Blockchain and Internal Control

The COSO Perspective

50th World Continuous Audit and Reporting Symposium

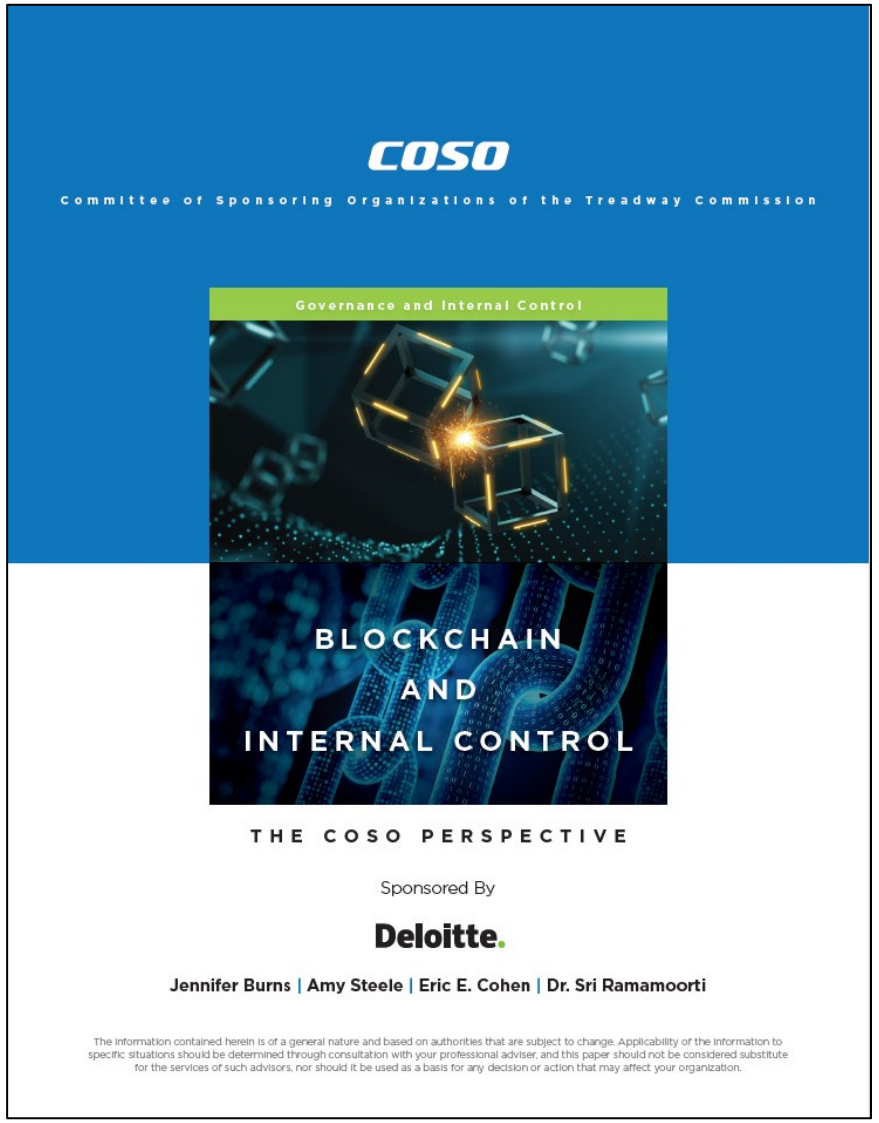
November 6, 2020

Today's speakers:

Jennifer Burns, Deloitte (Retired)

Eric E. Cohen, Cohen Computer Consulting

Paul Sobel, COSO



Executive Summary

Blockchain and Internal Control – The COSO Perspective

As blockchain becomes more mainstream, organizations interested in using it will need to evaluate the risks associated with the particular blockchain being considered and how to address those risks.

COSO's *Internal Control-Integrated Framework* (the 2013 Framework) provides an effective and efficient approach that can be leveraged to design and implement controls to address the unique risks associated with blockchain.

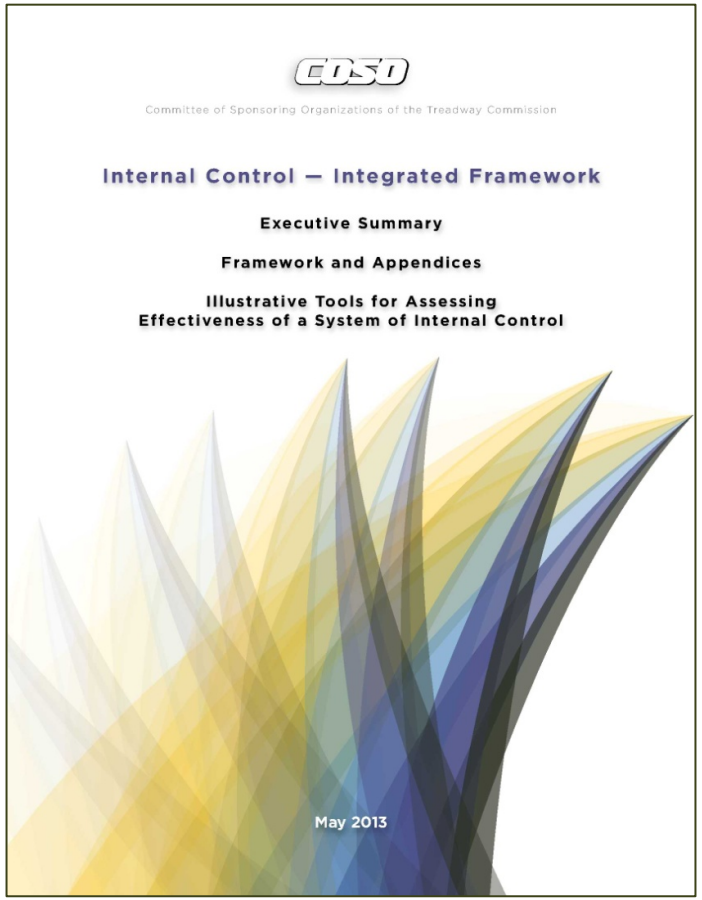
The paper provides perspectives for using the 2013 Framework to identify, evaluate, and mitigate risks related to the use of blockchain in the context of financial reporting.

- It is intended to help inform decisions regarding oversight, risks, and internal control over financial reporting related to the use of blockchain.

The paper also provides:

- High-level background on blockchain
- Examples of how blockchain may impact each of the components of the 2013 Framework
- Considerations for how stakeholders may use the guidance and next steps
- Ten things to know about blockchain

COSO's Internal Control: Integrated Framework



1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

13. Uses relevant information
14. Communicates internally
15. Communicates externally

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Background of Blockchain

What is Blockchain?

Blockchain is a secure and **transparent sequential database** maintained by a **decentralized network** of users responsible for **agreeing upon additions to the chain** and **secured through cryptography**.

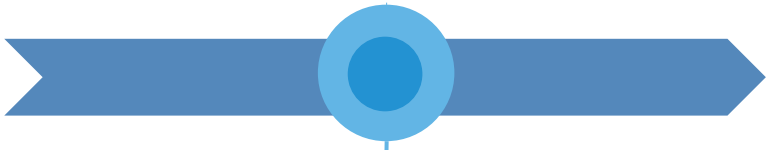
- Many different types of blockchains exist; there is no singular “the blockchain.”
- With blockchain functionality (e.g., facilitating the transfer of digital assets in near-real time), organizations have the opportunity to work differently, with new business models and value chains, and increased speed toward product or delivery.

Began in the early 1990s

Using math and cryptography to prove document integrity by linking new batches of document metadata to an existing chain.

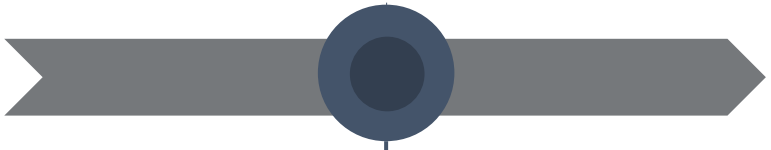
Leverages time-stamping and digital signatures, with the goal to ensure the integrity of data throughout the chain.

Initial adoption used for Bitcoin



While digital assets and their volatility in value made headlines, market participants began to investigate the underlying technology, blockchain, and its potential as a new means of connecting parties.

New blockchains created with tokens and smart contracts

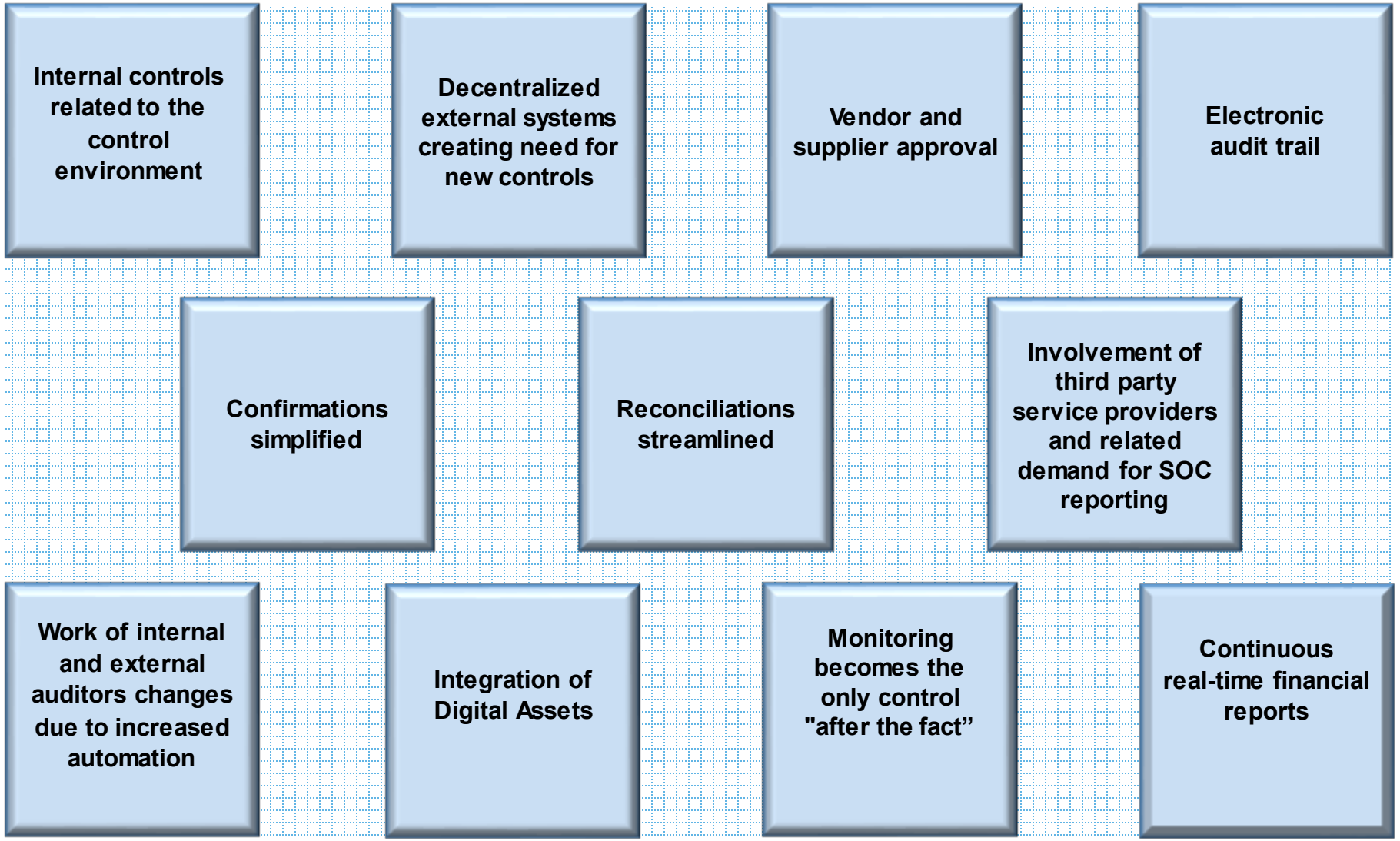


A number of other blockchains sprouted (e.g., the Ethereum blockchain). These added the ability to design custom digital assets called tokens and introduced a powerful programming environment called smart contracts.

Example of Financial Reporting Controls & Processes Impacted by Blockchain

The internal control environment is likely to be different in a blockchain-enabled world.

It is important to **consider and leverage these differences**, factoring in blockchain capabilities, attributes, risks, and benefits.



Control Environment – Example Impacts

Control Environment - Principles				
1. Demonstrates commitment to integrity and ethical values	2. Exercise oversight responsibility	3. Established structure, authority, and responsibility	4. Demonstrates commitment to competence	5.Enforces accountability

Enhancements

- Avoid human error and combat transactional and reporting fraud.
- Cryptographically-verifiable immutability and irreversibility.
- Real-time financial reports due to increased visibility.
- Timelier identification of deviations from organization's standards of conduct
- May facilitate removal of management's manual intervention from processes

New Threats/Risks

- Threat that a permissionless blockchain may be used for unethical exploits.
- Decentralization and lack of a central intermediary, system or oversight body
- Depending on nature of the blockchain and the fellow blockchain participants, an organization may face reputational risk
- Competent personnel are hard to find, and a commitment to competence is difficult to guarantee or assess

Mitigation

- Develop a code of conduct which governs the conduct of parties within a blockchain and establishes guidelines for addressing noncompliance
- Consider expectations regarding outsourced service providers
- Develop due diligence policies which establish guidelines and criteria for determining parties with whom the organization will transact, grant access to, and public blockchains that an organization may elect to use
- Assess the need to obtain or build expertise surrounding blockchain
- Ensure that the organization is capable of assessing and evaluating the new technology and processes
- Establish cross-disciplinary teams, which include blockchain specialists and representatives from each aspect of the business that may be effected
- Define degrees or levels of responsibility and authority surrounding the blockchain technology
- Establish clear reporting lines for consortium or private blockchains which identify individuals or a group responsible for handling disputes, if not built into the underlying protocol

Risk Assessment – Example Impacts

Risk Assessment - Principles			
6. Specifies suitable objectives	7. Identifies and analyzes risk	8. Assess fraud risk	9. Identifies and analyzes significant change

Enhancements

- More agile business environment, which identifies and assesses the achievement of various entity objectives

New Threats/Risks

- Different risk tolerances among members of a blockchain
- May be vulnerable to new fraud schemes or new avenues to carry out traditional fraud schemes
- Obtaining sufficient appropriate evidence to support transactions
- Unmanageably large amount of data available
- Digital assets introduce a new class of asset for which there exists little or no prior experience and few meaningful parallels
- Poor integration of blockchain with other entity systems
- Continuous evolvement surrounding blockchain, including fast paced and rapid evolvement of the business environment
- General IT and other risks may be exacerbated or heightened
- Smart contracts are both a potential risk and an important part of the risk mitigation tool set

Mitigation

- Establish objectives for use of blockchain such that its implementation supports reliable and verifiable books and records
- Engage appropriate IT and blockchain specialists to assess how blockchain will be integrated into and operate as a part of the entity's existing IT infrastructure
- Develop more robust risk assessment processes that consider the implications of blockchain
- Develop procedures to stay abreast of changes in the business and regulatory environment around blockchain
- Develop strong governance and change-control processes to deploy new or amend existing smart contracts or changes to the blockchain.
- Example controls to mitigate fraud and cybersecurity risks:
  1. Implementing appropriate segregation of duties
  2. Establishing controls over information transfer to and from the blockchain
  3. Using multi-signature or key sharding techniques
  4. Deploying a combination of preventive controls and detective controls to protect from IT intruders
  5. Identifying and assessing cybersecurity risks – considering how the organization and other members of the blockchain network may work together

Control Activities– Example Impacts

Control Activities - Principles		
10. Selects and develops control	11. Selects and develops general control over technology	12. Deploys through policies an procedures

Enhancements

- May reduce concern over direct access to record, modify, or delete historical data.
- Provides opportunities to combat transactional and reporting fraud
- Eliminates the need for certain IT general controls by minimizing the risk of data loss
- Mitigates the potential risk of untimely transaction processing and recording while also reducing errors
- Use of smart contracts prevents opportunities for fraud

New Threats/Risks

- Highly dependent upon underlying technology and implementation of business/IT controls
- Smart contracts with deficient business logic could lead to large-scale automatic execution and recording of invalid transactions, for which there could potentially be no recourse
- A lack of proper controls over the private keys could lead to potential loss or misappropriation of organization assets
- Consensus protocol could compromise the ability to properly validate transactions in accordance with the agreed-upon rules
- The completeness of transactions may be brought into question if the organization engages in recording off-chain transactions

Mitigation

- Revise policies and procedures to address new risks, internal controls, and accounting related to the use of blockchain
- Establish responsibility and accountability for executing the policies and procedures
- Consider identifying and implementing relevant controls over key aspects of the blockchain, including: nodes, consensus protocols, private keys, and smart contracts
- To mitigate the risks associated with smart contracts companies may:
  1. Implement controls to validate the appropriateness of the design and implementation effectiveness of smart contracts, track changes and updates in a controlled fashion, and ensure there is proper documentation and historical record to establish accountability.
  2. Implement controls over the inputs into smart contracts, including inputs from blockchain oracles.

Information & Communication – Example Impacts

Information & Communication - Principles		
13. Uses relevant, quality information	14. Communicates internally	15. Communicates externally

Enhancements

- Enhanced visibility of transactions and new avenues for management to communicate financial information to key stakeholders
- Promotes the availability of data that is accessible, accurate, consistent, current, retained, and timely
- Data is less likely to be lost when being entered into or aggregated within a common and comprehensive digital ledger, promoting better visibility and offering supplemental provenance evidence

New Threats/Risks

- False sense of comfort that data on blockchain is correct, available, the correct people have been notified, and feedback has been received
- Large amounts of data will need to be processed into useful and actionable information
- Potential challenges gathering sufficient appropriate evidence to support assertions about the digital assets or digital asset transactions
- Potential challenges with the ability of auditors to obtain the evidence they need to assess whether the books and records are adequately supported

Mitigation

- Educate key stakeholders on how blockchain will be used by the business and the associated benefits and risks of using the technology
- Establish a method for members of a blockchain network to report any concerns.
- Determine new information requirements needed in light of the use of blockchain
- Develop communication methods to ensure that operational and other changes/updates relating to the use of blockchain are communicated to appropriate personnel
- Develop data analytics procedures to identify and obtain relevant, quality data from the blockchain that can then be processed into information to be used to support management's business processes and reporting objectives.
- Engage in discussions with both internal and external auditors during the development of or identification of a blockchain to be used in the entity's processes.

Monitoring Activities– Example Impacts

Monitoring Activities - Principles	
16. Conducts ongoing and/or separate evaluations	17. Evaluates and communicates deficiencies

Enhancements

- Evaluations themselves can be built into a blockchain-enabled process using smart contracts, AI and standardized rules engines.
- Blockchain allows monitoring activities to catch problems closer to occurrence minimizing exposure and speeding remediation.
- Advanced analytics, AI and other tools can be used to analyze the detail allowing management to concentrate on higher risk areas.

New Threats/Risks

- Extensive amounts of data, leading to risk of information overload and challenges in monitoring
- Finding competent people to design and perform effective monitoring
- Difficulty in staying abreast of ongoing change and ensuring proper and timely updates to the technology and to any other procedural or operational processes
- Decentralization and lack of a central intermediary associated with certain blockchains may result in no established party or body responsible for executing monitoring controls

Mitigation

- Use ongoing evaluations to identify changes and updates to the technology, and to validate whether the components of internal control are present and functioning.
- Identify and obtain talent with requisite knowledge of an entity's baseline control environment, blockchain technology, and best practices surrounding monitoring techniques to
  1. assist in designing and implementing appropriate monitoring controls
  2. assess the results and efficiency of such monitoring activities.
- Assess the unique aspects of blockchain such as consensus protocols, smart contracts, private keys as well as factors relating to the ongoing health, governance, and overall reliability of the blockchain in use.
- Retain an objective third party to assess consortium blockchains.
- Monitor service-level agreements with and control reports from outsourced service providers.

Blockchain, Financial Reporting Assertions, and Audit Evidence

The list below highlights areas in which blockchain may present challenges with respect to how companies provide sufficient and appropriate audit evidence to support management's assertions surrounding assets or transactions stored on a blockchain

1. Valuation
2. Existence
3. Allocation
4. Occurrence
5. Completeness
6. Classification
7. Understandability & Presentation
8. Accuracy
9. Cut-off
10. Obligations & Rights

10 Things to Know about Blockchain

1

Information about blockchain in the news and on the Internet is often misleading or incorrect.

2

Blockchain encompasses far more than digital assets; the benefits it can bring to an organization can be substantial.

3

Blockchain is, however, not "magic", comes at a cost, and doesn't eliminate all risks; in fact, it introduces new risks.

4

Knowing how blockchain works is crucial for evaluating, preparing for and managing blockchain's impact on internal control and the organization as a whole.

5

Blockchain has both technology and governance implications.

6

Blockchain will not make management, accountants, or auditors less relevant, although it will impact what they do and how they do it.

7

Blockchain requires new skillsets (e.g., data science for greater insight and foresight) and new collaboration within and across organizations.

8

Now is the time to educate and engage stakeholders throughout the organization.

9

Blockchain is still in flux and continues to evolve.

10

Adoption of blockchain may not be a choice.

Next Steps for Key Stakeholders

1 Board of Directors & Audit Committee Members

- Gain a foundational understanding of blockchain.
- Build internal expertise on the board and among leadership.
- Understand how blockchain enabled processes may promote or reduce reporting efficiency and risk.
- Understand how internal and external auditors may be considering blockchain.

2 Executives, Internal Auditors, Management Accountants, & Internal Control Managers

- Build internal expertise and support discussion at management level about potential of blockchain.
- Gain insights about how blockchain is being used.
- Coordinate with blockchain developers.
- Understand how blockchain may impact the audit.
- Evaluate risks and control implications related to the use of blockchain (using 2013 Framework).

3 External Auditors

- Build knowledge and expertise of blockchain.
- Understand how blockchain may impact the audit
- Work to develop necessary tools (e.g., to understand the internal controls and audit blockchain transactions).

4 Academics

- Help educate students.
- Consider potential research projects related to the implementation of blockchain and its use cases

Thank You! Any questions?

- **Jennifer Burns, Deloitte (Retired)**
  - https://www.linkedin.com/in/jennifer-burns-5567936/
- **Eric E. Cohen, Cohen Computer Consulting**
  - https://www.linkedin.com/in/eric-cohen-53180b13/
- **Paul Sobel, COSO**
  - https://www.linkedin.com/in/paul-sobel-16a686/