Blockchain: The Making of a Simple, Secure Recording Concept

By Yigal Rechtman

Ever since the double-entry bookkeeping system was created in 1340, accountants and business owners have been focused on the fidelity of financial reporting systems. The double- entry system prevented misreporting and forced accounting to be reliable. With more reliance on computerized information systems, more reliable information is imperative. The blockchain database structure is designed to achieve this reliability.

What started as a theoretical vision of integrity in recordkeeping has evolved into a distributed database structure with high fidelity of information quality and availability. This database structure could help prevent and detect fraudulent transactions by trading parties. The blockchain concept carries some risks, but with a built-in audit trail, these risks are manageable. The implementation of blockchain technology into corporate information systems is in its early stages, but it is likely to be adopted by diverse businesses, large governmental agencies, and various exchanges. Once mature and widely adopted, blockchain may bring about a "system of systems," or a master "journal of journals." Accountants, managers, and educators can play a pivotal role in this growth opportunity, and should be familiar with its basic tenants: an independent database self-validating a single ledger.

Background

In 1991, the need for electronic security was a major concern of bankers, regulators, and service providers. The concept developed to enable the public trust financial data produced by online banking, online trading, and electronic commerce was a "distributed ledger," whereby the assumption is that every custodian of the ledger is independent from the others (Stefan Konst, "Secure Log Files Based on Cryptographically Concatenated Entries," August 2000, http://bit.ly/2r1f9qW). The ledgers are regularly synchronized, and because there is no single controlling custodian, if there are conflicts between entries in the ledgers, the entry with the simple majority of custodians becomes the de facto winner. This feature keeps all the custodians honest (error and fraud prevention) and accountable (error and fraud detection). With the advent of open-source computing in the late 1990s, blockchain open-source software was implemented, which enabled the creation of—among other financial innovations—virtual currencies such as bitcoin.

This article will revisit the historical development of blockchain infrastructure and highlight the accountant's perspective of such a platform. The question of risk from an accounting and auditing perspective are of particular interest, because these risks presented by virtual currencies are still causing concern and require risk management.

An Accounting Perspective

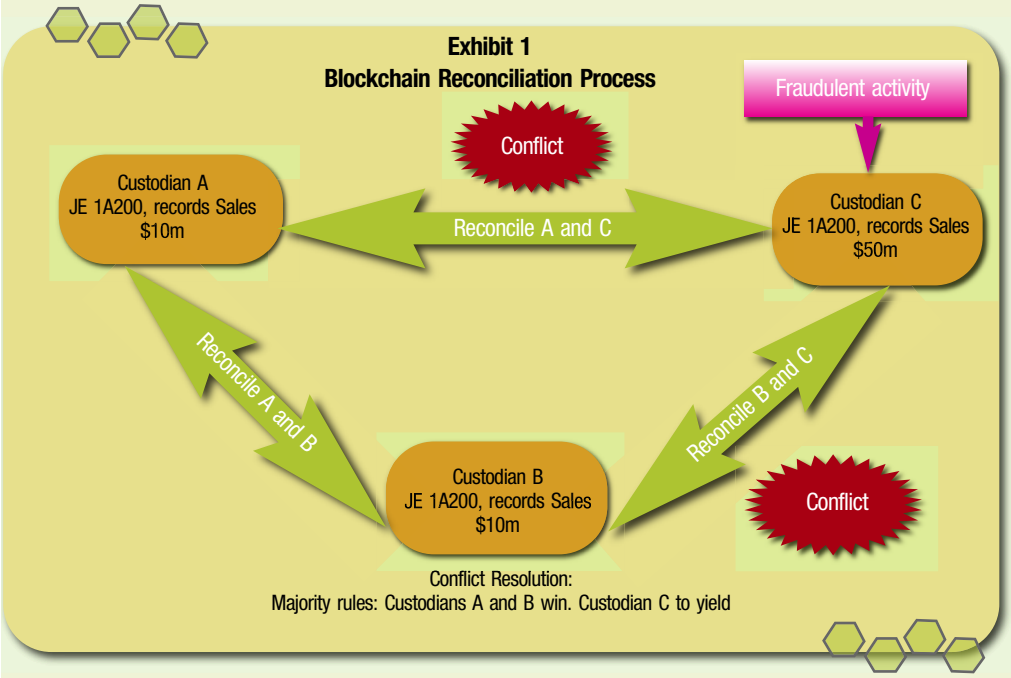
A blockchain is akin to journal entries in original books and records. As with a journal entry, a single datum is called a "block," which cannot be deleted or modified, only reversed. This way, changes have an audit trail, and transactions are secure—in theory. Blocks in a blockchain, in addition to containing required data, can carry additional audit trail and analysis data, such as the total of the affected accounts before and after the transaction. This additional data facilitates both antifraud measures and efficiencies in the database design.

At the onset, a blockchain exists in multiple, "sibling" databases, which have a "distrust" relationship between them; custodians might not even know who the custodians of the other siblings are. Because the exchange of information can be done in standardized, public domain format [for example, Extensible Markup Language (XML)], there is a higher level of fidelity between the single, majority rule concertation of ledgers. These ledgers could be helpful in multiple stock exchanges, dark pools for funding, or even with the much-awaited crowdfunding platform authorized

by the 2012 Jumpstart Our Business Startups (JOBS) Act (Yigal Rechtman and Susanne O'Callaghan, "Understanding the Basics of Crowdfunding," *CPA Journal,* November 2014, http://bit.ly/2r1cOw1).

Accordingly, in both theory and practice, even if one custodian misrecords an over-the-counter stock exchange, the fidelity of the record is maintained, with the majority of sibling databases "voting" to resolve the conflict. Each database synchronizes on a regular basis and uniquely identifies each transaction—along with other changes such as account total balances, user information, date/time stamps, and whatever audit trail could be helpful for the maintenance of the overall system fidelity. Accordingly, all postings and changes are synchronized at regular intervals. *Exhibit 1* illustrates this process.

Exhibit 1
Blockchain Reconciliation Process



In an over-the-counter stock exchange, the custodians remain the same, but the initiating party is the stockbroker or stock parties who executed the transaction, as in *Exhibit 2.* Custodian C will be found in violation of the two data elements; the majority rule will conclude that the stock price ($3) is different than the records, and that the multiplication of the number of shares by the dollar cost is erroneous. The strength of the blockchain is evident in this example because the terms can be checked both for integrity by the custodians' resolution and for the block's internal integrity, such as the total transaction value (units × cost).

A virtual currency such as bitcoin utilizes the blockchain method in its coding; because the virtual currency databases are decentralized, no single custodian has control of the entire ledger system at any time. The anonymity of the sibling databases' custodians causes them to maintain a high rate of accuracy. Some observers, however, are concerned that blockchain is reaching its practical limits. In theory, if a single person controls 51% or more of the custodians in a certain market this owner could effectively make changes to all databases at once. Under such circumstances, one person can be the master of the entire financial system. Although this practical limit has not been reached—yet—there is no assurance that it cannot happen. One theory contends that if the practical limit of 51% is reached, then more custodians can be generically started, diluting the majority; however, there has never been a test of such an incident. Regulators and researchers remain concerned about the "51%" scenario (Emily Spaven, "European Banking Authority: 51% Attack Remains Bitcoin's Biggest Problem," Jun. 17, 2015, http://bit.ly/2r1lJgX). The price of virtual currency is controlled by market forces of supply and demand, among other factors. If one person controls more than 51% of the custodians of a virtual currency, that price could be manipulated by revising the real price exchanged between two anonymous parties (as all parties in a blockchain transaction are), creating a fraudulent gain.

Audit Trail

A blockchain can also be constructed with a built-in, native audit trail; for example, a record of a dividend disbursement cycle can be constructed in such a way that the disparate databases maintain blocks that describe the dividend recipients and also include the audit trail for the cycle (e.g., owner's identity, stock split terms, date stamp for stock transactions, owner details for tax reporting and compliance). Although such a data set can be maintained by a single, centralized database that controls the entire stock ownership for a single listed company, the multiple sibling databases of blockchain create a more robust audit trail. Even if one block in one database is deleted, the other databases will synchronize themselves, correcting the damaged database and undoing the deletion. This redundancy feature can be performed on multiple levels during the life cycle of the stock ownership.

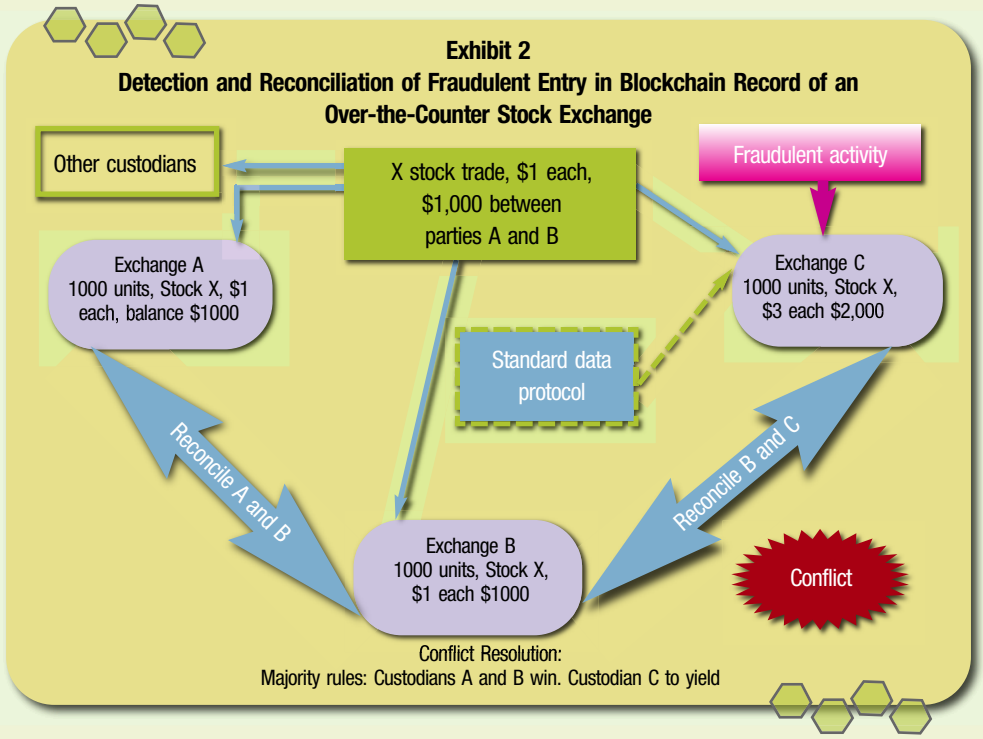
Some argue that such a redundancy could reduce the risk that the business cycle will be tampered with without leaving marks ("Blockchain Application in Insurance," Deloitte, 2016, http://bit.ly/2qGjU68). In expanding the blockchain for an audit trail, the dividend

payment system in the example above could facilitate an end-to-end trusted journal containing the trusted ledgers of everyone who actually received a payment. The blockchain dividend journal could also interface with the tax reporting journal; this type of integration can generate a journal of journals, fully supported by the audit trail. The unique journals of various business cycles could be maintained both separately and in a journal of journals for the collective. Each system's ledger would be robust and redundant and have high fidelity. Such redundancy, with a single point of entry and multiple points of disposition and resolution, can also create efficiencies for trading parties. These efficiencies are viewed by some, especially in the virtual currency world, as an incentive for growth in the capital markets (Paul Vigna, "Delaware Considers Using Blockchain Technology," *Wall Street Journal,* May 1, 2016, http://on.wsj.com/2rAUfec).

Other Implementation Risks

There are risks to blockchain other than the above-mentioned risk of a single person controlling an entire system. First, the risk of misconfiguration when implementing abstract, generic, redundant databases is not trivial. XML is a mature communication and exchange technology, as are Extensible Business Reporting Language (XBRL) and other standard protocols for data exchange. Blockchain, however, may test the limit of data integrity, as it is exchanged and synchronized between distrustful custodians of large databases. This is a well-documented risk; even well designed information systems can experience a breakdown when user access controls are poorly configured. Software in general, and user access in particular, can easily become poorly configured (see Vincent C. Hu, David F. Ferraiolo, and D. Rick Kuhn, "Assessment of Access Control Systems," National Institute for Standards in Technology (NIST), September 2006, http://bit.ly/2q4V5yI; "Security and Privacy Controls for Federal Information Systems and Organizations," NIST, revised Jan. 22, 2015, http://bit.ly/2q5cFTr). Equivalently, the configuration of a blockchain system is not yet a mature, error-free, or frictionless process. Rather, the risks of misconfiguration of access controls, processing, and storage integrity should give pause to managers who adopt blockchain, consultants who advise on the implementation, and auditors facing the challenge of auditing such a system.

Exhibit 2
Detection and Reconciliation of Fraudulent Entry in Blockchain Record of an Over-the-Counter Stock Exchange



The Road Ahead

Blockchain databases represent a promising tool for the capital and regulatory markets, but it also presents certain risks. Business leaders in large, diverse companies would do well to consider a blockchain database underlying their companies' enterprise resource planning and accounting information systems (ERP/AIS). Besides the built-in features for prevention and detection of fraud, as well as the benefits to the audit trail, the underlying database provides redundancy in reporting and efficiencies in populating data. Larger, diverse entities are the ideal subjects for such adoption and evolution, being able to spend greater resources on such systems.

Accounting professionals can also take a lead role in advising on the implementations of blockchain systems, or the auditing of the implementation's fidelity. Educators and researchers also have their work cut out for them; once investment in new underlying databases is under way, researchers will find plenty of practical applications to be addressed. Educators will also need to prepare future managers and accountants to take advantage of the opportunities of blockchain databases.

While the concept of a high-fidelity journal is an idea as old as double-entry bookkeeping, new technology means dramatic changes for the CPA of tomorrow. ❑

Yigal Rechtman, CPA, CFE, CITP, CISM, *is a principal at Grassi & Co. CPAs and is in charge of the litigation support and forensic accounting practice. He is also a member of The CPA Journal Editorial Board.*