. With the introduction of an intermediary or Public Block Chain Ledger (public ledger above) and communications based upon existing inter-ledger protocols, today we have a full implementation of a commercial "triple entry accounting".

Each end accounting system and the intermediary public block chain provides a "secure" distributed triple entry ledger, which can be reconciled instantly on each and every transition on a global basis.

The globally decentralised Block Chain Ledgers will always be reconciled, each and every ledger journal will always balance across the global ledger.

This concept can be expanded, Bob above can maintain a local ledger containing all its adjustments, however, and it can also maintain a distributed ledger which contains details of all transaction or contracts. As the distributed ledger is agreed upon by all participants and there are hardware secured digital signatures to provide a degree of non-reputability, Auditors can rely on this ledger. The auditor's job starts getting easier, finally, the digital world helps to secure old-world double-entry systems.

Worked Purchase Contract Example:

1. Alice -> Purchase Widget from ->Bob.
2. Bob ->Ships Widget and Invoice -> Alice
3. Bob -> Posts journal DR Account Receivable, CR Income to Private BCL
4. Posts Transaction, with unique TxnId to Public Block Chain Ledger(PBCL)
5. Alice-> Posts Transaction DR Expenses, CR Accounts Payable to Private BCL
6. Post-transaction with same TxnId to Public Block Chain Ledger(PBCL)
7. PBCL-> combines messages 4, and 6 along with their signatures (Contract)
8. PBCL-> countersigns and timestamps the combined message 7, along with transactions (i.e DRs and CRs) and posts to the PBCL.

Worked Payment Contract Example:

1. Alice -> Pays ->Bob.

2. Alice-> Posts Transaction CR Bank, DR Accounts Payable to Private BCL
3. Posts Transaction, with unique TxnId to Public Block Chain Ledger(PBCL)
4. Bob->Receives Payment->From Alice
5. Posts journal CR Account Receivable, DR Bank to Private BCL
6. Posts Transaction, with unique TxnId to Public Block Chain Ledger(PBCL)
7. PBCL-> combines messages 3, and 6 along with their signatures (Contract)
8. PBCL-> countersigns and timestamps the combined message 7, along with transactions (i.e. DRs and CRs) and posts to the PBCL.

While the above could represent a practical Public Block Chain Ledger, the commercial reality is likely to drive a range of specialist PBCL, i.e. each focused on a specific use case. Collectively these will form the globally decentralised Public Block Chain Ledger. Each segment of the PBCL is navigated using Internet-accessible entries, within the domain blockchainledger.net. This is what a "true" distributed systems mean, it is not about shuffling around the same blobs of data as is the case with all blockchains including bitcoin today., it's similar to try and use a single double-entry accounting ledger to running the whole world's transactions, it is conceptually flawed... but digress.

In the case where a bank is offering the PBCL the changes to the above example are trivial. The point is all types of interactions P2P or traditional intermediary are supported. In the case of a bank intermediary, the Public Block Chain Ledger for each entity would simply be their "Bank Statement". The unique aspect of an architecture with both private and public Block Chain Ledgers, is that the distributed PBCL supports all "between" entity transactions, and hence the concept of "gateways" as used in almost all crypto-currencies is not required. With the PBCL and P2P transactions, there is no settlement or clearing delays, as all entries are atomic and instantaneous. In the case of no intermediary there are some addition joint signatures required to secure the transaction, over the intermediary signature used, but all standard cryptographic techniques.

The fully distributed Global Public Block Chain Ledger is the record of truth, and available to all, the atomic nature of all Block Chain Ledger transaction, allow instantaneous transfers to occur.

In fact when the PBCL is applied to P2P payments, we do not see why all payments should not be free, as our analysis shows the incremental cost is close to zero, and each Private Block Chain Ledger can easily support its part of the decentralised PBCL. The same could be applied to all commercial transactions which are capable of being processed through an accounting system, virtually everything.

An enhancement within the Block Chain Ledger over bitcoin, allows each and every block to have a unique private ECDSA key based signature, is applied to each transaction block, This enhancement allows instantaneous sealing of each block and all transactions in time (sequence), plus globally unique identification of each block and hence the ability to instantly post to the PBCL, this also supports detection of duplicate transactions, as the private Block Chain Ledgers cannot be changed or altered in any way by either Alice or Bob, the PBCL can request the parts of the block chain necessary to validate each Private Block Chain Ledger before signing the triple entry.

The public block chain ledger provides a real-time, atomic transaction, and reporting system.

The atomic transaction is completed once the PBCL entry in 8 above is posted to the PBCL, each party Alice and Bob and anyone else can verify the "Contract" or transaction, with a deterministic level of non-repudiation.

An auditor can request all transaction data, and if required can counter sign, a Block within the PBCL and hence bind parts of both Alice and Bob's private Block Chain Ledger and also the PBCL in time.

The point is that if one is inherently happy about Transactions, then the accounting and audit process becomes much simpler; no need for reconciliation or for an auditor to mess about with 3rd party confirmations (which are almost never returned!). An auditor can also gain 100% assurance into existence and completeness of transactions with counterparties – this is the holy grail of audit.

As mentioned in the above comment, this is super useful, not only for audit. Due diligence, tax reporting, generating data for financial reporting also benefit, in fact almost everything benefits form this approach.

The inter-ledger protocol contains a set of transactional protocols which will allow interaction between each Private Block Chains and the Public Block Chain, this existing code and global internet, underpins the commercial set of Block Chain Applications that in most part have nothing do with digital money. Additionally as the Block Chain Ledger is based on traditional double entry accounting systems a mixture of P2P and more traditional Public Block Chains can be utilised. As above the Reserve Bank could run an inter banking Block Chain Ledger, that has all of the existing frameworks, but in this case actually secure and suitable for the modern "digital" world we all work in.

Welcome to the Internet of Transactions.

The intermediary Public Block Chain Ledger is in fact "signing off" or witnessing, both sides of the block chain ledgers transaction, this is in fact the "Contract" process, the ledger Transactions could be stock trading, property sales, or in fact anything that can be processed through a standard double entry accounting system.

The Internet of transactions ubiquitous, seamless, comprehensive and secure method of transferring money value allows for the distribution of monetary value in all sorts of novel ways.