EDPACS

THE STATE OF INFORMATION SECURITY LAW: A FOCUS ON THE KEY LEGAL TRENDS

Taylor & Francis
Taylor & Francis Group

EDPACS

The EDP Audit, Control, and Security Newsletter

ISSN: 0736-6981 (Print) 1936-1009 (Online) Journal homepage: https://www.tandfonline.com/loi/uedp20

BLOCKCHAIN AUDITING – ACCELERATING THE NEED FOR AUTOMATED AUDITS!

Michael P. Cangemi & Gerard (Rod) Brennan

To cite this article: Michael P. Cangemi & Gerard (Rod) Brennan (2019) BLOCKCHAIN AUDITING – ACCELERATING THE NEED FOR AUTOMATED AUDITS!, EDPACS, 59:4, 1-11

To link to this article: https://doi.org/10.1080/07366981.2019.1615176

Published online: 04 Jun 2019.

EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

2019 VOL. 59, NO. 4

BLOCKCHAIN AUDITING – ACCELERATING THE NEED FOR AUTOMATED AUDITS!

MICHAEL P. CANGEMI AND GERARD (ROD) BRENNAN

Abstract. This article explores issues related to auditing Blockchain ledgers (BC) or Distributed Ledgers (DL). These very new technologies and audits thereof are in the infancy stage. While auditing BC/DL networks in the future is still being studied, we believe this paper will provide food for thought and discussion. That said, we also believe that due to the structure of these new technologies audit approaches are sure to include the use of continuous controls/analytics and continuous monitoring. We discuss BC attributes that have resulted in assumptions that the BC is self-auditing. While in some respects they are, there are significant new risks on blockchains which require new controls and audit programs. New control features in a BC/DL include the concept that all the users have a complete copy of the ledger with all the data and all the transactions and system features that make transactions immutable – plainly speaking, they cannot be changed. We explain the Consensus Mechanism for a BC and how it and public/private keys replace heretofore traditional controls. Assertions such as occurrence, completeness, cutoff, accuracy, etc., are all addressed by BC systems providing significant improvements in control precision. There are, however, new assertions and controls that need to be addressed with BCs and new risks especially with the introduction of smart contracts. We have assumed the reader has a basic level of understanding about a BC. For further background we recommend you consult our bibliography. As noted, we do not believe this paper has all the answers or addresses all the risks associated with BC/DL. We trust new approaches will be leveraging a whole new set of controls and audit practices unique to this exciting rapidly emerging technology.

Our early reading on Blockchain (BC) ledgers made them appear to be self-auditing systems, and along with many accountants/auditors, we started to think of it as a new world order for accounting and auditing. We were drawn to the word ‘ledgers’ and thought, along with many others, perhaps this innovative ledger technology would replace all accounting ledgers?

IN THIS ISSUE

Editor
DAN SWANSON

Editor Emeritus
BELDEN MENKUS, CISA

Taylor & Francis
Taylor & Francis Group

CELEBRATING OVER 4 DECADES OF PUBLICATION!

Since then, after attending conferences, reading journals and discussions at the Rutgers University Continuous Audit & Reporting Laboratory (CarLab) Advisory Board, where we both serve, we have learned much more about the control advantages and vulnerabilities of the BC. In the process, we were also invited to work with a progressive software firm Lukka, formerly known as Libra, a blockchain and digital asset-focused accounting, audit and tax software provider (www.lukka.tech).

In a 2015 article, by Ryan Lazanis, the founder of XEN Accounting, blockchain was described as follows, "The blockchain is a public, decentralized, distributed ledger that is capable of storing and confirming the transactions that pass through it. This means that the ledger is not owned or controlled by any one party. Instead, the control of the network, or protocol, is distributed among the network's users. As transactions hit the blockchain, they are confirmed as true and accurate by the network's users called miners."[1]

Lazanis went on to say; "We're not there yet, but in less than 10 years, I believe that the technology behind bitcoin will transform the accounting profession entirely."[2] These were bold prognostications, and we were hooked on the concept of blockchain and had to learn more.

Starting our fintech careers as IT auditor's in the 1970s & 1980s and both serving for a time as CFOs; we witnessed many fintech evolutions including the early centralized database systems (DBs) and early networks eventually leading to the internet. Centralized DBs were very effective but brought with them some control issues related to having all the data in one place and under one systems control.

The BC is a new iteration of a distributed ledger systems in which the data are not centrally stored and controlled but rather distributed to all the ledgers users. Furthermore, there are various types of BCs, for example: private BCs like the one a bank or supply chain parties may deploy and a public BC like for a cryptocurrency i.e.: Bitcoin.

CRYPTOCURRENCY OR CRYPTO ASSETS

As with many discussions about the blockchain, there is always a mention of cryptocurrency as a type of digital asset. This is only logical since the BC technology was first launched as part of the now well-known bitcoin, a digital or cryptocurrency. These are two separate but related subjects! DLs existed before the bitcoin blockchain. Since bitcoin is a new currency, and trust and eliminating intermediaries were key objectives, the founder started with a BC/DL technology where trust is added by many users having a copy of the ledger.

Regulatory oversight of both digital assets and BC is also in the very early stages. According to Phil Zongo, "Until recently there have been very few global laws to govern digital currency's (part of digital assets) and (initial coin offerings) ICOs".[3] Issues related to digital assets and ICOs frauds and hacks are beyond the scope of this article.

Early on we learned there were some nice control features in a distributed ledger, for example, all the users had all the data and all the transactions making transactions essentially immutable. This is accomplished by having a unique hash for each transaction captured in an integrated log. Transactions are recorded and confirmed in a pseudo-anonymous manner. In the case of the Bitcoin BC, transactions are confirmed by "miners" who run programs to ensure the transactions are valid. Enabled by today's robust computer networks, the DL records, and shares, in real-time all transactions which are append-only, so once information is entered, it cannot be altered.

The DL distributed approach and related mining, using a Proof of Work Consensus mechanism (defined below) as is the case for Bitcoin, requires very large amounts of computer processing and costs for electricity, which can in some cases make the BC/DL very costly. In addition, while the transaction confirmation process that is executed by miners is acceptable for Bitcoin, it is one of the key assertions that is still being studied.[4] Alternative consensus mechanisms using less resources such as "Proof of Stake" are gaining attention.

How is providing Audit/Assurance on Blockchain/DL Different? Lukka conducted research with Rutgers University's Continuous Audit & Reporting Laboratory - "CarLab" and is working on blockchain native automated auditing/monitoring solutions. There are fascinating distinctions about this innovative technology which promises to answer the above questions and to fundamentally change the way we view and provide assurance/auditing on BC/DL.

We also learned Blockchains introduce new sets of risks which we will cover later. On the plus side, we learned that to a considerable extent a properly designed BC/DL network is "self-auditing" for many of the traditional system audit IT general controls (i.e., Authentication, Authorization, Segregation of Duties, Change Management, Archiving, etc.). These types of controls are often built into BC/DL technology via the use of cryptography, consensus mechanisms and the sharing or distribution of the DL. This showed us that DL controls can be better in some instances to the control precision provided by these same controls in traditional central database systems.

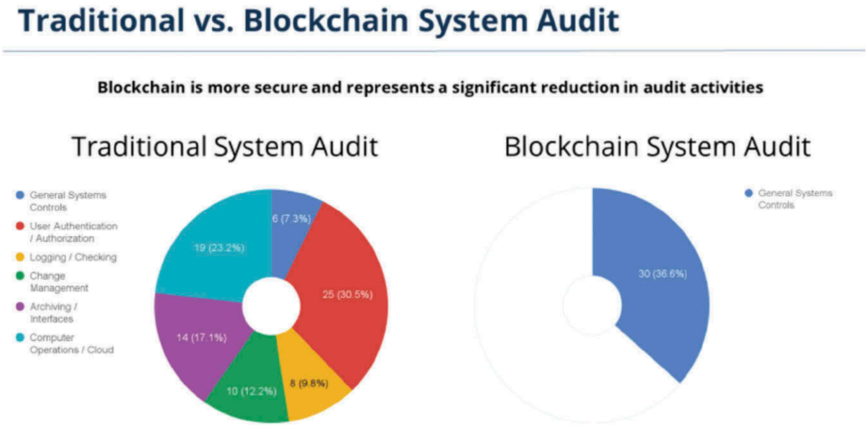
Take for instance segregation of duties (SOD) controls, which generally only assure a "4-eyes" level of control (i.e., a purchase approver cannot also pay an invoice). The 2018 ACFE Fraud Report To The Nations, based on actual fraud cases, reports that nearly 50% of all fraud is collusive – so in even the most secure central databases we generally only need two colluding bad actors to perpetrate or conceal a fraud![5] With private or public blockchains we may have 10, 50, 100 or even 1000s of "eyes" "approving" every transaction on the ledger in real time by leveraging the consensus mechanism – this is part of what makes the security of BC/DL networks more secure than their central database counterparts.

The Consensus Mechanism for a BC or DL is simply the agreed method by which all transactions or changes will be reviewed and approved before being submitted to the BC ledger. Most public and private blockchains require the consensus approval of at least some simple majority (i.e., 51% or more) of the validators (stakers or miners) and generally include some type of analytics review and a proof of work or stake to confirm which miner submits the new version of the ledger to all nodes or participants on the network. Public or private keys replace passwords, the consensus mechanism replaces change management (as well as SOD), a complete distributed ledger replaces archiving, etc. – a properly designed blockchain really is way more secure than a traditional central database!

We need to acknowledge that a process in the BC is basically the execution of a computer program, for example, the consensus mechanism or any smart contract, and any computer programs can be flawed and could be vulnerable to malicious coders. In addition, we acknowledge hacking by a simple majority, for example, 51%, of the nodes on a BC is possible, even if improbable.

The chart below contrasts the common control sets found in a traditional system audit on a single database with those needed on a properly designed private blockchain – note the BC/DL network needs only about a third of the controls applied in a traditional system audit. Blockchains, however, introduce a whole new set of risks and controls that do need to be addressed by auditors.

Exhibit 1 [(7)]:



Blockchain controls are addressing completely different objectives, risks, and assertions. For a BC/DL network the risks are not so much around individual participants access/authentication, but more around the activities of network nodes represented by activity and transactions they generate on the network. Some of these transactions/controls are ubiquitous to any BC/DL network and others will be unique to the specific processes the network is supporting (i.e., Financial Services, Supply Chain, etc.).

The immutable transaction history provided by BC/DL's address accounting assertions in a much more robust manner. Assertions such as occurrence, completeness, cutoff, accuracy, etc., are all memorialized for the population of transactions on blockchains, providing an improvement in control precision over traditional periodic sample-based testing of assertions.

The greatest risk to BC/DL networks, as evidenced by the DAO hack in June of 2016[6] on the Ethereum network (a bad actor exploiting a deficiency in a "Smart Contract" and stealing some ~$70M from the network) and others since, is with vulnerable "smart contracts" running on blockchains. A smart contract is simply a self-executing digital agreement in a computer program.

We believe, BC/DL technology lends itself by design to a much more automated population-based continuous auditing methodology. This is because most of the blockchain protocol code, consensus mechanism, and smart contracts are automated allowing for population and often preventive analytics running on every transaction or block of transactions in the network! This enables and contributes further to the "cheaper, better, faster and more secure" advantage of BC/DL, possibly making the ultimate cost of compliance lower with a significantly higher level of assurance.

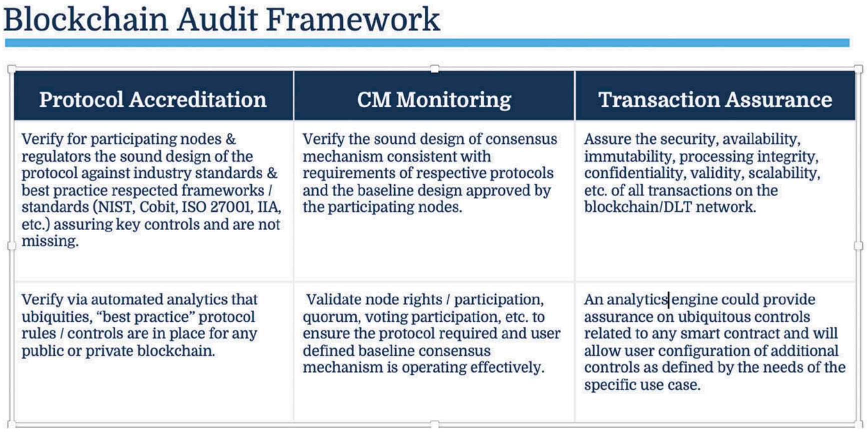
The Biggest Risks are Generally with the Smart Contracts and Not with the Blockchains Themselves

Although blockchains can record relevant information, the transaction may be unauthorized, incorrectly classified in the financial statements or linked to a side agreement that is "off-chain." Even if the transactions are recorded in the blockchain, auditors will still have to perform routine audit analysis for any required financial statement audits.

Blockchains introduce new sets of risks around protocol code, consensus mechanisms, smart contracts and with the many interfaces with blockchains such as wallets, exchanges, and funds in the whole ecosystem. Controls and assertions are also very different on blockchains and testing them will by design need to be much more automated and cross-functional than we see today with traditional control activities.

We see three key areas outlined below of risk where controls are needed to provide assurance for blockchain and distributed ledger technology.

Exhibit 2 [7]:



Blockchain Audit Framework

Protocol Accreditation	CM Monitoring	Transaction Assurance
Verify for participating nodes & regulators the sound design of the protocol against industry standards & best practice respected frameworks / standards (NIST, Cobit, ISO 27001, IIA, etc.) assuring key controls and are not missing.	Verify the sound design of consensus mechanism consistent with requirements of respective protocols and the baseline design approved by the participating nodes.	Assure the security, availability, immutability, processing integrity, confidentiality, validity, scalability, etc. of all transactions on the blockchain/DLT network.
Verify via automated analytics that ubiquities, "best practice" protocol rules / controls are in place for any public or private blockchain.	Validate node rights / participation, quorum, voting participation, etc. to ensure the protocol required and user defined baseline consensus mechanism is operating effectively.	An analytics engine could provide assurance on ubiquitous controls related to any smart contract and will allow user configuration of additional controls as defined by the needs of the specific use case.

We see addressing the vulnerabilities within this framework as the perfect application for mitigating risks on blockchains with population-based, continuous controls/analytics.

We have observed that the current risk management and internal controls methodology and processes for developing internal controls and auditing conventional databases is sound and is applicable to blockchain technology. The practice and approach to implementing internal controls and auditing on BC/DL networks will, however, be completely different and needs to be changed dramatically!

LIMITATIONS OF AUDITING BLOCKCHAINS

Blockchains are not a panacea and will not cure all that ails accounting and auditing. There are clear limitations as to where and how blockchains can contribute to the next generation of commerce and accounting practice. For the foreseeable future, it is doubtful a BC/DL will ever be used for the primary general ledger of large entities. Most BC/DL on the horizon will be for supplemental or supporting shared sub-ledgers within or among cooperating individuals or organizations.

Another key limitation of leveraging BC/DL networks is that blockchain networks often have incomplete or a limited amount of data needed to perform an audit of a complete process of end-to-end transactions. Blockchains by design carry a limited amount of information in the database in order to ensure privacy and prevent the network from "bloating" (getting too large to efficiently be sent out to all nodes on the blockchain) as the network grows. Remember, blockchains are generally not archived and must keep and distribute all of the information on the chain from the first or "genesis" block to the current block. A blockchain record may only have a few fields such as a public key, a number of units, a date stamp, etc., lacking any valuation, link to source documents, and other critical information needed to evaluate internal controls and perform a comprehensive audit, therefore new audit approaches are required.

Blockchain networks transacting with cryptocurrencies on public blockchains have a unique limitation in evaluating or auditing transactions because the blockchain often provides an incomplete picture of the transactions related to an individual or entity. This results from cryptocurrency Exchanges and Wallets centrally clearing and settling transactions (i.e., trades) at the exchange such that some intraexchange transactions are never submitted to the blockchain. As an example, if cryptocurrency trader "A" on exchange "X" transfers 5 Bitcoin to cryptocurrency trader "B" also on exchange "X", this transaction may never be submitted to the Bitcoin blockchain because exchange "X" will just clear/settle the trades between the two clients. This common trading practice results in many "off-chain" transactions allowing cryptocurrency exchanges to save time, effort and money by not submitting intra-exchange trades to the blockchain. In Over The Counter Trading (OTC) of cryptocurrencies and with most deposits and withdrawals on exchanges the transactions are bilaterally cleared with each counterparty and settled on the blockchain – these are referred to as "on-chain" transactions.

Therefore, the Vast Majority of Economic Transactions with Crypto Assets Today are Not Transacted on the Blockchain!

A complete view of an entities crypto asset activity includes transactions sourced from both the blockchain and third party/counterparty exchange venues.

The implication for internal controls and auditing is that the control environment and auditing approach for cryptocurrencies must address the entire blockchain ecosystem and not just the blockchain itself to ensure a comprehensive control review or audit. For private BC the auditor will need to define the BC ecosystem. However, today an approach for a system audit or any audit involving cryptocurrencies must be able to identify all transactions across all stakeholders in the cryptocurrency ecosystem including exchanges, wallets, over-the-counter traders, banks and other third parties to ensure a complete picture of the processes and transactions.

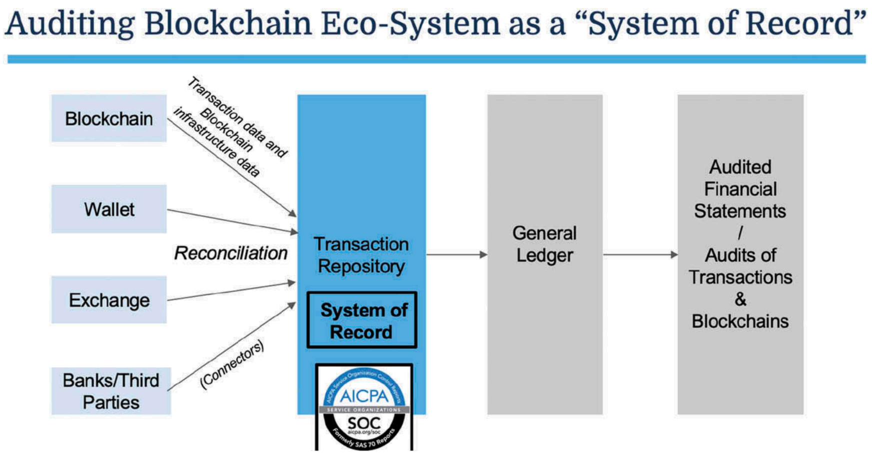
AUDITING THE BROADER BLOCKCHAIN/DL ECOSYSTEM

Given the above limitations of auditing blockchain as a separate entity, it quickly becomes apparent that comprehensive financial reporting or auditing of any blockchain or distributed ledger network needs to encompass the broader ecosystem in the audit scope in order to capture the end to end processes and transactions. An innovative approach to accomplish this is being developed by Lukka.

As outlined above, blockchains provide a limited amount of information and do not provide complete transactions for cryptocurrencies because of the "off chain" trades on most of the major exchanges.

Lukka's approach, outlined in the chart below, is to extract append only transactions with permissioned client meta data (i.e., keys, etc.) via open and proprietary APIs into an accredited (Via: SOC 1 & 2 Type 2) "System of Record" secure cloud database. Data are ingested for the client from the entire blockchain eco-system including all the major blockchains, exchanges, wallets, banks, OTC desks, miner pools, etc., assuring that all client transactions are captured and integrated into an accredited system of record. The data then are normalized and enriched with valuation, pricing, positions in LIFO, FIFO, etc. and provided back to the client for financial or tax reporting.

Exhibit 3 [7]:


Auditing Blockchain Eco-System as a "System of Record"

Lukka, with research input from Rutgers and other major universities, accounting firms, and others will also soon be extracting infrastructure data about the blockchains into its current secure system of record database. They could then include running continuous automated control analytics with a versatile "analytics engine" to monitor risk-based blockchain system audit controls in the three key areas of its audit framework outlined above. Thereby providing an example of why we suggest the structure of these new audit approaches must include the use of continuous controls/analytics and continuous monitoring.

For example:

- Protocol Accreditation (Are the Protocol Analytics secure, complete and appropriate for this blockchain use case/application?)
- Consensus Mechanism (Is the public or private blockchain conforming to its Consensus Mechanism?)
- Transactions & Smart Contracts (Are transaction combinations and ubiquitous smart contract controls in place to mitigate the risks of manipulation and smart contract hacks?)

Further, Lukka currently has an inventory of about 75 blockchain-specific controls across the above three risk categories which it may opensource to glean additional input from clients, accounting firms, academic researchers and others in order to provide an automated system audit of any blockchain network.

Smart Audit Analytics

Another anticipated approach to performing a comprehensive system audit on blockchain or distributed ledger is to establish a read-only "audit" node on a public or private blockchain with the controls monitoring analytics executing as a smart contract within the blockchain. The smart audit analytics would be approved by the consensus mechanism.

According to Andrea Rosario, Ph.D, "smart audit procedures that can automate manual and repetitive audit tasks that do not require audit judgment offer auditors the opportunity to focus resources on higher risk areas and thus improve audit quality." [8]

While these approaches are being considered the audit of BC and DL is still in its infancy. As discussed above, smart contracts are the greatest single control risk to blockchains networks. In addition, the limited amount of data on any given blockchain needed to perform end-to-end audit process may be a limitation.

As noted, there are still many questions that need to be answered and processes deployed to audit a BC – this article presents some preliminary thoughts to spur on this discussion.

CONCLUSION

Blockchains do need to be audited! Independent auditing/assurance of blockchains is needed now from both internal and external assurance providers on both public and private blockchains. Auditors will continue to be an important part of the assurance process; however, blockchain will force auditors and accountants to advance their use of automation, including automated analytics and continuous monitoring, thereby improving audit scope and efficiency!

Blockchain may not remove auditors from assessing transactions, but it can transform the way auditors perform system and financial statement audits. The core control activities that most blockchains provide by design will allow auditors to trade up to the more forensic audit activities leveraging more, analytics, automation, AI and machine-learning capabilities to improve audit effectiveness and efficiency. If auditors are freed up to use these technical capabilities, the length of the whole financial reporting and auditing cycle could be reduced significantly.

The risks and controls needed to mitigate exposure on BCs are different than those needed for central data-based systems, and the practice guidance and audit programs for auditing must be very different because of the inherent design and technology deployed in blockchain/DL ledgers. The first priority in providing audit/assurance on blockchains is the accreditation of the BC/DL system (i.e., "systems audit") – without this assurance, any business or reporting process built upon the network is at risk.

Clearly, current audit practice leveraging periodic, often non-statistical sampling methods will not adequately address the assurance needs of a dynamic, distributed, automated BL/DL ecosystems. We have the tools, technology, and methodologies today to re-define audit practices to address blockchain ledgers and should apply the same innovative assurance methodologies to existing auditing practices on central databases. How we audit in the BC/DL networks in the future is still being studied. However, we believe it is sure to include the use of analytics and continuous monitoring, leveraging a whole new set of controls and audit practices unique to this exciting rapidly emerging technology.

Notes

1. How Technology Behind Bitcoin Could Transform Accounting As We Know It by Ryan Lazanis, the founder of XEN Accounting, an accounting firm based in Quebec, Canada
2. IBID
3. The Promises and Jeopardies of Blockchain Technology Phil Zongo; ISACA Journal Vol. 4 2018 page 30
4. Caseware Analytics blog: Cangemi Perspectives: Introduction to Blockchain and the Potential for Advancing Analytics https://idea.caseware.com/blockchain-advancing-analytics/
5. 2018 ACFE Fraud Report To The Nations, https://www.acfe.com/report-to-the-nations/2018/page. 42
6. Information on the DAO hack of 2016 can be found here: https://www.coindesk.com/understanding-dao-hack-journalists
7. Exhibits 1, 2 and 3 from Lukka, formerly known as Libra Tech – website: https://lukka.tech
8. "Reengineering the Audit with Blockchain and Smart Contracts" Andrea Rosario and Chanta Thomas; Journal of Emerging Technologies in Accounting.

REFERENCES

Blockchain Fundamentals: An Inside Look at the Technology With the Potential to Impact Everything; 29 pages 2017 ISACA

The Promises and Jeopardies of Blockchain Technology Phil Zongo ISACA Journal Vol. 4 2018

The Five Anchors of Cyber Resilience Phil Zongo https://www.amazon.com/Five-Anchors-Cyber-Resilience-Enterprises/dp/0648007847

Michael P. Cangemi is a former CFO and CEO, a prolific writer, active speaker and senior advisor to various companies; he has had a wide-ranging career having served as a CAE, CIO, CFO and then in two CEO positions, as well as, on Boards and as Audit Committee Chair. Mr. Cangemi now has a significant focus on Technology for Business and specifically Continuous Monitoring, Analytics and Blockchain DLs for GRC, Finance and Business Process Improvement. He is a Senior Fellow at and serves on the Rutgers Continuous Auditing and Reporting Lab - Advisory Board, a Senior Advisor to CaseWare Analytics (CA & CM Analytics); he serves on the Lukka Audit Advisory Board (Distributed Ledgers/blockchain); and he is an investor in and former advisor to Solink Corp (Video & Contextual Analytics).

His experiences as a CAE were published in his second successful book, Managing the Audit Function. The book, now in a third edition, was featured in the business section of the Sunday New York Times in August 2002 and translated into Chinese in 2005 and Serbian in 2013.

A CPA retired and CISA retired he was President, Chief Executive Officer and Director of Etienne Aigner Group, Inc., a leading designer of women's accessories and President and Chief Executive Officer and Director of Financial Executives International, the professional association for senior-level corporate financial executives. He currently serves as President of Cangemi Company LLC, which he founded, and through which he serves as senior advisor to various companies and manages his other business interests. He also serves on FEI's Committee on Finance & Technology (CFIT) and their GRC Sub Committee; the EDPACS Editorial Advisory Board; and the ISACA 50 Anniversary Committee.

He has served in numerous volunteer positions at IIA and ISACA, including ISACA International President & Board Chair and IIARF Trustee. He went on to serve as Editor-in-Chief of the ISACA Journal for 2 decades, as well as, serving as a COSO Board Member, four years on the Financial Accounting Standards Advisory Council (FASAC) and two years on the International Accounting Standards Board-Standards Advisory Council in London. These and other positions give him an excellent window into the audit/GRC & financial verticals.

Gerard (Rod) Brennan PhD, CFE is the Audit Technologies Director for Lukka, a US-based (NY, NY) software company that automates and optimizes financial business processes for professionals who interact with distributed and decentralized technologies (i.e. Blockchain, Smart Contracts, DLT, Cryptocurrencies, etc.) helping develop innovative/automated audit and reporting solutions. Rod is an audit practitioner, frequent speaker and *published researcher on the topic of blockchain, continuous auditing/monitoring/analytics, he is the former Audit Director and North America Risk & Internal Control Officer for Siemens Corp. and an Adjunct Professor in Rutgers Univ. MBA program teaching "Advanced Auditing and Info Technology". He is excited about helping develop the next generation of automated audit/reporting applications to provide assurance on DLT/ Blockchains.*

Rod successfully defended his Ph.D. thesis on "The Use of Intelligent Software to Enable Continuous Auditing". The research work included the design and development of an ERP (SAP) continuous auditing software model incorporating some of the latest continuous auditing research concepts. The model was co-developed with Rutgers Universities' Continuous Auditing Research Laboratory (CarLab) – a leading Continuous Auditing research group. Rod continues to speak and do research in the area of automated audit and reporting for applications on DLT/Blockchains.