

Blockchains: A New Horizon for Accountants

Anshuman Singh

Information Systems and Technology Department
College of Business Administration
University of Missouri-St. Louis
St. Louis, MO 63121, USA.

Vijay Anand

Information Systems and Technology Department
College of Business Administration
University of Missouri-St. Louis
St. Louis, MO 63121, USA.

Stephen Moehrle

Accounting Department
College of Business Administration
University of Missouri-St. Louis
St. Louis, MO 63121, USA.

Dinesh Mirchandani

Information Systems and Technology Department
College of Business Administration
University of Missouri-St. Louis
St. Louis, MO 63121, USA.

Abstract

The technology with arguably the greatest potential to impact the Accounting profession is blockchain. A blockchain is an implementation of a shared ledger in a peer-to-peer network of participating members. A ledger records monetary transactions for an account where the transactions are organized into debit and credit (or assets and liabilities) columns, and a beginning and ending balance is calculated for a given period of time. Historically, ledgers were maintained in a centralized manner with some entity responsible for adding entries into the ledger and another (or the same) entity verifying the integrity and correctness of the ledger. The separation of duties of recording and verifying entries in the ledger gave birth to the audit profession. This paper provides a high-level overview of blockchain technology, smart contracts and triple-entry accounting and discusses impacts on the Accounting profession and education.

Introduction

In today's digital economy, blockchain-based shared ledgers are making the entry and verification of ledgers decentralized and more robust against fraud and cyberattacks. Blockchain technology enables the ledger to be shared across any number of participants over a peer-to-peer computer network, with each participant having a copy of the ledger [1]. A peer-to-peer network is not hosted by a single centralized entity. A client software is installed by each participant and the software runs the consensus protocol as well as manages a copy of the ledger.

The client lets the participant add entries to the ledger as well as perform validation by executing the implementation of the consensus algorithm. The network agrees upon rules that determine which participants can access and add entries to a copy of the shared ledger as well as which participants can verify the integrity of entries in the ledger. The enforcement of such rules is made possible using cryptography, access control, and consensus protocols. Any changes made to the shared ledger are reflected in each copy within minutes. This interaction is displayed in Figure 1, wherein each participant (represented as a human figure) maintains a copy of the blockchain. Whenever a transaction is requested, it is broadcast to the network, and verified by the participants. When consensus is reached, a new block (containing the transaction’s details, as explained below) is added to each participant’s copy.

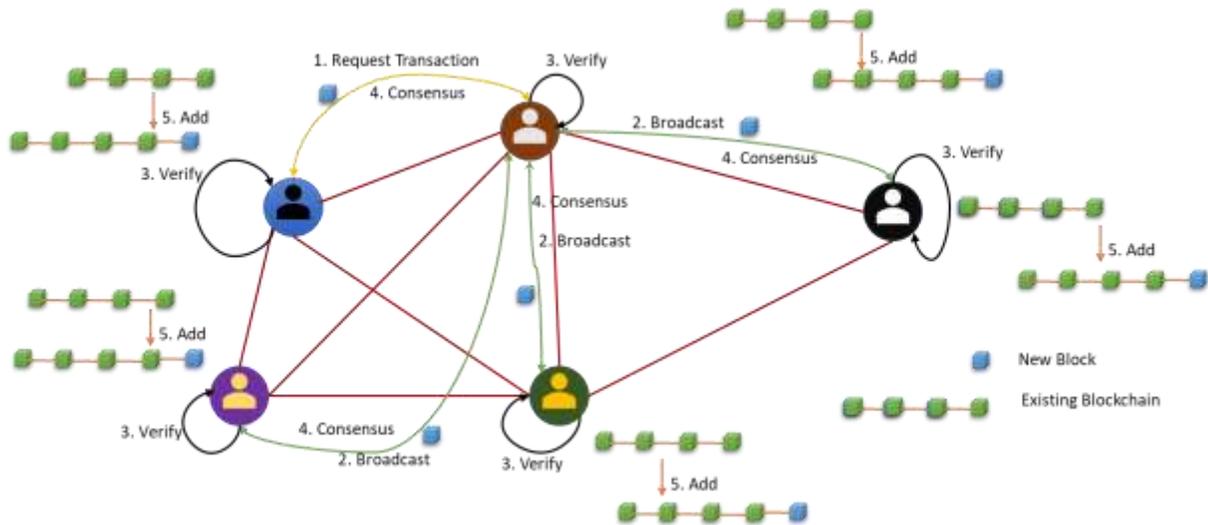


Figure 1. Operation of the Blockchain

Shared ledgers can be made *public* or alternatively be made *private* to a set of users. They can also be classified as either *permissioned* or *unpermissioned*. The integrity of permissioned ledgers can only be verified by trusted ledger owners whereas the integrity of unpermissioned ledgers can be validated by a consensus among users. A well-known unpermissioned public shared ledger is utilized by Bitcoin. Bitcoin supports operations on the ledger that lets users create monetary units that act as a store of value and also as a medium of exchange. these operations are made possible using cryptography, Bitcoin is called a *cryptocurrency*. Bitcoin consists of three components:

- A data structure called blockchain
- A consensus protocol for validating the integrity of the public shared ledger
- A peer-to-peer (i.e., decentralized) computer network for sharing the ledger ensuring all participants have equal access.

Blockchain

A blockchain’s data structure is a variant of a data structure called the *linked list* in computer science. Linked lists consist of noncontiguous data items connected by links (called pointers). Each link points to the *next* data block. Figure 2 shows the structure of a linked list.

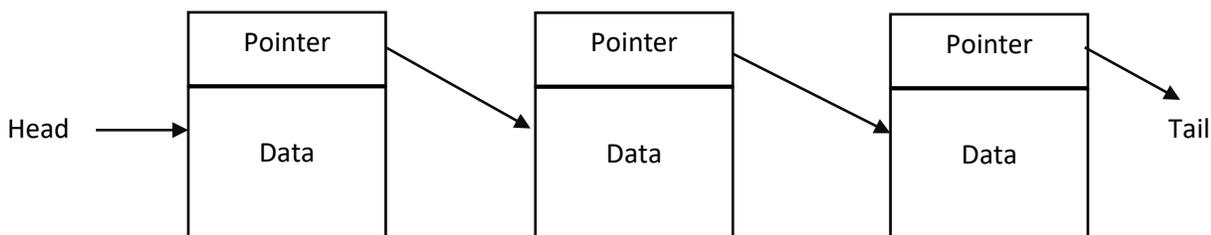


Figure 2: Linked list data structure

A blockchain is a linked list in which data blocks consist of transactions in the ledger and pointers point to the previous data block [2] (the original idea was proposed in the context of timestamping of document [3], [4]). A mathematical algorithm is used to map the data in the block to a fixed-length binary digit string known as the *cryptographic hash* (for example, the popular SHA-256 algorithm produces a 256-bit cryptographic hash). The pointer contains the hash of the previous transaction block. This combination of the pointer and the hash of the previous block is called a *hash pointer*. Since this data structure consists of a “chain” of transaction blocks pointing to previous transactions, it is referred to as a *blockchain*. Figure 3 shows the blockchain data structure.

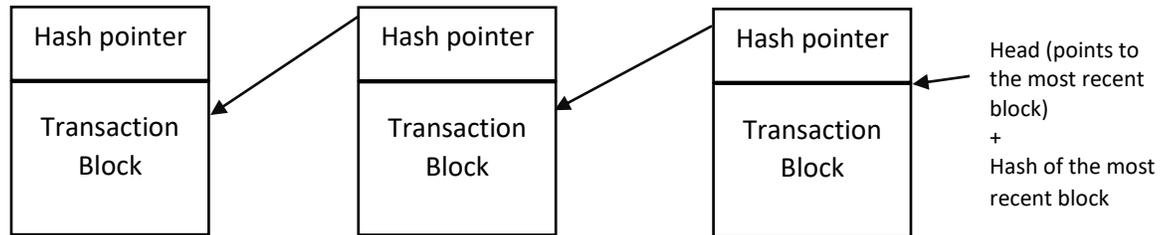


Figure 3: Blockchain data structure

Cryptographic hashes have two desirable properties: *Collision resistance* and the *one-way property*. *Collision resistance* means that no two data blocks can have the same cryptographic hash. So, if someone tampers with transactions in a block, the hash of the tampered block will not match its original hash and thereby break the chain in which the block is a member. The other property, called the *one-way property*, means that one can only compute the hash of the block, but given a hash, it is not feasible to compute the original block. In other words, you can only go in one direction, i.e., from the block to the hash and not vice-versa. This implies that once the hash of a block is added to the next block, the transactions of the previous block are locked. You cannot go back and change the transactions because of the one-way property of cryptographic hash.

As mentioned earlier, Bitcoin is an unpermissioned public shared ledger. Hence, any network participant can add and validate entries in the ledger. This leads to the question: *How does Bitcoin ensure that the ledger's integrity is preserved and there are no malicious entries in the ledger?* The answer is a cleverly designed distributed *consensus protocol*. Distributed consensus protocols ensure that participants reach a consensus on the true or correct state of the shared ledger. It has been shown theoretically that if no more than one-third of the participants are malicious, then the consensus protocol will always lead to a correct state of the shared ledger [2]. The consensus protocol comes in different flavors depending on the incentives offered to the participants to be involved and honest. Two commonly used consensus protocols are:

- **Proof of work:** This protocol is used by Bitcoin and rewards participants for their work in validating the ledger by creating new Bitcoins. This process of earning newly created Bitcoins in exchange for ledger validation work is called mining.
- **Proof of stake:** This protocol is used by Ethereum and is based on rewarding participants with a transaction fee using existing monetary units for the ledger validation work.

There are many other consensus protocols, each having its method of incentivizing honest ledger validation for participants.

Separation of duties and Smart contracts

The consensus protocol reinforces an important security principle that has long existed in accounting terminology called *separation of duties*. Separation of duties is the concept of not making a singular authority responsible for all phases of a transaction. As an example, we can split the context of acquiring an asset into two phases; one where a person places an order to purchase an asset, and second, where a different person enters this transaction into accounting records. With such a separation, collusion of two or more people will be necessary to commit a fraud, which is much less likely than when a single person is responsible for all phases of this transaction.

In recent years, there has been an emergence of shared ledger frameworks like Ethereum and Hyperledger [5], [6]. These frameworks let developers decide the types of transactions they want to support in their shared ledger system by implementing *smart contracts*.

Smart contracts allow participants to design more flexible mechanisms to trigger and validate transactions without the need for an intermediary [7]. For example, an account transfer is triggered only upon reaching a certain balance. Once the parties agree upon and enter into a smart contract, it becomes a part of the shared ledger system and is irreversible and fully trackable. Smart contracts are written in a programming language supported by these frameworks. Ethereum is based on its native cryptocurrency called Ether and the proof of stake consensus protocol. It provides the Solidity programming language to create smart contracts. Ethereum is suitable for deploying public ledgers in a business to consumer (B2C) setting. Hyperledger does not depend on a native cryptocurrency and works with a pluggable consensus protocol. In other words, you can bring your consensus protocol and plug it into the system. It provides the Golang programming language for creating smart contracts. It is suitable for unpermissioned (and even permissioned) private ledgers in a business to business (B2B) setting. Currently, there are many projects in the Hyperledger framework. The Hyperledger Fabric project is the most widely used for implementing private ledgers that support smart contracts [4].

Smart contracts coded into blockchains represent an important development for the accounting profession. For over 600 years, double-entry bookkeeping has enabled firms to maintain records that reflect what the firm owns and owes and also what the firm has earned and spent over any given period of time. For each transaction, separate entries are made in the books of the transacting parties. The issue with double-entry accounting is that there is not any connection between the different sets of books each firm holds.

Triple entry accounting

Triple entry accounting has been proposed as an enhancement to the traditional double-entry system [8]. The third entry in the system, which is entered into a blockchain, acts as both a receipt and a transaction. It provides irrefutable proof that a transaction happened between two parties, and goes beyond the receipts that each party holds in the double-entry system. Since the entries are distributed and cryptographically sealed, falsifying them or destroying them to conceal activity is practically impossible [9].

The underlying concept in triple-entry accounting is that a transaction between parties goes through a smart contract, and this contract includes details about the transaction such as the product, the price, the seller, and the buyer [10]. It is digitally signed and can include a hash that links to further public documentation of the transaction. So the accounting books of the transacting parties are now linked together by this third entry, i.e., the triple-entry, that can potentially be viewed for external auditing purposes. Triple-entry links two separate double entries. That link is created through a smart contract that works to ensure that the two double entries in separate legal entities are always the same. This is auto enforced by the smart contract, and as with all smart contracts, it is tamper-proof.

Conclusion

Blockchains have the potential to transform accounting and the audit process. With blockchains, companies can create immutable financial records that are verifiable and secure. As described above, each transaction can be audited as the transaction occurs before it is added to the blockchain. Every participant in the network can observe the transaction. The auditor's role in this environment will be to monitor the computer code, protocols, and smart contracts in the blockchain to provide assurance that the information on the distributed ledger is accurate and trustworthy. The preparation of future accounting professionals may thus involve enhancing the traditional Accounting Information Systems courses to teach coding in languages such as Solidity and Golang. This need for upskilling comes at an important inflection point for the profession and can free up the valuable time of accounting professionals to focus more on analytical problem solving by eliminating inefficiencies and human errors in bookkeeping. It will enable accounting firms to significantly expand their client base and serve them better by complementing the efficiency and integrity of computer algorithms with the knowledge and insights of human accountants. With some states exploring blockchain technology for state record keeping (New York Bill No. A08793) and others creating blockchain-based limited liability companies (Vermont, Act 205 (S.269)) whose material operations and ownership interests are entirely managed on a blockchain, the time is right for universities as well as CPA firms working in government and forensic accounting, auditing, and advisory services to consider the promising new horizon of blockchains.

References

- [1] “Distributed ledger technology: beyond block chain,” *GOV.UK*. <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain> (accessed Mar. 04, 2020).
- [2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.
- [3] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, Jan. 1991, doi: 10.1007/BF00196791.
- [4] D. Bayer, S. Haber, and W. S. Stornetta, “Improving the Efficiency and Reliability of Digital Time-Stamping,” in *Sequences II*, New York, NY, 1993, pp. 329–334, doi: 10.1007/978-1-4613-9323-8_24.
- [5] V. Buterin, “Ethereum,” *ethereum.org*. <https://ethereum.org> (accessed Mar. 06, 2020).
- [6] “Hyperledger – Open Source Blockchain Technologies,” *Hyperledger*. <https://www.hyperledger.org/> (accessed Mar. 06, 2020).
- [7] N. Szabo, “A Formal Language for Analyzing Contracts,” *archive.is*, 2002. <http://archive.is/QfvwL> (accessed May 28, 2020).
- [8] I. Grigg, “Triple Entry Accounting,” 2005. https://iang.org/papers/triple_entry.html (accessed May 27, 2020).
- [9] J. Colchester, “Triple-Entry Accounting,” *Systems Innovation*, Mar. 21, 2018. <https://systemsinnovation.io/triple-entry-accounting-articles/> (accessed May 28, 2020).
- [10] F. D. O. Simoyama, I. Grigg, R. L. P. Bueno, and L. C. D. Oliveira, “Triple entry ledgers with blockchain for auditing,” *Int. J. Audit. Technol.*, vol. 3, no. 3, pp. 163–183, Jan. 2017, doi: 10.1504/IJAUDIT.2017.086741.