Blockchain Versus Financial Statement Fraud

Lead Author: Randal Wolverton, CPA/CFF, CFE
Contributing Author: Johnny Lee, JD
Notice to readers

This publication is designed to provide illustrative information about the subject matter covered. It does not establish standards or preferred practices. The material was prepared by Association of International Certified Professional Accountants (Association) staff and volunteers and has not been considered or acted upon by AICPA senior technical committees or the Association board of directors and does not represent an official opinion or position of the Association. It is provided with the understanding that the Association staff and the publisher are not engaged in rendering any legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The Association staff and this publisher make no representations, warranties, or guarantees about, and assume no responsibility for, the content or application of the materials contained herein and expressly disclaim all liability for any damages arising out of the use of, reference to, or reliance on such material.

Acknowledgments

Randal Wolverton, CPA/CFF, CFE, is the lead author of Blockchain Versus Financial Statement Fraud. Johnny Lee, JD is a contributing author.

In addition, members of the Forensic and Litigation Services Committee, and Forensic and Valuation Services Executive Committee also provided review to the authors and Association staff for this white paper.

Staff

Barbara Andrews
Director, Forensic, Technology, Management Consulting Services
FVS Section

Christine N. Cutti-Fox
Senior Manager, Forensic Services
FVS Section

Disclaimer: The contents of this publication do not necessarily reflect the position or opinion of the American Institute of CPAs, its divisions and its committees. This publication is designed to provide accurate and authoritative information on the subject covered. It is distributed with the understanding that the authors are not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

For more information about the procedure for requesting permission to make copies of any part of this work, please email copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707-8110.
# Contents

2 Executive Summary

3 Can Blockchain Technology Become a Factor in the Fight Against Financial Statement Fraud?

4 A Review of Blockchain Technology
   - Public Blockchain
   - Private Blockchain
   - Smart Contracts

6 When Is Blockchain Needed?

7 To Blockchain or Not to Blockchain

8 The Paperwork Problem

9 Historic Financial Statement Fraud Cases
   - Enron Financial Fraud
   - HealthSouth Financial Fraud
   - WorldCom Financial Fraud

11 Modern Financial Fraud Cases

13 Could Blockchain Technology Have Prevented These Schemes?
   - Employee Corruption Fraud and Blockchain Technology
   - Executive Impersonation Schemes

15 The Changing Roles of CPAs

16 What About the Fraud Risk of Blockchain Technology?

18 Appendix A: Glossary

21 Appendix B: Prominent Fraud Schemes — Details
   - Enron Fraud Schemes
   - HealthSouth Fraud Schemes
   - WorldCom Financial Fraud
Executive Summary

Blockchain can be simply described as a transaction database shared by all participants, or nodes, participating in a distributed system. Each addition to the blockchain ledger must be approved by the participants, and any update to the ledger is dated, time-stamped, made available to each participant, and is irreversible.

Current blockchain technology is successfully used in a wide and growing variety of financial systems to accurately record the transfer of value in the preparation of truthful and reliable financial statements.

Blockchain technology can be an effective fraud deterrent in certain fraud schemes, especially schemes in which the fraudsters are not the participants who review and approve transactions. As such, blockchain may be effective in preventing or exposing fraud schemes, such as corrupt employees embezzling corporate funds or business email compromise (BEC) schemes in which payment instructions are misdirected to the accounts of the fraudsters. Such schemes are responsible for millions of dollars in losses but may not rise to the level of materiality for financial statement reporting purposes.

Major corporate fraud accounting cheating scandals such as Enron, WorldCom, and HealthSouth present different fraud challenges. Corrupt senior executives are positioned to formulate and manipulate internal control procedures, internal and external auditing procedures, and financial statement reporting. It remains to be seen if blockchain technology can be developed to prevent or disrupt executive-level fraud schemes.

Blockchain, like any other financial control system, can accurately document transactions but cannot measure the integrity of the transactions. Similar to any financial reporting system, blockchain remains vulnerable to collusion between corrupt persons.

The accounting profession will see increased opportunities for understanding and explaining blockchain technology, implementing blockchain to enhance accountability and auditability of financial reporting, and discussing lead risk analysis associated with a shared ledger system.

Blockchain technology is here to stay and will grow in importance in the future. CPAs will need to learn, adjust, and adapt to emerging uses of blockchain.
Can Blockchain Technology Become a Factor in the Fight Against Financial Statement Fraud?

The brash young CFO had a big problem. He arrived at work every day to occupy his desk in the executive suites of an amazingly successful American corporation. In the year 2000, the company’s annual revenue hit $100 billion, and the company ranked as the seventh-largest on the Fortune 500 and the sixth-largest energy company in the world. But the numbers were fake, and he knew it. He formed partnerships, known as special purpose entities (SPEs) to manipulate financial results. The complex transactions created the appearance of profitable trading but were used to hide the massive company debt, generate false revenues, and enrich the company insiders. He explained to the company’s board of directors, internal and external auditors, and regulators that he was in the gray area of accounting rules and was technically correct in his positions.

Outward appearances indicated that the company was growing, extremely profitable, and meeting all analyst projections. In reality, the company was engaged in a massive accounting fraud by manufacturing and manipulating reported earnings through the improper use of reserves, concealing massive losses by fraudulently manipulating the company’s business segment reporting, manufacturing earnings from the earnings of the company’s rising stock price, and committing additional insider trading transgressions.

The collapse of the company began in 2001 when the CEO and previous CFO departed. The company reported a loss of $618 million, its first quarterly loss in four years. Later the same year, the company’s stock was down to less than $1.00 per share, and investors had lost billions of dollars. After filing for bankruptcy, about 5,600 employees lost their jobs.

This is the true story of the fall of Enron and how the “smartest guys in the room” charted a course toward massive accounting fraud. The SEC charged that Enron executives engaged in a scheme to deceive the investing public between 1999 and 2001. The scheme was designed to make it appear that Enron was growing at a healthy and predictable rate consistent with analysts’ published expectations; did not have significant write-offs and was worthy of an investment-grade credit rating; comprised many successful business units; and had an appropriate cash flow. It had the effect of artificially inflating Enron’s stock price from about $30 per share in early 1998 to over $80 per share in 2001 and artificially stemming the decline of the stock during the first three quarters of 2001.

The CFO in the story is Andrew Fastow, and his plea agreement with the U.S. Government explains his actions. Fastow admitted that he and other members of Enron’s senior management conspired in wide-ranging schemes to fraudulently manipulate Enron’s publicly reported financial results. Fastow admitted participating in schemes to enrich himself at the expense of the company and its shareholders. Specifically, Fastow admitted that he conspired with senior management to cause Enron to enter into improper transactions with related entities under Fastow’s control. He also admitted to engaging in self-dealing transactions to enrich himself and others in connection with an SPE he controlled. By engaging in these transactions, Fastow conceded that he violated his duties of loyalty and honesty to Enron’s shareholders.

The collapse of Enron is an example of why the emergence of blockchain technology has transformed current accounting guidelines. Blockchain is the underpinning of Bitcoin and other virtual currencies, but blockchain is now being seen as a way to record the transfer of value in a manner that is both transparent and unimpeachable. A review of the manifold accounting abuses in the Enron case reveals that the failure to accurately record value transfer was the root cause of the misleading financial statements.
A Review of Blockchain Technology

A blockchain is a type of distributed ledger that records all transactions within the network in theoretically unchangeable, digitally recorded data packages (called blocks). Each block contains a batch of records or transactions, including a time stamp and a reference to the previous block, linking the blocks together in a chain. The system relies on cryptographic techniques to secure the recording of both individual transactions and blocks. A blockchain can be shared and accessed by anyone with appropriate permissions, and participants with appropriate permissions exchange value on the blockchain using public keys and private keys.

A transactional system of blockchain allows for the tracking and/or transfer of assets, the recording of payments, and/or the memorialization of interactions among participants who require secure, trusted, and transparent record-keeping in a manner not achievable via traditional database and/or application-development architectures.1

Bitcoin is an example of a "permissionless," or public, blockchain. All participants share a unified view of the Bitcoin blockchain, which is updated when Bitcoin network participants reach a consensus on the validity of a block of transactions under review (as well as all previously validated blocks).

In the Bitcoin blockchain, mining is the process by which a “block” of transactions is verified and added to a chain of previously verified transaction blocks. This verification process consists of solving cryptographic problems using computing hardware, and miners are the individuals directing the computers to solve these cryptographic problems.2

The architecture of a blockchain can be any of the following:

- Public (fully decentralized)
- Permissioned (partially decentralized)
- Private (centralized)3

Public Blockchain

A public blockchain is referred to as a permissionless system, indicating that a central administrator is not required.4 The data on a public blockchain are accessible via nodes by any user who wants to take part in the network. Examples of a public blockchain would be Bitcoin, Ethereum, and Augur.5 A public blockchain, such as the one supporting Bitcoin, operates as follows:

1. A transaction between network participants is made.
2. Miners in the network work to solve algorithms to verify the transaction.
3. Miners reach consensus on the validity of the transaction, thereby adding it to the blockchain.
4. Each node in the network has access to the verified and immutable distributed ledger.6

---

1 Blockchain — Beyond Cryptocurrency, 2018 Forensic & Valuation Services Conference, presented by Johnny Lee; Principal & National Practice Leader, Forensic Technology Services, Grant Thornton LLP.
2 See footnote 1.
3 See footnote 1.
4 See footnote 1.
5 See footnote 1.
Private Blockchain
Permissioned or private blockchains require servers to be configured in a manner consistent with the consensus model of the blockchain in question. The administration of the records is available to any entity or group permitted to participate via the agreement (or “consensus”) among them. The incentive structure unique to each consensus model provides rewards and punishments designed to maintain the accuracy of the system. Examples of private blockchains include Hyperledger, MultiChain, and Corda.7

Smart Contracts
Blockchain technology also can facilitate the administration of smart contracts. These digital contracts are essentially software code that executes the terms of a contract automatically when certain triggering conditions are met.8

By hard-coding the contract terms and defining triggering events, licensees to a contract agree to termination clauses and other conditions. In terms of financial statement transparency, this is an absolute control with predictable and quantifiable terms.

---

7 See footnote 1 and appendix A, “Glossary.”
8 See footnote 6.
Blockchain technology is gaining traction in different business and government applications in the United States and around the world. For example, Dubai is becoming a leading center for business in the Middle East by transforming to an economy that relies heavily on blockchain technology. Many other examples can be found by reviewing information about IBM blockchain networks.

Blockchain technology is being developed for use in the rapidly changing world of the Internet of Things (IoT). Blockchain is using the identity of devices in large distributed networks of information-gathering technology to secure communications, the exchange of sensitive personally identifiable information, and health care records.

A closer look at where blockchain is successful might provide insight into whether blockchain is even needed. Generally speaking, blockchain can be useful when assets are being moved between entities, and a shared ledger is desired. Blockchain technology is more effective when multiple entities share and update data requiring verification. On a blockchain, time-sensitive and interacting complex transactions can be recorded and cannot be altered. This creates a clear, agreed-upon, auditable record of transactions. Any changes to the initial entries are reflected in subsequent blocks in the blockchain.

Business and government entities who consider the adoption of blockchain technology will be forced to consider the sharing of private sensitive data with other participants, who may also be competitors, in a permissioned system. One significant question is whether participants in a blockchain system will, through shared interests and goals, still protect the privacy of their own entity. An example of a successful resolution to this problem is found in a Reserve Bank of India case. Separate exchanges needed a way to share sensitive data between themselves to allow the exchanges a way to validate transactions without sharing valuable customer lists or violating their customer’s privacy. A solution involved storing data on the blockchain in a way that allowed for verification without revealing any part of the underlying data.

The solution is further described by Mr. Kalyan Basu, Managing Director & CEO, A. Treds Ltd. as follows:

Our clients are particularly sensitive about their sourcing inputs, and we absolutely could not broadcast any of their private information to a shared network. This technology, however, enables us to work together with the other exchanges to achieve shared goals without sharing specific data. I look forward to the day when other players in the financial services industry also appreciate the value added in terms of preventing frauds related to Bill Discounting and become part of this system.

---

10 See the IBM Blockchain, accessed February 20, 2019.
11 See footnote 1.
12 See footnote 1.
13 See footnote 1.
To Blockchain or Not to Blockchain

A blockchain database overcomes two limitations found with traditional database architectures: trust and extreme resiliency. The overarching litmus test is can this be done using a database other than blockchain? Decision-makers will weigh traditional databases offering greater speed, performance, and privacy against slower performance, reduced privacy, and increased resiliency associated with blockchain.13

13 See footnote 1.
The Paperwork Problem

Those involved, including banks, financiers, shipping companies, and governments, come with a myriad of competing interests. These participants have little trust in each other and are actively trying to identify “cheaters.” To get everyone on board with a common solution, they need a system that is decentralized (not controlled by any one network participant), immutable (trustworthy as a system of record), and independently verifiable (transparent to any network participant).14

HSBC Bank and the Maersk shipping company both believe that a consortium blockchain may be the way to bridge the competing agendas into a unified and trusted system. Together, they have developed a blockchain-based, smart-contract system designed to reduce the friction associated with paper records. HSBC has $2 trillion in trade that currently depends on the physical exchange of letters of credit. The Maersk and IBM platforms enable importers and exporters, customs brokers, and trusted third parties (for example, government agencies and non-governmental organizations) to securely exchange information using an open, secure system with an immutable audit trail.15

Though some cases are compelling because they address the core attributes of blockchain — namely, trust and resiliency — the vast majority are not because they seek to use blockchain technologies for things for which it is not well suited. Additionally, blockchain technology still suffers from a certain stigma, borne largely of residual associations with criminal activities (like Silk Road) as well as the volatility of Bitcoin. Additionally, the adoption of blockchain also requires a shift of trust from known institutions to software.17

“HSBC Bank and the Maersk shipping company both believe that a consortium blockchain may be the way to bridge the competing agendas into a unified and trusted system.”

---

14 See footnote 1.
15 See footnote 1.
17 See footnote 1.
Is it possible that frauds like Enron might have been prevented or discovered earlier had blockchain systems been implemented at the time? In particular, could smart contracts have prevented the corruption of the general ledger and subsequent financial statements? To answer these questions and test the theory about blockchain’s utility as a fraud-prevention mechanism, it is necessary to review the accounting fraud issues identified by the SEC in the Enron, HealthSouth, and WorldCom financial statement fraud cases.

Enron Financial Fraud
The SEC identified the following issues (among others) at Enron:

- Used reserves within Enron’s wholesale energy trading business, Enron Wholesale, to manufacture and manipulate reported earnings
- Manipulated Enron’s business segment reporting to conceal losses at Enron’s energy business, Enron Energy Services
- Manufactured earnings by fraudulently promoting Enron’s broadband unit, Enron Broadband Services (EBS)
- Improperly used special purpose entities and the LJM Partnerships to manipulate Enron’s financial results
- Insider trading by company executives
- Improperly used special purpose entities and the LJM Partnerships to manipulate Enron’s financial results
- False and misleading statements by company executives

HealthSouth Financial Fraud
The HealthSouth company, with headquarters in Birmingham, Alabama, was formed in 1984. At the time, HealthSouth was the nation’s largest provider of outpatient surgery, diagnostic, and rehabilitative health care services. It owned or operated over 1,800 different facilities throughout the United States and abroad, including inpatient and outpatient rehabilitation facilities, outpatient surgery centers, diagnostic centers, medical centers, and other health care facilities. For the year-end 2001, the company reported total revenues of $4 billion and net income of $76 million. The company’s stock was listed on the New York Stock Exchange.

Shortly after HealthSouth became publicly traded in 1986, the company began to artificially inflate its earnings to match Wall Street analysts’ expectations and maintain market price for its stock. Between 1999 and the second quarter of 2002, the company intentionally overstated its earnings, identified as income before income taxes and minority interests, by at least $1.4 billion.

The SEC identified the following accounting fraud issues at HealthSouth:

- Recording false earnings
- Recording false fixed assets
- Deceiving outside auditors

WorldCom Financial Fraud
WorldCom, a company based in Clinton, Mississippi and incorporated in Georgia, provided a broad range of communications services to businesses and consumers in more than 65 countries. WorldCom provided data transmission services to businesses and, through its MCI Inc. unit, provided telecommunications services for businesses and consumers. WorldCom was a public company whose stock was listed on the NASDAQ national market system. Its stock was covered by Wall Street analysts who routinely issued quarterly and annual earnings estimates.

See appendix B “Prominent Fraud Schemes — Details.”


See footnote 11.
In March 2004, former CEO and President Bernard J. Ebbers and former CFO Scott D. Sullivan were charged by the United States Attorney’s Office, Southern District of New York with conspiracy and securities fraud covering the time period of September 2000 through June 2002. A scheme to defraud was charged for artificially inflating the price of WorldCom common stock by hiding the truth from investors about WorldCom's declining operating performance and financial results. Rather than reporting WorldCom's true financial condition, which likely would have resulted in a decline in the price of WorldCom's stock, the CEO and CFO insisted that WorldCom publicly report financial results that met analysts' expectations. To accomplish this goal, the CEO and CFO agreed that false and fraudulent adjustments would be made to WorldCom's books and records. The CEO and CFO artificially manipulated reported revenue; selling, general, and administrative (SG&A) expenses; line cost expenses; earnings before income, depreciation, taxes, and amortization (EBITDA); depreciation expenses; net income; and earnings per share (EPS).

The WorldCom collapse cost 30,000 employees their jobs and cost investors $180 billion. In 2005, CEO Bernard Ebbers was found guilty of all charges and was convicted of fraud, conspiracy, and filing false documents with regulators, and was sentenced to 25 years in prison.

The SEC identified the following accounting fraud issues at WorldCom:

• Certain manipulation of financial results
• Improper accounting entries for line costs

This review of SEC findings in the Enron, WorldCom, and HealthSouth cases illustrates that corrupt executives colluded to falsely manipulate corporate earnings to conceal the actual financial position of the companies. Enron executives falsely used SPEs to hide debt and inflate earnings. WorldCom was falsely portrayed as a profitable business by concealing large losses. HealthSouth executives manipulated earnings by falsely reporting nonexistent fixed assets, cash, and reducing expenses.

Enron, WorldCom, and a host of other major accounting fraud cases spurred the passage of the Sarbanes-Oxley Act of 2002, or SOX, to protect investors from fraudulent financial reporting by corporations. It mandated strict reforms to existing securities regulations and imposed tough new penalties on lawbreakers. HealthSouth executives were held responsible for presenting fraudulent financial statements in part because they were required to personally sign the financial statements. The corrupt executives in each of these cases overcame accounting controls and audit procedures designed to produce accurate financial reporting. The executives could then control both sides of the transactions to claim inflated profits or to hide debt from the financial statements. The complex schemes lasted several years before discovery.
Modern Financial Fraud Cases

The Enron, HealthSouth, and WorldCom cases clearly illustrate accounting fraud and abuse issues in the 1990s and 2000s, making it fair to ask if these accounting abuses remain relevant today. The following cases identified by the SEC will show that similar accounting fraud cases continue to plague large, medium, and small companies. As the following examples show, most corporate entities are not formed with the intention of committing fraud in their financial statements; however, certain business events can form pressures and opportunities to commit accounting fraud that compromises the original entry and general ledger.

• The SEC announced in March 2017 that the Mexico-based homebuilding company Desarrolladora Homex S.A.B. de C.V. agreed to settle charges that it reported fake sales of more than 100,000 homes to boost revenues in its financial statements during a three-year period.

The SEC alleges that Homex inflated the number of homes sold during the three-year time period by about 317% and overstated its revenue by 355% (about $3.3 billion). The following statement was made by Stephanie Avakian, Acting Director of the SEC’s Enforcement Division regarding Homex:

Homex deprived its investors of accurate and reliable financial results by reporting key numbers that were almost completely made up. The settlement takes into account that the fraud occurred entirely under the watch of prior ownership and management, the company’s new leaders provided critical information regarding the full scope of the fraudulent conduct, and the company continues to significantly cooperate with our ongoing investigation.25

• Technology manufacturer Logitech International agreed to pay a $7.5 million penalty for fraudulently inflating its fiscal year 2011 financial results to meet earnings guidance and for committing other accounting-related violations during a five-year period. Logitech’s then-controller and then-director of accounting agreed to pay penalties for violations related to Logitech’s warranty accrual accounting and failure to amortize intangibles from an earlier acquisition. The SEC filed a complaint in federal court against Logitech’s then-CFO and then-acting controller alleging that they deliberately minimized the write-down of millions of dollars of excess component parts for a product for which Logitech had excess inventory in fiscal year 2011. For Logitech’s financial statements, the two executives falsely assumed the company would build all the components into finished products despite their knowledge of contrary facts and events.26

• Three then-executives at battery manufacturer Ener1 agreed to pay penalties for the company’s materially overstated revenues and assets for year-end 2010 and overstated assets in the first quarter of 2011. The financial misstatements stemmed from management’s failure to impair investments and receivables related to an electric car manufacturer that was one of its largest customers. The former CEO and chairman of the board, former CFO, and former chief accounting officer agreed to pay penalties of $100,000, $50,000, and $30,000, respectively.

In the Ener1 case, the SEC also found that the engagement partner for PricewaterhouseCoopers LLP’s audit of Ener1’s financial statements violated PCAOB and professional auditing standards when he failed to perform sufficient procedures to support his audit conclusions that Ener1 management had appropriately accounted for its assets and revenues.

Modern Financial Fraud Cases

- The SEC announced in June 2017 that charges were brought against a Canadian-based oil and gas company and three of its former top finance executives for their roles in an extensive, multi-year accounting fraud.

  The SEC’s complaint alleges that Penn West Petroleum Ltd., which has since been renamed Obsidian Energy Ltd., fraudulently moved hundreds of millions of dollars in expenses from operating expense accounts to capital expenditure accounts. This alleged fraudulent movement caused Penn West to artificially reduce its operating costs by as much as 20% in certain periods, which falsely improved reported metrics for oil extraction efficiency and profitability. Penn West was one of Canada’s largest oil producers at the time.

  The SEC alleges that executives manipulated the company’s operating expenses in order to lower a key publicly reported metric concerning the cost of oil extraction and processing needed to sell a barrel of oil. Penn West allegedly created an internal budget target representing the amount it would improperly move in its publicly reported financial statements and gave the illusion that it was spending less money than it actually was to get oil out of the ground. In fact, the company historically struggled to keep its operating costs under control, and the executives managed operating expenses to meet the budget target. The executives frequently met this target to the dollar by having the company record large, round number, and unsupported adjusting journal entries. Within the company, this practice was referred to as ‘reclass to capital.’ The executives directed the reclass-to-capital practices without ensuring that the accounting entries reconciled with actual capital spending amounts and were repeatedly warned by a subordinate accountant that the reclass entries lacked support.

  The reviews of the Desarrolladora Homes, Logitech, and Penn West Petroleum cases also illustrate that corrupt executives continue to manipulate financial statements to the detriment of employees and investors despite stricter government mandates and enhanced audit practices.

  In modern financial fraud cases, we see that the person or persons who decide to engage in fraud will usually start small, test the system, and if left undiscovered, will continue the fraud, just as they did in the Enron, HealthSouth, and WorldCom cases. Corrupt executives seem to believe that they must understand and defeat the auditors and regulators who are trying to guard against such activity. Accountants currently encounter revenue recognition problems, false embellishment of assets, false decreases of liabilities, false increase of revenues, and false decrease of expenses, all designed to present misleading financial statements. In bankruptcy fraud matters, we may see the opposite: Fraudsters drain the entity of assets and deploy false and misleading accounting tricks designed to understate the true financial condition of the company and to defraud creditors and the bankruptcy system.

---

Could Blockchain Technology Have Prevented These Schemes?

Enron, HealthSouth, WorldCom, and the more recent cases discussed illustrate that accounting fraud cases incorporate different schemes to manipulate earnings. Schemes such as hiding debt, inflating earnings, decreasing expenses, increasing fixed assets, and withholding reserves for later use to offset negative information require the participation of multiple individuals to complete the fraud. However, blockchain technology would have necessitated multiple participants approving transactions before new blocks could be added. The independence of the participating nodes may well be a key to enhancing the potential for blockchain to identify or prevent fraud.

Current blockchain technology offers some promise in preventing or exposing fraud schemes, such as employee corruption or BEC, in which perpetrators have no access to the blockchain approval process.

Employee Corruption Fraud and Blockchain Technology

The experience of forensic accountants persuades us that the fraud mindset embodied by corrupt individuals will likely be the strongest opponent in the fight to prevent fraud. Forensic accountants believe that for fraud to occur, three factors generally need to be present: opportunity, rationalization, and pressure. In asset misappropriations, pressure tends to be individualized, and in financial statement misrepresentations, pressure tends to be more organizational.28

Corporate fraud is apparent at all levels, including among supervisors, management, and even executives. The problem for forensic accountants is that if a person is corrupt, he or she will always have the ability to rationalize theft. Some of the most troubling projects that an investigator pursues can involve employee theft through such violations as expense report abuse, improper vendor relationships, and low-dollar bribes.

Imagine a manufacturing engineer who awards million-dollar contracts for factory maintenance, who then has a barn built at his or her personal residence for free or at a very low cost, using his or her employer’s resources or discounts from vendors. Corrupt activities might be committed acts, such as defalcation of records or misrepresentation of work performed, or omitted acts, such as looking the other way or failing to enforce policies or regulations in exchange for something of value.

The following are some examples of employee corruption schemes:

- Payroll and ghost employees
- Billing and fictitious vendors
- Expense reimbursement
- Bid rigging
- Kickbacks
- Bribery

It is reasonable to ask if blockchain technology will prove a potent adversary against the collaboration of corrupt corporate executives who choose to produce fraudulent financial statements. It could be argued that collusion among top executives could result in the manipulation of a closed permissioned blockchain system by stacking the participants, or nodes, to their favor. The Enron case is particularly haunting because the fraud was perpetrated and concealed by corrupt executives who profited from the schemes. They had every incentive to continue the fraud. Incentive to continue the fraud may be true particularly if executives participated in designing and administering the blockchain system. Ultimately, though, corrupt executives would not have a shared interest to collaborate with other participants in a blockchain environment to expose their own fraud.

---

Could Blockchain Technology Have Prevented These Schemes?

**Executive Impersonation Schemes**

Business Email Compromise (BEC) schemes, also known as executive impersonation schemes, are accomplished by a criminal creating a fake email that closely resembles the victim company’s own email and appears to come from a high-ranking executive. The recipient is an unsuspecting mid- or lower-level employee selected for his or her access and authority to transfer large sums of money between subsidiaries or to suppliers on behalf of the company.

BEC scams usually begin in one of two ways: either by getting an unsuspecting employee to click on an email attachment that compromises the network (malware) or by sending an email impersonating a high-ranking company official. Sophisticated hackers usually research their target and the company to craft highly convincing emails. Using information gleaned from mining corporate websites and social networks, the impersonations used in BEC emails can be extremely accurate and convincing. Because the email appears to come from a known and trusted source, the request to release valuable data or take urgent action appears to be more plausible.29

So, the same questions can be asked about emerging blockchain technology. Could closed, permissioned blockchain systems help to discover or prevent corrupt employee schemes, BEC schemes, and hosts of other schemes to defraud businesses? Answers may lie in the design of the businesses and the nature of the attacks. A blockchain system may make it more difficult for corrupt employees to create fictitious invoices in a fake vendor scheme or bribery and kickback scheme. It is also possible that theft of corporate funds in a BEC scheme could be prevented by having multiple participants with a shared interest in preventing fraud focus on changes in payment instructions. This could lead to identifying suspicious activity before payments are sent, thereby avoiding costly losses and litigation.

The massive accounting fraud cases discussed show that corrupt executives colluding with one another have overcome accounting controls designed to produce reliable financial statements. Blockchain technology offers new ways of addressing these complex problems. A key factor may be in using independent participants chosen to evaluate additions to the blockchain based on adherence to generally accepted accounting principles and fundamental integrity. The participants would be in a position to identify and prevent the introduction of fraudulent manipulations to the accounting system. There may be little doubt that determined, fraud-motivated persons would work to overcome any advantages presented by a shared ledger. However, a well-designed blockchain system using persons dedicated to accurate financial reporting would be in a better position to identify and address red flags at early stages of activity. A combination of trained and independent participants in the blockchain system with trained and independent auditors could dissuade corrupt executives from manipulating earnings. This combination of independent participants and auditors would also increase the chances of detecting and preventing corrupt employees from hatching damaging theft schemes or hackers from infiltrating the cyber system to change payment instructions.

---

The Changing Roles of CPAs

Should CPAs be worried that emerging blockchain applications will render them outdated in the future? No, because the opposite is actually occurring. The accounting profession is currently being presented with opportunities to establish a leadership role in formulating new procedures in auditing, accounting rules, financial statement procedures, and tax treatments of events, as well as in educating the public about blockchain developments.

Many professionals engaged in blockchain developments estimate that blockchain technology is still 5–10 years away from full implementation. However, it is very apparent that blockchain is currently being absorbed into business and government environments at a rapid pace, and the accounting world will need to adapt to the emerging developments. To be sure, fraud-motivated persons are also studying blockchain technology and will adapt accordingly. The accounting industry must also adapt, only better.
What About the Fraud Risk of Blockchain Technology?

As discussed, blockchain technology may provide more tools to guard against known forms of traditional fraud, for instance, revenue recognition fraud, financial statement manipulation, embezzlement by corrupt employees, vendor fraud, and BEC scams. However, the emergence of a new breed of cybercriminal will present new challenges to the world of blockchain. By understanding the strengths and weaknesses of blockchain, CPAs will be in a better position to provide input about how to improve the application of the new technology, including the design and implementation of internal controls specific to the blockchain environment.

CPAs are in a unique position to provide unbiased advice about the benefits and potential drawbacks to those considering implementing a blockchain system. Questions for consideration could include the following:

- Could a synthetically created false identity impersonate a node or participant in a closed blockchain system?
- Could criminals or terrorists create synthetic identities to be incorporated into blockchain systems?
- Could corrupt executives, such as in the Enron case, collude with each other to inject fraud into the blockchain system?
- What about zero-day vulnerabilities (security flaws that are unknown to users and developers)?
- What about intelligence spills? Dealing with governmental entities may expose the blockchain system to various levels of classifications. An intelligence spill could occur if classified information is inadvertently or intentionally placed into unclassified information.
- How do blockchain developers protect intellectual property?
- How are private keys protected from theft?
- In the event of disputes or inquiries, who owns the blockchain?
- Can smart contracts be corrupted and used in cybercrimes to cause financial harm in a binding contract?
- Could blockchain technology be used to promote money laundering?

Despite the promise blockchain technology may hold, it is important to remember that, ultimately, transactions are initiated by human beings. Therefore, we should continue to question whether it is possible for two or more nodes (or participants) to dishonestly collude to introduce fraudulent transactions into the blockchain, whether corrupt executives can game the system and create false or misleading financial statements, and whether the identities of nodes can be compromised in order to promote fraudulent transactions.

Another issue to be explored: Because corrupt individuals naturally have no shared interest in participating in a blockchain environment, or any other environment that would expose fraud, could the U.S. government impose requirements to develop and implement a permissioned blockchain system to prevent fraud in massive government-sponsored programs? Examples would be vast sums of taxpayer dollars expended for Medicare and Medicaid, government procurement programs, disaster relief programs, or treatment for U.S. veterans.
Can blockchain eradicate fraud? The answer is no. There is no accounting system, blockchain or otherwise, that guarantees the elimination of fraud. Present-day blockchain applications may be more effective in smaller, more focused environments where the participants have a mutual shared interest in preventing fraud. Examples would be the prevention of embezzlement schemes, corrupt vendor fraud, and BEC schemes. It is not likely, at this point in time, that blockchain is developed enough to prevent major corporate accounting fraud matters in which corrupt executives will produce false and misleading financial statements. However, blockchain may serve to move many known fraud schemes closer to eventual discovery to counteract determined criminals who find and exploit weaknesses in any system to their corrupt advantage.
## Appendix A: Glossary

<table>
<thead>
<tr>
<th>Word</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Augur                               | Augur is a decentralized oracle and peer-to-peer protocol for prediction markets. Augur is free, public, open-source software, portions of which are licensed under the General Public license and portions of which are licensed under the Massachusetts Institute of Technology license. Augur is a set of smart contracts written in solidity that can be deployed to the Ethereum blockchain.  
  See [https://www.augur.net/faq/](https://www.augur.net/faq/), accessed December 17, 2019. |
| Bid-rigging schemes                 | Bid rigging occurs when participants work together to make it appear as though several competitive bids have been received, when, in fact, the process is rigged to favor a higher-than-necessary price.                                                                                                                                                                                                                                           |
| Billing and fictitious vendor schemes | This fraud scheme is perpetrated by issuing disbursement to either a fictitious vendor or to a legitimate vendor for fictitious goods or services. The fictitious vendor is entered into the vendor master file and receives payment for goods and services not actually provided. Legitimate vendor accounts might also be used to commit fraud. Payments to legitimate vendors for fictitious goods or services may be intercepted and converted. Employees can also collude with existing vendors to create inflated invoices or false invoices and in exchange for kickbacks or bribes to the employee. |
| Bitcoin                             | The SEC defines Bitcoin as a decentralized, peer-to-peer virtual currency that is used like money. It can be exchanged for traditional currencies such as the U.S. dollar or used to purchase goods or services, usually online. Unlike traditional currencies, Bitcoin operates without central authority or banks and is not backed by any government.  
| Bribery schemes                     | This type of scheme involves the corrupt payment of money, gifts, or other rewards to influence the action of another person. The U.S. Foreign Corrupt Practices Act prohibits corrupt payments to foreign officials and requires that books and records be maintained in a manner to assure that such corrupt payments are not made.                                                                                                                                                                                    |
| Corda                               | An open-source blockchain platform built for business. Corda enables businesses to transact directly and in strict privacy using smart contracts.  
<table>
<thead>
<tr>
<th>Word</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ethereum</strong></td>
<td>Ethereum is a decentralized blockchain platform founded in 2014 by Vitalik Buterin. Like Bitcoin, Ethereum is an open-source project that is not owned or operated by a single individual, meaning that anyone, anywhere can download the software and begin interacting with the network. Ethereum uses a “virtual machine,” which is like a giant, global computer made up of many individual computers running the Ethereum software. The virtual currency unit that allows this system to work is called ether. People interact with the Ethereum network by using ether to pay the network to execute smart contracts.³³</td>
</tr>
<tr>
<td><strong>Expense reimbursement schemes</strong></td>
<td>These schemes include submitting personal expenses as business expenses, writing in overstated amounts on a receipt, duplicating reimbursement, and masking the true nature of an expense to one that is allowed by company policy.</td>
</tr>
<tr>
<td><strong>Hyperledger</strong></td>
<td>Hyperledger is hosted by the Linux Foundation. Innovators in finance, banking, health care, the Internet of Things, supply chain, manufacturing, and technology are creating open, standardized, and enterprise-grade distributed ledger blockchain frameworks and code bases to produce tangible business results.³⁴</td>
</tr>
<tr>
<td><strong>Kickback schemes</strong></td>
<td>Kickbacks can be in the form of goods, services, or cash. For example, a hiring manager negotiates with a potential recruit and offers the recruit a high-paying position, as long as 5% of the new salary is secretly given back to the hiring manager.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Word</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Miners                                  | Bitcoin mining is the process through which Bitcoins are released into circulation. Basically, it involves solving a computationally difficult puzzle to discover a new block, which is added to the blockchain, and receiving a reward in the form of a few bitcoins. The block reward was 50 new bitcoins in 2009, and it decreases every four years. As more and more bitcoins are created, the difficulty of the mining process, that is, the amount of computing power involved, increases. The mining difficulty began at 1.0 with Bitcoin's debut in 2009. At the end of the year, it was only 1.18. As of February, the mining difficulty is over 6.06 billion. Once, the ordinary desktop computer sufficed for the mining process. Now, to combat the difficulty level, miners must use faster hardware like Application-Specific Integrated Circuits (ASIC), more advanced processing units like Graphic Processing Units (GPUs), and so on.  
| MultiChain                              | MultiChain technology is a platform that helps users to establish certain private blockchains that can be used by organizations for financial transactions.  
| Payroll and ghost employees schemes     | Ghost employees are individuals who receive paychecks but do not exist or exist but are not legitimate employees.                                                                                           |
| Private key                             | A private key is a string of letters and numbers that can be used to spend bitcoins associated with a specific bitcoin address.  
| Public key                              | A public key is a string of letters and numbers that is derived from a private key. A public key allows one to receive bitcoins.  
38 See footnote 36 |
| Synthetic identify theft                | A synthetic identity is created by using a combination of real information (such as a legitimate Social Security number) with fictional information (which can include a made-up name, address, or date of birth).  
The following information from the SEC provides a more detailed description of the fraudulent conduct discovered in the investigations involving Enron, HealthSouth, and WorldCom cases.

Enron Fraud Schemes:

(A) Used Reserves Within Enron’s Wholesale Energy Trading Business, Enron Wholesale, to Manufacture and Manipulate Reported Earnings.

1. SEC: “From the third quarter of 2000 through the third quarter of 2001, Skilling and others fraudulently used reserve accounts within Enron Wholesale to mask the extent and volatility of its windfall trading profits, particularly its profits from the California energy markets; avoid reporting large losses in other areas of its business; and preserve the earnings for use in later quarters. By early 2001, Enron Wholesale’s undisclosed reserve accounts contained over $1 billion in earnings. Skilling and others improperly used hundreds of millions of dollars of these reserves to ensure that analysts’ expectations were met. In addition, Skilling and others improperly used the reserves to conceal hundreds of millions of dollars in losses within Enron’s EES business unit from the investing public.

Further, Skilling and others approved the improper release of reserves in certain quarters prior to 2001, in order for Enron to make or exceed analysts’ earnings estimates. For example, in mid-July 2000, well after the end of the second quarter, Skilling and others decided to beat Wall Street analysts’ quarterly earnings expectations by two cents a share and publicly report an earnings-per-share figure of 34 cents. They did this despite knowing that Enron’s performance for the quarter did not support the 34-cent earnings-per-share figure. In order to achieve this goal, they caused a senior Enron executive to release improperly millions of dollars of “prudency” reserves from Enron’s energy trading business into earnings.”


1. SEC: “Skilling and others concealed massive losses in EES by fraudulently manipulating Enron’s “business segment reporting.” At the close of the first quarter of 2001, Skilling and others approved moving a large portion of EES’s business into Enron Wholesale under the guise of reorganizing Enron’s business segments. Skilling and others knew that the reorganization was designed to fraudulently conceal hundreds of millions of dollars in losses at EES, Enron’s heavily touted retail energy trading business, losses which Enron otherwise would have had to report. Enron moved the losing portion of EES’s business into Enron Wholesale because Enron Wholesale had ample earnings, including the massive reserve accounts described above, to absorb EES’s huge losses while continuing to meet Enron’s budget targets.

(C) Manufactured Earnings by Fraudulently Promoting Enron’s Broadband Unit, Enron Broadband Services (EBS).

Appendix B: Prominent Fraud Schemes — Details


41 See footnote 29.
1. SEC: “Skilling and others fraudulently promoted EBS at Enron’s January 20, 2000, corporate analyst conference and manufactured earnings from the resulting increase in Enron’s stock price. At the analyst conference, Skilling and others knowingly made false and misleading statements about the status of EBS’s broadband network, EBS’s proprietary "network control software," and the "conservative" value — $30 billion — of EBS’s business. In reality, EBS had neither the broadband network that Skilling claimed, nor the critical proprietary network control software to run it. In addition, Skilling inflated the value of EBS by billions of dollars over what both internal and external valuations had advised.

2. Knowing about the planned EBS presentation, Skilling and others — prior to the analyst conference — constructed and approved a scheme that allowed Enron to recognize approximately $85 million in earnings from the increase in the value of its stock. The earnings were recorded through a partnership interest Enron held in a large energy investment named JEDI that held, as one of its investment holdings, Enron stock. In connection with the January 20, 2000 analyst conference, Enron and JEDI purportedly executed a series of transactions, known as "Project Greyhawk," that allowed JEDI's income to increase as the price of Enron's stock increased. Project Greyhawk allowed Enron to recognize, through its partnership interest in JEDI, approximately $85 million in earnings as a result of the manufactured increase in Enron stock from the false and misleading presentation at the analyst conference." 42

(D) Improperly Used Special Purpose Entities and the LJM Partnerships to Manipulate Enron’s Financial Results.

1. SEC: "Enron entered into fraudulent transactions with LJM Cayman, L.P. and LJM2 Co-Investment, L.P. (collectively "LJM"), two unconsolidated partnerships created and managed by Andrew Fastow, Enron’s then-Chief Financial Officer, when Skilling and others knew that LJM was not a legitimate third party acting independently from Enron. Enron used transactions with LJM to manipulate its financial results.

2. For example, Enron and LJM engaged in a series of financial transactions with four SPEs called Raptor I, Raptor II, Raptor III and Raptor IV (collectively referred to as the "Raptors"). Skilling, Causey, Fastow and others used the Raptors to manipulate fraudulently Enron’s reported financial results. They designed Raptor I, among other things, to protect Enron from having to report publicly decreases in value in large portions of its energy “merchant asset portfolio” and technology investments by allowing Enron to "hedge" the value of those investments with an allegedly independent third party, known as Talon. The Raptor I structure, however, was invalid under applicable accounting rules because, among other things, (i) Talon was not independent from Enron and LJM’s investment in Talon was not at risk, and (ii) Causey and Fastow had entered into an oral side agreement that LJM would receive its initial investment in Talon ($30 million) plus a large profit ($11 million) from Enron, all prior to Talon engaging in any of the hedging transactions. As a quid pro quo for this payment,

42 See footnote 29.
Fastow agreed with Causey that Enron employees could use Raptor I to manipulate Enron’s financial statements, including by allowing Enron employees, without negotiation or due diligence by LJM, to select the values at which the Enron assets were hedged with Talon. Skilling was informed of and approved Fastow’s deal with Causey in order to ensure that Enron achieved the financial reporting goals for which Raptor I was designed, even though it was clear that the Raptor I structure was not a true hedging device.

3. In another transaction — the “Cuiaba project” — Skilling and others used LJM to move a poorly performing asset temporarily off Enron’s balance sheet, when in fact such off-balance-sheet treatment was improper. When no true third-party buyer could be found, Skilling and others caused Enron to “sell” a portion of Enron’s interest in the Cuiaba project to LJM for $11.3 million. LJM agreed to “buy” this interest only because Skilling, Causey, Fastow and others, in an undisclosed side deal, agreed that Enron would buy back the interest, if necessary, at a profit to LJM. Based on this purported “sale,” which was, in fact, an asset parking or warehousing arrangement, Enron improperly recognized approximately $65 million in income in the third and fourth quarters of 1999. In the spring of 2001, even though the project was approximately $200 million over budget, Skilling, Causey and Fastow agreed that Enron would buy back LJM’s interest in the Cuiaba project at a considerable profit to LJM. After agreeing to execute the repurchase, Skilling, Causey, Fastow and others delayed consummating the deal until Fastow sold his interest in LJM so that Fastow’s role in the transaction would not have to be publicly disclosed.

4. In the “Nigerian barge” transaction, Skilling and others agreed to a sham “sale” of an interest in certain power-producing barges off the coast of Nigeria to Merrill Lynch so that Enron could meet its fourth-quarter 1999 budget targets. In order to induce Merrill Lynch to enter into the transaction, Enron promised — in an oral and undisclosed “handshake” deal — that Merrill Lynch would receive a return of its investment plus an agreed-upon profit within six months. As a result, Merrill Lynch’s equity investment was not “at risk” and Enron should not have treated the transaction as a sale from which it could record earnings and cash flow. In June 2000, Enron delivered on its “handshake” promise. Causey and Fastow ensured that LJM repurchased the Nigerian barges from Merrill Lynch at the agreed-upon profit.”

(E) Insider Trading

1. SEC: “Skilling profited from the scheme to defraud by selling large amounts of Enron stock at the inflated prices. These trades also occurred while Skilling was in possession of material non-public information, including information about Enron’s actual financial performance and the failure of its business units as described above. From April 2000 to September 2001, Skilling sold over one million shares of Enron stock that generated unlawful proceeds of approximately $63 million.”

43 See footnote 29.
44 See footnote 29.
(F) False and Misleading Statements

1. SEC: “In addition, the Amended Complaint alleges that Skilling made false and misleading statements concerning Enron’s financial results and the performance of its businesses, and that these misrepresentations were also contained in Enron’s public filings with the Commission. The Amended Complaint further alleges that Skilling sold Enron stock while in possession of material, non-public information that generated unlawful proceeds of approximately $63 million.” 45

HealthSouth Fraud Schemes:

(A) Recording False Earnings

1. Pursuant to the scheme, on a quarterly basis, HRC’s senior officers would present Scrushy with an analysis of HRC’s actual, but as yet unreported, earnings for the quarter as compared to Wall Street’s expected earnings for the company. If HRC’s actual results fell short of expectations, Scrushy would tell HRC’s management to “fix it” by recording false earnings on HRC’s accounting records to make up the shortfall. HRC’s senior accounting personnel then convened a meeting to “fix” the earnings shortfall. By 1997, the attendees referred to these meetings as “family meetings” and referred to themselves as “family members.” At these meetings, HRC’s senior accounting personnel discussed what false accounting entries could be made and recorded to inflate reported earnings to match Wall Street analysts’ expectations. These entries primarily consisted of reducing a contra revenue account, called “contractual adjustment,” and/or decreasing expenses, (either of which increased earnings), and correspondingly increasing assets or decreasing liabilities.

(B) Recording False Fixed Assets

1. SEC: “Since 1999, HealthSouth Corp. ("HRC"), one of the nation’s largest healthcare providers, has overstated its earnings by at least $1.4 billion. This massive overstatement occurred because HRC’s founder, Chief Executive Officer and Chairman of the Board, Richard M. Scrushy ("Scrushy"), insisted that HRC meet or exceed earnings expectations established by Wall Street analysts. When HRC’s earnings fell short of such estimates, Scrushy directed HRC’s accounting personnel to “fix it” by artificially inflating the company’s earnings to match Wall Street expectations. To balance HRC’s books, the false increases in earnings were matched by false increases in HRC’s assets. By the third quarter of 2002, HRC’s assets were overstated by at least $800 million, or approximately 10 percent of total assets.” 47

45 See footnote 29.
46 See footnote 20.
47 See footnote 30.
(C) Deceived Outside Auditors

1. SEC: “HRC’s accounting personnel designed the false journal entries to the income statement and balance sheet accounts in a manner calculated to avoid detection by the outside auditors. For example, instead of increasing the revenue account directly, HRC inflated earnings by decreasing the "contractual adjustment" account. Because the amounts booked to this account are estimated, there is a limited paper trail and the individual entries to this account are more difficult to verify than other revenue entries.

2. HRC also created false documents to support its fictitious accounting entries. For example, during the audit of HRC’s 2000 financial statements, the auditors questioned an addition to fixed assets at one particular HRC facility. HRC accounting personnel, knowing that this addition was fictitious, altered an existing invoice (that reflected an actual purchase of an asset at another facility that approximated the dollar amount of the fictitious addition) to fraudulently indicate that the facility in question had actually purchased that asset. This altered invoice was then given to the auditors to support the recording of the fictitious asset in question. Also, when the auditors asked HRC for a fixed assets ledger for various facilities, HRC accounting personnel would re-generate the fixed asset ledger, replacing the "AP Summary" line item with the name of a specific fixed asset that did not exist at the facility, while leaving the dollar amount of the line item unchanged.”

WorldCom Financial Fraud:

(A) Certain Manipulation of Financial Results

1. SEC: “WorldCom reduced its operating expenses by improperly releasing certain reserves held against operating expenses. Second, WorldCom improperly reduced its operating expenses by recharacterizing certain expenses as capital assets.

2. Neither practice was in conformity with generally accepted accounting principles ("GAAP"). Neither practice was disclosed to WorldCom’s investors, despite the fact that both practices constituted changes from WorldCom’s previous accounting practices. Both practices falsely reduced WorldCom’s expenses and, accordingly, had the effect of artificially inflating the income WorldCom reported to the public on its financial statements from 1999 through the first quarter of 2002.”

(B) Improper Accounting Entries for Line Costs

1. SEC: “Line costs” represented the various fees WorldCom paid to third-party telecommunications carriers for WorldCom’s right to access the third-party’s network facilities in order to serve customers. Under GAAP, these fees must be reported as an expense on a company’s income statement.

See footnote 30.

2. From at least the third quarter of 2000 through the first quarter of 2002, in a scheme directed and approved by members of senior management, WorldCom concealed the true extent of its “line costs.” By improperly reducing reserves held against “line costs” and by transferring certain “line costs” to its capital asset accounts, WorldCom falsely portrayed itself as a profitable business when it was not, and concealed large losses WorldCom suffered. WorldCom’s fraudulent accounting practices with respect to “line costs” were designed to and did falsely and fraudulently inflate its income to correspond with estimates by Wall Street analysts and to support the price of WorldCom’s common stock in the market.

3. There was no documentation supporting, nor was there any proper business rationale for, the false and fraudulent entries made to the general ledger by WorldCom officers and employees.

4. As a result of these fraudulent, false and improper accounting manipulations, WorldCom materially overstated its earnings as well as its assets and materially understated its expenses in its filings with the Commission.50

50 See footnote 33.