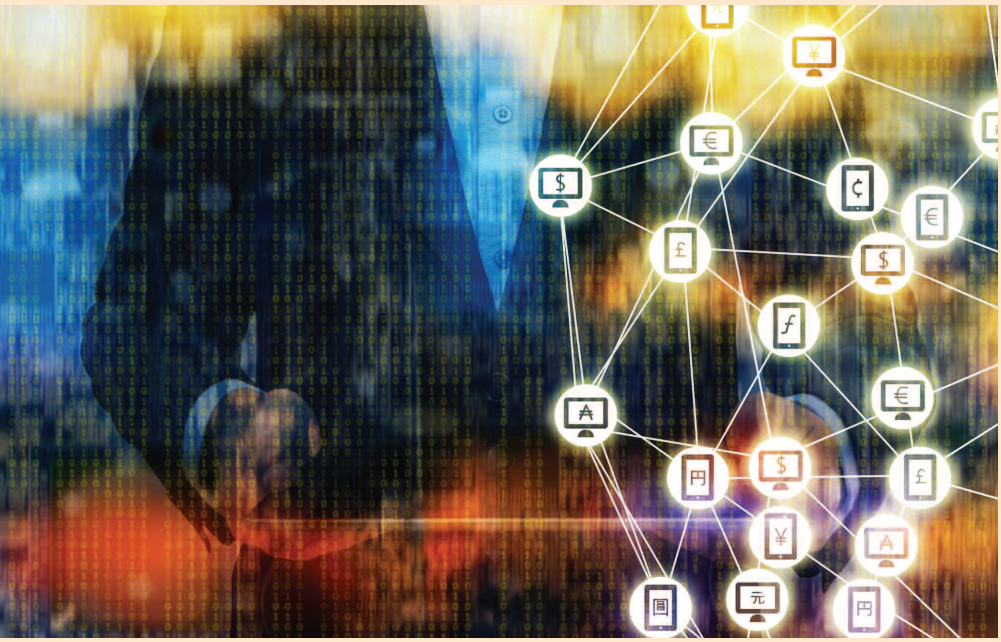
Blockchain: An Emerging Solution for Fraud Prevention

By Jun Dai, Yunsen Wang, and Miklos A. Vasarhelyi

Fraud prevention is a critical and ongoing consideration for companies all over the world. According to the 2016 *Report to the Nations on Occupational Fraud and Abuse* issued by the Association of Certified Fraud Examiners (ACFE) (http://bit.ly/2r0JGVC), the total loss caused by fraud events in 2016 exceeded $6.3 billion, with an estimated 5% loss of annual revenues in a typical organization. Altering or deleting information in the companies' accounting systems, changing electronic documents, and creating fraudulent electronic files were the main methods to conceal frauds. In order to reduce fraud risk or even prevent frauds, a more secure accounting information system that can deter tampering from either outside parties (e.g., cyber attackers) or inside parties (e.g., employees) is needed.



Blockchain, a public, decentralized ledger first used to enable bitcoin trading, has the potential to serve as a secure accounting information system. A key feature of blockchain is that it decentralizes system management and authorization to a network of computers. Those computers together verify transactions based on certain prespecified rules (controls) that have been embedded in the system. To avoid a single point of failure, the transaction verification process is controlled by all the computers, rather than managed centrally. The computers jointly supervise system operation and prevent the information in the ledger from being tampered with. Because of this feature, blockchain can effectively prevent one or several individuals in collusion from overriding controls, or illicitly changing or deleting official accounting records. Moreover, as the embedded rules are automatically followed without much human intervention, it can enforce the operation of controls. By incorporating blockchain technology to their accounting information systems, companies could reduce fraud risk by maintaining a clean, secure database and a strengthened control system.

What Is Blockchain?

The first generation of blockchain was a public ledger that securely recorded the trading of bitcoin in the form of a chain of interlocked blocks (Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 2008, http://bit.ly/2q4tihZ). The *Exhibit* shows the general process of sending money to another party in a blockchain. Any party can participate in trading and contribute to the verification of transactions based on preencoded rules; the validated transactions are then posted on the blockchain ledger. Once a transaction is posted and confirmed, the entries related to it will be cryptographically sealed and shared with the entire chain. This makes falsifying or destroying records to conceal fraud activities practically impossible.

The main characteristics of blockchain are as follows:

- Decentralized—everyone in the blockchain network can access the entire list of transactions, and they jointly operate and control the whole system.
- Strongly authenticated—the identity of each participant in blockchain transactions can be verified.
- Tamper-resistant—once a transaction is posted on the blockchain, it becomes unchangeable and irreversible.

These characteristics allow blockchain to serve as the foundation of a new accounting information system that prevents accounting records or related electronic documents from being altered or deleted. In addition, sharing accounting information with many parties (e.g., business partners, stakeholders, managers, auditors) allows all of them to participate in performing independent examination of transactions and delivering real-time

assurance (Jun Dai and Miklos A. Vasarhelyi, "Towards Blockchain-based Accounting and Assurance," forthcoming, 2017).

The second generation of blockchain moved towards a new type of application called a "smart contract." Smart contracts are defined as "user-defined programs that specify rules-governing transactions" (Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi, "Step by Step towards Creating a Safe Smart Contract," Nov. 18, 2015, http://bit.ly/2q1ywf6). For example, a person's last will and testament could be encoded as a smart contract so that the inheritance could be automatically bequeathed to recipients if predetermined conditions (e.g., the death of the donor or a specific point in time) are reached (Melanie Swan, *Blockchain: Blueprint for a New Economy,* O'Reilly Media, 2015). Smart contracts can securely operate on a blockchain; any party can perform verification of transactions in compliance with the embedded rules. More importantly, blockchain users can program their own rules into a smart contract to execute specific tasks. For example, management can encode company-specific rules into smart contracts to enable automatic controls (Dai and Vasarhelyi 2017). The applications of smart contracts have been discussed in a wide range of areas, from peer-to-peer intellectual property trading to self-monitoring online gambling. Ultimately, they could facilitate the establishment of decentralized autonomous organizations/corporations (DAO/DAC) (Swan 2015). In a DAO/DAC, management could use smart contracts to transcribe governance into a blockchain, which could be shared and supervised by many independent crowdfunding investors to help mitigate fraud risk.

Using Blockchain to Prevent Fraud

The convergence of accounting and blockchain could create a totally new accounting information system in which every transaction ever executed is publicly available and verifiable in real time. Furthermore, blockchain could be used to prevent and detect fraudulent transactions. Because blockchain keeps the record of an asset transfer, any type of misappropriation can be detected by tracing through the blockchain.

To combat financial reporting fraud, such as overstatement of revenues by means of channel stuffing or round-tripping, the transactional data in blockchain could provide valid evidence showing any potential irregularities involving revenue recognition (Yunsen Wang and Alexander Kogan, "Designing Privacy-Preserving Blockchain-Based Accounting Information Systems," working paper, 2017, http://bit.ly/2qJDEJc). In addition, the continuity, irrevocability, and irreversibility of a blockchain ledger could prevent management from creating fictitious transactions or backdating options. The transparency of blockchain will make it easy for forensic accountants to access and examine the material related-party transactions (Dai and Vasarhelyi 2017). Furthermore, the risk of receiving checks without sufficient funds could be avoided. Therefore, blockchains not only increase the chance of detecting fraud, but also pressure management to reduce earnings manipulation.

Smart contracts encoded with accounting and business rules could also provide efficient controls of business processes in order to prevent fraud. Smart contracts can be embedded with advanced access control criteria that allow only authorized users to create transactions. A well-designed blockchain should have a precise and dynamically controlled system to designate the roles of connecting to the blockchain, initiating transactions, and creating assets. In addition, the relevant criteria could be encoded in smart contracts to ensure all conditions have been met before recognizing any sales revenue. Moreover, smart contracts could add intelligence into accounting processes by integrating big data and predictive analytics. Combined with big data, smart contracts could layer on top of the reactive-to-predictive transformation to achieve a dynamic, self-optimal, risk-aware measurement of companies' performance. For example, by encoding a fraud prediction model into a smart contract, a credit card company could adjust the credit limit of an account based on the spending behavior of the account holders (Dai and Vasarhelyi 2017).

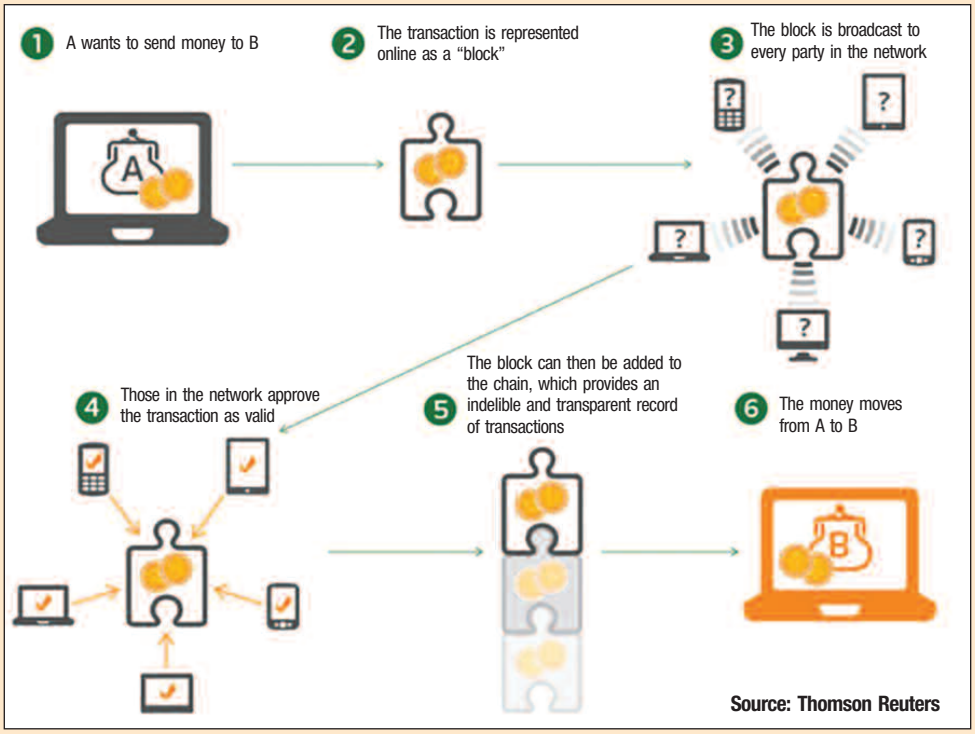
Because blockchain keeps the record of an asset transfer, any type of misappropriation can be detected by tracing through the blockchain.

Unfortunately, not every fraud scheme can be automatically prevented by blockchain. For example, corruption or bribery schemes are hard to detect in both traditional accounting and blockchain accounting systems.

Challenges and Potential Solutions

Ideally, the concept behind using blockchain to prevent fraud is to increase information transparency and allow

Exhibit
Illustration of a Bitcoin Blockchain



many independent parties to perform verification in order to guarantee the validity and accuracy of transactions. In the real world, however, this mechanism may not be as effective as it should. For example, if the CEO of a company has exclusive and total control over its blockchain (i.e., the CEO can create fictitious transactions and force a group of entities to pass the verification), the whole spirit of decentralization of management and supervision is nullified. Instead, a blockchain should be deployed among different, relatively independent parties such as suppliers, clients, creditors, and banks. These parties could become independent verifiers charged with uncovering fraudulent transactions, especially those transactions involving outside parties. For example, if a company claims it did not receive a payment from its client, many independent parties could go into the blockchain and see if the payment transaction exists; similarly, different areas within a company can also verify and supervise transactions for each other.

Alternatively, the involved outside parties could also publish their accounting information on a blockchain, providing additional independent evidence (e.g., payment check, cash transaction, bank account statement). These pieces of information make up a network of "crowdsourced evidence" that can be used to prove the validity of transactions booked on blockchain systems. Moreover, in a DAO/DAC, the investors could also contribute to the review of the company's accounting information by utilizing their continuous access to data via blockchain.

Many blockchain mechanisms are designed to avoid the "51% attack"—that is, one in which the attacker has more computational power than the rest of the network combined—in order to guarantee the validity of transactions. The basic assumption of these blockchain mechanisms is that a large amount of nodes participate in the system, making it almost impossible for one to have the capability to control more than half of the nodes in the system. In general, the more companies are involved in the network, the harder it is for one or a few to take over the blockchain system. In reality, however, and especially in the adoption stage of a new technology, it is difficult to motivate a large number of enterprises to participate. Therefore, blockchain is more likely to be deployed and used among a limited number of pilot entities, which could collude to create fraudulent transactions. To mitigate the collusion risk, different priorities could be granted to different parties for transaction verification based upon their roles. For example, a bank could have the priority to verify a cash transaction, or regulators or auditors could be given the authority to hold a transaction with high risk of fraud before it is confirmed.

Changing the Rules of the Game

Blockchain provides the potential opportunity to prevent fraud in advance or detect fraud shortly after it occurs. By bringing various outside parties, such as business partners, creditors, and investors, into the loop, blockchain could enable a real-time alerting schema for fraud prevention. It must be noted that the process of mapping the double-entry accounting system onto a blockchain infrastructure, and using it to deter corporate frauds, is still in its infancy. There are many challenges and risks, not only for the trading partners that potentially rely on blockchain for transactions, but also for the regulators who oversee them. ❑

Jun Dai *and* ***Yunsen Wang*** *are assistant professors at Southwestern University of Finance and Economics, Chengdu, China, and Ph.D. candidates at Rutgers University, Newark, N.J.* ***Miklos A. Vasarhelyi, PhD,*** *is the KPMG Distinguished Professor of Accounting Information Systems and Director of Rutgers Accounting Research Center and Continuous Auditing & Reporting Lab at Rutgers University.*