Continuous Auditing

An Audit Ecosystem to Support Blockchain-based Accounting and Assurance

Stephen Kozlowski,

An Audit Ecosystem to Support Blockchain-based Accounting and Assurance

Stephen Kozlowski
Eastern Illinois University, IL, USA

In introducing the concept, an audit ecosystem was defined as a "holistic approach to the design and development of a technology-driven framework to provide overall management and control of the audit technology components employed, and coordination of the activities of the participants involved" (Kozlowski & Vasarhelyi, 2014). An ecosystem approach allows the underlying automated audit functions to address ongoing changes to the environment in which they operate as that environment continues to evolve. An audit ecosystem is a specific configuration of a "digital" ecosystem to support computer-driven audit techniques. Zuiderwijk, Janssen, and Davis (2014) present an overview of the characteristics of digital ecosystems, which includes, among others, the following:

- a digital ecosystem operates as a functioning whole;
- a digital ecosystem is structured as a multi-level and multi-dimensional entity;
- development of a digital ecosystem occurs primarily through local specializations and adaption;
- a digital ecosystem is influenced by:
  - an information, communication, and networking technology infrastructure;
  - e-government, e-business, and e-society;
  - human resource development; and
  - a policy and regulatory environment.

It was also noted that this proposal for an audit ecosystem represents a natural progression from initial computer-based audit analytic tools that had been used for over 20 years, including Continuous Auditing and Continuous Monitoring (CA/CM) technologies (Vasarhelyi & Halper, 1991).

The initial research posited that the time was appropriate for an audit ecosystem approach, as the audit landscape had changed significantly since the mid-20th century, to a great extent because of the implementation of technology-based

Continuous Auditing: Theory and Application, 299–313

ISBN: 978-1-78743-414-1/doi:10.1108/978-1-78743-413-420181015

accounting tools (Kozlowski & Vasarhelyi, 2014). Prior to this period the audit was a manual, labor-intensive process, due in part to the following:

- Manual record-keeping procedures by the client;
- Manually generated accounting data maintained in paper-based records;
- Manual audit procedures conducted by the audit firm.

The replacing of these manual procedures with technical solutions now presents the opportunity for even more advanced technical solutions to be implemented, in particular in an audit ecosystem approach. The technology landscape requires a significantly sophisticated management mechanism to not only manage the individual tools but also coordinate their activities in order to provide results in the most efficient and effective manner possible to both client and auditor. The audit ecosystem will provide the technology needed to perform this critical management function.

More recently blockchain technology has emerged as one of several contemporary technologies that has the potential to significantly alter business processes, and in particular the accounting and assurance functions (Dai & Vasarhelyi, 2017). It seems appropriate to re-visit the audit ecosystem proposal and assess whether the characteristics and attributes defined for an audit ecosystem can lend themselves to support the audit function in a blockchain-enabled accounting environment.

Given the potential impact that blockchain may have over the accounting function, the "present" audit scenario, as described in the initial research (Kozlowski & Vasarhelyi, 2014), has been enhanced with blockchain-relevant comments (in italics):

- The major participants are the client and audit firm.
- Most client organizations include a formal internal audit function and many, especially larger organizations, have implemented computer-based continuous auditing and monitoring tools.
- Clients have implemented a computer-based accounting system, as well as, in the cases of larger organizations, a computer-based Enterprise Resource Planning (ERP) system and function-specific systems, such as an automated Customer Relationship Management (CRM) system.
- Financial reporting is computer-generated and presented in several formats.
- Client data is maintained digitally, possibly in several databases as well as cloud-based.
  - *The blockchain architecture typically incorporates a decentralized public database, which can lead to even greater control and security concerns for the client (Dai & Vasarhelyi, 2017).*
  - *Distributed databases are a reality as blockchain relies on multiple computers for both operation and maintenance.*
- The audit function includes a mix of manual and computer-based audit routines, which may or may not synchronize with technology-based audit tools used internally by the client.
- The technology-driven client implements both continuous reporting technologies as well as continuous auditing and monitoring tools that detect errors on a real-time basis.

The audit paradigm may also be impacted by a number of blockchain-related concepts and functions:

- If the client participates in what is known as a permissioned blockchain where the trusted parties are preselected by a central authority and given the authorization to verify transactions, should the audit function provide an external verification and validation of these parties given this form of blockchain is based on a highly trusted entity model?
- Will the clients configure themselves into what is called a "Decentralized Autonomous Organization/Corporation (DAO/DAC)" concept, where the firm leverages the use of blockchain technology to self-organize and operate (Dai & Vasarhelyi, 2017)?
  - The governance rules and decision-making policies by which the client and its trading partners operate are automated by imbedding them into what is termed a "smart contract." Smart controls would be embedded in the blockchain operations that enforce the pre-determined rules over the business processes (Dai & Vasarhelyi, 2017). Decision-making power will typically be distributed to multiple participants in the blockchain. Does the audit function need to verify and validate the assignment of authority to change these rules, as the potential exists for firms to manipulate these rules to gain illicit benefits?
- The concept of a "triple-entry accounting system" has been proposed for several years, and Dai and Vasarhelyi (2017) apply the concept to documenting the accounting entries in a blockchain environment. In this scenario every transaction creates three records: one record that is stored in the blockchain ledger as well as two transactions recorded in the traditional double-entry system. The entries in the blockchain ledger would be recorded in the form of token transfers between accounts. Should the audit function perform a verification and validation of consistency between blockchain and double-entry records, and also the tokens?
- A blockchain-enabled audit model would need to function over two environments: a physical world, and a mirror world, which consists of a virtual model reflecting business activities occurring in the physical world (Dai & Vasarhelyi, 2017). The mirror world is composed of three layers: blockchain, smart control, and payment. The blockchain layer is an ecosystem of blockchains, each of which would record a type of data that is needed for audits. Does the current audit model need to be enhanced to verify and validate the accuracy of the transactions in both physical and mirror worlds?

In the initial proposal for an audit ecosystem the starting point included a review of both current and significant articles in the areas of robotics, digital ecosystems, and software agents (Kozlowski & Vasarhelyi, 2014). The concepts presented in these research articles provide the foundation for not only the overall design and function of an audit ecosystem but also the CA/CM agents operating within an audit ecosystem that undertake much of the processing activities.

The basis for practical robotics dates back to 1948 when Norbert Wiener developed the principles of cybernetics (Wiener, 1948). Development progressed with the introduction of programmable robots in the 1950s and mobile robots in the 1960s, and has continued with an increasing proliferation of robots being deployed (Brown, 2006).

The concept of a digital ecosystem originated in the early part of the 21st century, triggered by the European Commission-sponsored Go Digital initiative, whose aim was to boost the adoption of information and communication technologies (ICT) by European small and medium-sized enterprises as ICT was considered to be a major contributor to economic growth and efficiency (Nachira, Dini, & Nicolai, 2007).

Software-based agent research is generally accredited with beginning in the 1980s (Nwana & Ndumu, 1999). The goal in the development of agent-based software was to create software that could interoperate, that is, programs that could exchange information and services with other programs and thus together solve problems that neither could address individually (Genesereth & Ketchpel, 1994). The application programs that were developed consisted of software components that communicated with their peers, and communicated by exchanging messages in an agent-specific communication language (Genesereth & Ketchpel, 1994).

Several of the following topics are found to be applicable in defining a blockchain-enabled audit ecosystem and have been appended (in italics) to the concepts as presented in the initial research.

Troubleyn, Moerman, and Demeester (2013) present the requirements for a flexible Quality of Service Framework and these items also provide the attributes of an audit ecosystem:

- Adaptive: An audit ecosystem accommodates data from any number of sources and configurations structures.
  - *The focus of auditing needs to adapt from record tracing and verification to more complex analysis such as systemic evaluation, risk assessment, predictive audits, and fraud detection. The audit function would also need to provide an evaluation and examination of the design, creation, and execution of smart controls. Auditors should understand the codes in smart controls, and investigate the accuracy of program operation (Dai & Vasarhelyi, 2017).*
  - *A new audit paradigm would need to function over two environments: (1) a physical world, and (2) a mirror world, which is a virtual model that reflects business activities and conditions of objects in the physical world. The mirror world consists of three layers: blockchain, smart control, and payment. The blockchain layer is an ecosystem of blockchains, each of which would record a type of data that is needed for audits (Dai & Vasarhelyi, 2017).*
- Scalable: An audit ecosystem must accommodate varying database sizes due to client size and scope of audit, and may include big data.
  - *Enabling blockchain technology in large client systems will require development and implementation of larger storage systems (Dai & Vasarhelyi, 2017).*

- Distributed approach: To complete audit activities in a reasonable amount of time, the underlying activities must be decentralized so that the CA/CM agents can operate independently and undertake decision-making locally.
  - *The implementation of blockchain technology by large clients will depend on the development of not only larger storage systems, as noted above, but also wider bandwidth for data transmission, and a significant increase in computing power (Dai & Vasarhelyi, 2017).*
  - *Blockchain technology could support the auditing function by enabling the reconciliation of the related accounting entries, which are present on the books of each of the trading parties as the blockchain will provide the links between the relevant records (Fanning & Centers, 2016). To access records on numerous databases will likely require distributed processing capabilities to coincide with the data validation efforts in order to complete these tasks in a reasonable amount of time.*
- Support heterogeneity: Due to data variabilities in format and structure as well as various communication technologies and CA/CM agents with unique capabilities:
  - *The ability to store blockchain-related accounting records on the databases of all the trading partners will most likely include the use of various data formats and structures by each of the partners, possibly including big data scenarios.*

Barraca, Sadeghi, and Aguiar (2013) provide mobile robotics concepts that also support the design and function of an audit ecosystem:

- Policies (audit rules) will be continually updated and distributed so that all CA/CM agents have access to the latest versions. Rules may be altered as a result of specific data situations or anomalies encountered during the analysis.
  - *In presenting the concept of a DAO/DAC earlier, it was noted that the governance rules for business transactions will be embedded in smart contracts. Krahel (2012) recommends that most accounting standards should also be embedded into the infrastructure that will execute the recording process in a blockchain environment. As part of the audit CA/CM agents can verify that the accounting rules embedded in the smart contracts coincide with the published accounting pronouncements at the time of the transaction and flag situations where the rules do not coincide.*
- Collaborative and cooperative communication between CA/CM agents, especially when conducting multiple, related tests simultaneously which may be required when analyzing big data.
- Autonomous (autonomic) control loops allow for the coordination of simultaneous activities as may occur when analyzing big data.
  - *As noted above, storing blockchain-related accounting records on the databases of all the trading partners will most likely involve the use of various data formats and structures analogous to those found in big data scenarios.*
- Management mechanisms support CA/CM agents in completing their tasks while reacting to unpredicted events or data conditions.

- Distributed knowledge allows CA/CM agents to consider local rules as well as neighboring rules (for other CA/CM agents) which allows agents to act in coordination.
  - *Given a DAC/DAO scenario, governance rules for business transactions will be embedded in smart contracts, which the CA/CM agents can verify to each copy of blockchain data for a specific transaction, as well as providing assurance that the rules embedded in the smart contracts coincide with existing laws and/or accounting rules.*

Sacha et al. (2007) describe service oriented computing (SOC) as an example of collections of application-based services that communicate using formalized interfaces, defined data formats, and access protocols.

- *The blockchain-based accounting system as proposed will function as a permissioned blockchain in which only entities inside a company (e.g., its ERP system or accountants) can submit a transaction record to the blockchain ledger, with the verification function being restricted to accountants, management, and auditors (Dai & Vasarhelyi, 2017). An audit ecosystem can leverage the access protocol capabilities provided through SOC to validate if the transactions under audit were submitted by authorized agents using an accepted access protocol.*
- *The blockchain ledger can provide a reliable repository for audit-related documents. As this information is shared between the participants, that is, business partners, creditors, and government entities, for example, the role of providing assurance as to the validity of the documents can be expanded to include the participants who each maintain a copy of the documents (Dai & Vasarhelyi, 2017). An audit ecosystem's SOC capabilities can provide assurance that all of the participants acting in this capacity are accessing the documents through an appropriate access protocol.*

An audit ecosystem can incorporate the abilities of multi-agent systems (MAS) as presented by Briscoe and De Wilde (2009) as it is envisioned that multiple CA/CM agents will be interacting with the specific data under audit at a point in time, with each agent not only undertaking the specific audit tasks defined for it but also acting in concert with the other agents performing their specified audit functions in order to achieve greater goals than could be achieved individually.

- *A benefit of a blockchain-enabled infrastructure is the increased auditability of information. Since a blockchain ledger, as noted above, provides a secure repository for the data posted on it, it could also lend veracity to additional audit-related documents (Dai & Vasarhelyi, 2017). Using a MAS approach will allow an audit ecosystem's agents auditing specific transaction-related documentation interact with the agents simultaneously auditing related documentation to ensure the accuracy and comparability of the entirety of the documentation under audit.*
- *Automatic verification, processing, storing, and reporting of the information in the blockchain-based triple-entry accounting information system could together form a self-sufficient accounting ecosystem (Dai & Vasarhelyi, 2017). MAS in an audit*

ecosystem can simultaneously confirm the accuracy of the blockchain-based verification, processing, storing, and reporting functions.

The distributed resource protection mechanism described by Pranata, Skinner, and Athauda (2011) is relevant to audit ecosystem requirements that ensure only appropriate entities are able to access the resources (data and agents). Such a mechanism is also required to maintain the confidentiality and integrity of resources when audit ecosystem activities occur over an untrusted network.

- *As noted above in presenting the DAO/DAC concept, assigning authority to change the accounting and business rules imbedded in the smart controls is very important, as companies may manipulate these rules to gain illicit benefits (Dai & Vasarhelyi, 2017). Smart controls must rely on a governance process by which the users agree to the requirements for changing the programming code that provides the rules, as well as provisions for dispute resolution (Yermack, 2017). A distributed resource protection mechanism, as incorporated in an audit ecosystem, can authenticate that any changes were undertaken only by authorized parties that are involved in the verification process.*
- *Although the verification process for the transactions submitted to the blockchain will be automated by blockchain-provided technology, this process needs to be restricted to certain parties, such as accountants, management, and auditors (Dai & Vasarhelyi, 2017). A distributed resource protection mechanism incorporated in an audit ecosystem can provide assurance that only authorized parties have been involved in the verification process.*

Foon and Yen (2011) present a corporate knowledge ecosystem designed to create, utilize, and capitalize on knowledge resources can be used to provide storage of audit test criteria and evolutionary updates to those criteria.

- *In the discussion above that stated that most accounting standards should be embedded into the infrastructure that will execute the recording process in a blockchain environment, it has been noted that the laws and regulations to be automated must be "rule-based," as "principle-based" rules are difficult to automate (Krahel, 2012). Will the accounting discipline, especially in those countries that follow International Financial Reporting Standards (IFRS) principles-based rules, alter their accounting rules solely to support blockchain-based accounting, or will a mechanism need to be developed within blockchain that can accommodate principle-based rules? A corporate knowledge ecosystem concept might provide this capability to not only the blockchain accounting system but also an audit ecosystem that verifies that proper accounting rules were applied to the blockchain transactions.*

Papazoglou (2001) describes using software agent technology to allow for both a flexible design and usable e-business applications, and categorizes the agents to be incorporated in a multi-agent e-business environment based on functionality and competency. These agents are also applicable to an audit ecosystem:

- Application agents represent CA/CM agents that are specialized to a single area of expertise and work in cooperation with other agents to solve complex audit problems are but one example of the many application agents that encompass an audit ecosystem.
  - *Application agents can undertake the more complex analyses required of the audit function in a blockchain environment such as systemic evaluation, risk assessment, predictive audits, and fraud detection, as well as providing an evaluation and examination of the design, creation, and execution of smart controls (Dai & Vasarhelyi, 2017).*
- Personal (or interface) agents work directly with users, primarily client and provider staff, to help support the presentation, organization, requests, and information collections, such as providing user access to audit results.
- General business activity agents perform a large number of general support activities such as search agents that navigate effectively through fragmented online electronic information in order to provide guidance to the CA/CM agents.
  - Information brokering agents provide facilities such as locating information on Web sources or other agents that are required to solve a common problem, such as specialized agents to support CA/CM agents in addressing data anomalies, for example.
    - *As noted above, distributed databases are a reality as blockchain relies on multiple computers for both operation and maintenance. There will need to be a mechanism within the audit function to identify data anomalies between the various databases.*
  - Negotiation and contracting agents negotiate the terms of a business transaction as regards to exchange and payment, as is required when transacting for audit services.
    - *These agents could provide support to verifying the accuracy of the payment-related transactions of a blockchain-based business event.*
- System-level support agents provide objects with access not only to other application objects but also to such facilities as transaction processing when acquiring audit services.
  - Planning and scheduling agents: A multi-agent plan is formed that specifies the future actions and interactions for each agent. Typically, an agent may act as the group planner for a cluster of agents surrounding an application agent such as to support multiple CA/CM agents analyzing big data simultaneously, for example.
    - *Again, storing blockchain-related accounting records on the databases of all the trading partners will most likely involve the use of various data formats and structures analogous to those found in big data scenarios.*
  - Interoperation agents: Audit processes may require accessing information from legacy systems with unique data formats, and also engaging CA/CM agents from different providers that may each require specific communication protocols.
  - Business transaction agents: Can be used to determine new CA/CM product offerings to incorporate in the audit ecosystem.

– Security agents: Provide security measures for information, communications, and data to/from the audit ecosystem (Based on Papazoglou, 2001).

One area where technology can provide significant leverage in supporting a blockchain-enabled audit ecosystem is in the use of application agents to undertake many of the tasks required to audit blockchain accounting records. The potential uses of application agents in a blockchain-enabled ecosystem are described in more detail. Given the distributed nature of blockchain data, application agents can substantiate the controls and security over the public and other distributed databases that hold the blockchain data. Application agents can also verify the consistency of the data between the blockchain environment, the double-entry system, the tokens, the smart contracts, and the payment records, for example. Regarding smart contracts, application agents can also provide the means to evaluate the design, creation, and execution of smart controls (Dai & Vasarhelyi, 2017).

Application agents can document and confirm the governance rules and decision-making processes embedded in the smart contracts that govern the blockchain business events. Dai and Vasarhelyi (2017) propose that the audit function in a blockchain environment will need to include complex analytics, such as systemic evaluations, risk assessments, predictive audits, and fraud detection, all of which can be supported by application agents.

Application agents can test the consistency, that is, reconcile the accounting records on each of the trading partner's books, as well as the links between them. Application agents will be able to provide the technologies to undertake the distributed processing activities that will be required in order to conduct audits over the large expanse of the blockchain environment in a reasonable timeframe.

A blockchain audit requirement that application agents can support will be the certification that only authorized agents have submitted transactions, and they undertook this using accepted access protocols. Similarly, application agents will be enlisted to validate that the participants have accessed the relevant documents through an authorized protocol.

Since blockchain-related accounting records will be stored on the databases of all the trading partners, this will very likely involve the use of various data formats and structures by each of the partners, and application agents can provide the technologies to reconcile these varied data formats in order to provide consistency in comparison of the data records.

The capabilities of application agents acting in a blockchain-enabled environment are presented in Figure 1.

Having described the characteristics of an audit ecosystem, these characteristics, including attributes, features, and software agents are diagramed in Figure 2.

The external influences (participants) to an audit ecosystem are identified for this research as auditor, auditee, auditee data, audit standards, and audit analytic results/outputs. These represent the participants that are included in the traditional audit with its focuses on a single client, a single audit firm conducting the audit, the data that is the subject of the audit, which may originate from numerous sources in a blockchain environment, and the results of the audit activity.

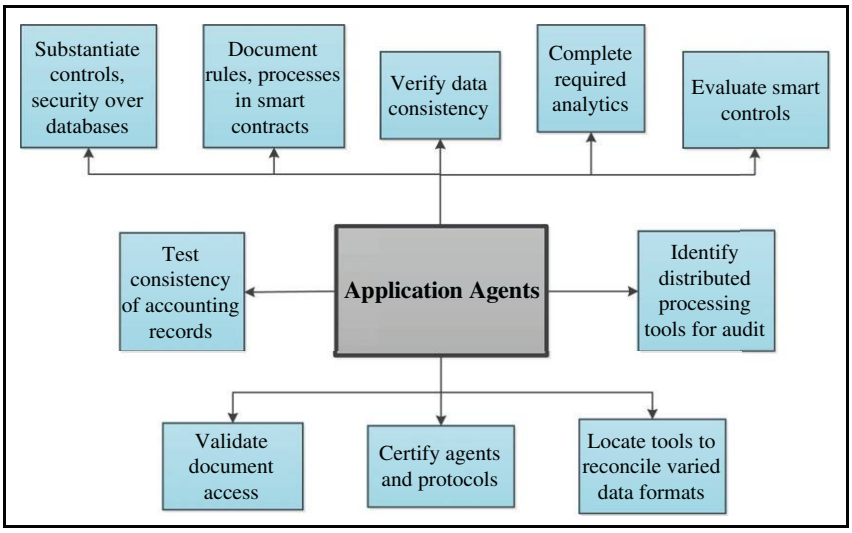

Figure 1: Application Agent Examples.

An audit ecosystem supports the automated CA/CM tools that replace manual auditor activities with automated procedures that not only provide capabilities beyond that afforded by manual procedures, such as an audit of all the data and not just selected items, but also in a much more efficient manner. Given that technology is driving the new audit process, inputs are provided in a digital format: the data must be available in a machine-readable format, and the resultant audit findings from the CA/CM tools are provided in a digital format. Most importantly, the inputs, referred to as auditee profile, auditor profile, and audit standards, drive the selection of audit apps that are appropriate with the current situation. In a blockchain-enabled accounting environment the audit function will likely require concurrent auditing of not only the primary audit client but also all blockchain participants. An audit ecosystem approach can accommodate incorporating multiple auditee profiles as inputs.

These audit app selections are made via an audit app recommender system (Dai, Krahel, & Vasarhelyi, 2014). An audit ecosystem will manage changes to these external elements as they evolve over time, primarily to accommodate new and enhanced audit apps but to also accommodate changes to auditee and auditor profile information, audit standards, and auditee data. Audit standards may also be incorporated into blockchain data, in the smart contracts. By accessing accounting standards via two independent means, an audit ecosystem can include agents specifically tasked to confirm consistency between the actual pronouncements and those included in the smart contracts. This information is presented in Figure 3.

Figure 3 also depicts the software agents that are incorporated in an audit ecosystem. General business agents, and in particular agents that undertake the negotiations for CA/CM agents, support the recommender system. Similarly, business transaction

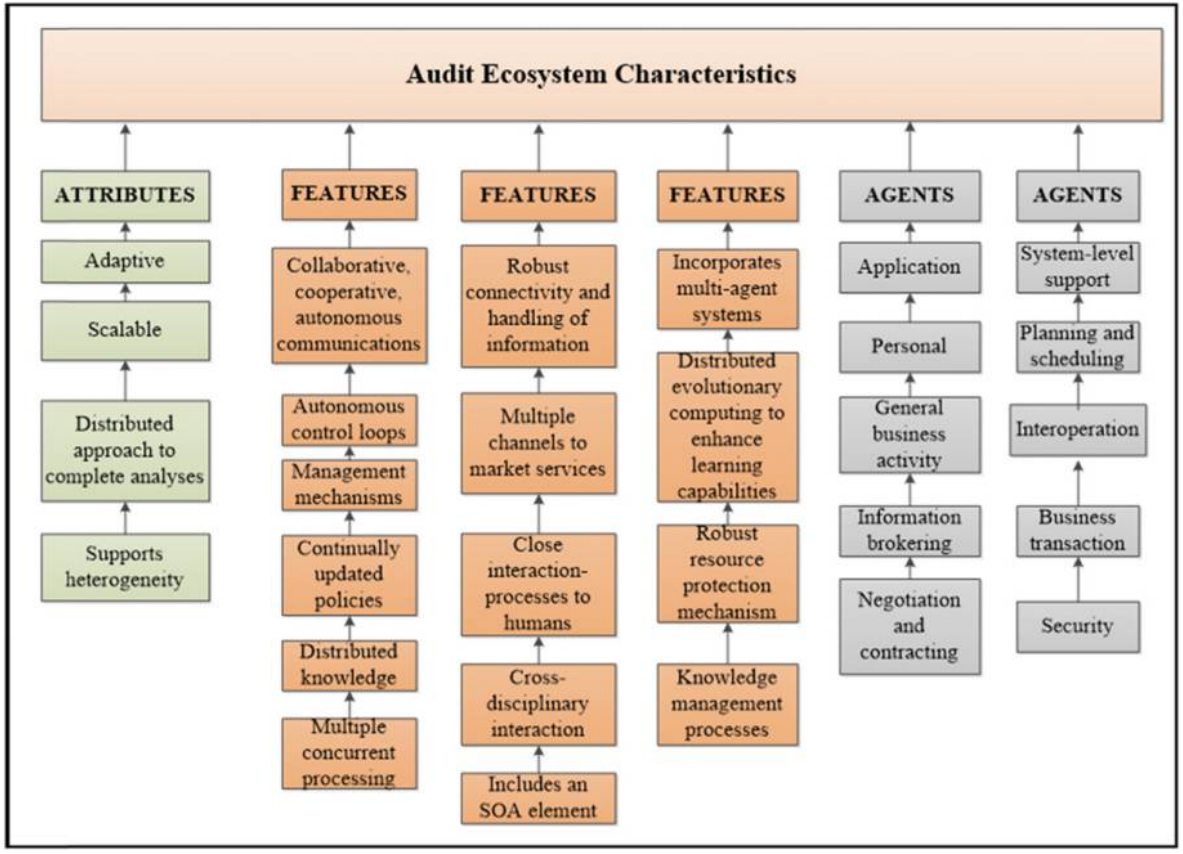

Figure 2: Audit Ecosystem Characteristics.

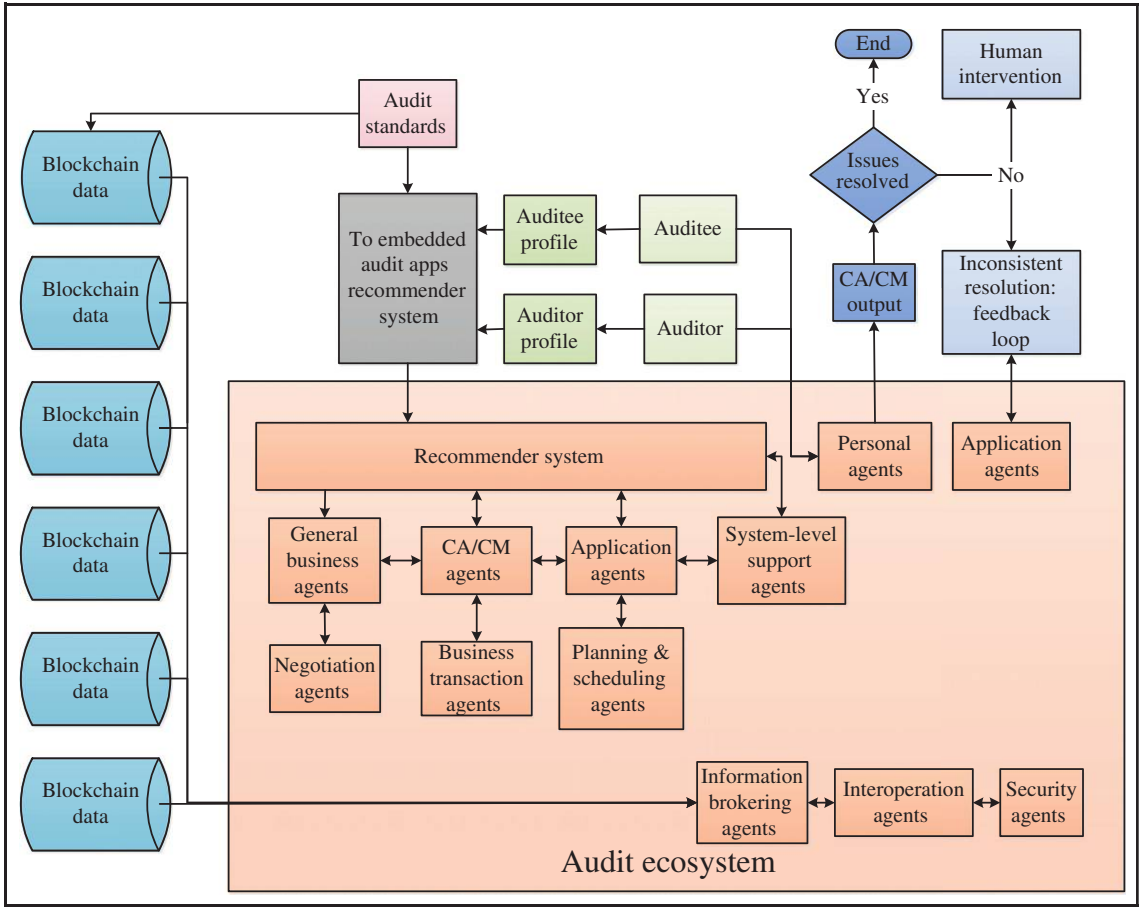

Figure 3: External Influences.

agents support the acquiring and deploying of CA/CM agents as identified by the recommender system. Application agents (see Figure 1), planning and scheduling agents, and system-level support agents support the operation of the CA/CM agents. Application agents also support the issue resolution process. Personal agents support the auditor and auditee participants and the presentation of the results of the CA/CM activities for these participants. Information brokering agents and interoperation agents locate information as required with respect to the identification of auditee data and its characteristics. Security agents act to protect the auditee data from incursion during the transmittal process from auditee to audit ecosystem.

Conclusion

Blockchain technology has emerged as one of the several contemporary technologies that has the potential to significantly alter business processes, and in particular the accounting and assurance functions (Dai & Vasarhelyi, 2017). The design, implementation, and use of blockchain in accounting, and the specific technologies included, have yet to be defined. Blockchain is viewed favorably as it enables a decentralized public ledger that provides a secure transactional platform for use among unfamiliar parties without a central authority (Dai & Vasarhelyi, 2017). One would hope the robustness required to support required functions would be embedded into the resultant blockchain-enabled accounting application. However, where some light and scalable blockchains have already been tested, the security models on which those functions rely may not be robust enough for accounting applications (Dai & Vasarhelyi, 2017). More robust audit functions will be required to identify any security weaknesses.

A significant shift in the technologies underlying automated accounting systems will require a similarly significant change in the tools that perform the audit and assurance functions over these accounting systems. The development of CA/CM tools is one of few instances where a significant innovation in accounting practice has been driven by the academic community (Alles, Kogan, & Vasarhelyi, 2008). Academic researchers continue to play an important role in CA/CM development. Academic researchers who create a conceptual model of CA/CM ensure that it becomes a true audit methodology, and not simply a collection of disparate technologies.

As noted by Alles et al. (2008), academic researchers can conduct innovative implementations without facing the challenges practitioners will have as they turn to CA/CM for the process of reengineering the audit practice. The development of a blockchain-capable audit ecosystem is the natural progression in the deployment of computer-based CA/CM tools, and as with earlier CA/CM development efforts this activity is preferably undertaken in the academic community.

Perhaps with the onset of blockchain technology that is changing the accounting function, the time is appropriate for the audit function to embrace an audit ecosystem approach, as presented in this and other academic articles, in order to be able to provide assurance over a blockchain-enabled accounting function.

The information presented in this research expands on the use of an audit ecosystem as a tool to not only support the current technology-driven accounting environment but also discusses how an audit ecosystem's features and functions can be leveraged to provide a robust audit function over the blockchain-enabled accounting systems being developed for use in the not-too-distant future.

References

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems*, *22*(2), 195–214.

Barraca, J. P., Sadeghi, R., & Aguiar, R. L. (2013). Collaborative relaying strategies in autonomic management of mobile robotics. *Wireless Personal Communications*, *70*, 1077–1096.

Briscoe, G., & De Wilde, P. (2009). Computing of applied digital ecosystems. In *Proceedings of the international conference on management of emergent digital ecosystems*, October, ACM, p. 5.

Brown, A. (2006). The robotic economy. *Futurist*, July/August, *40*(4), 50–55.

Dai, J., Krahel, J. P., & Vasarhelyi, M. (2014). *Which audit app(s) should auditors use? An exploratory study of using recommender systems for audit app selection*. Rutgers Working Paper.

Dai, J., & Vasarhelyi, M. A. (2017). Towards blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3).

Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, *27*(5), 53–57.

Foon, L. S., & Yen, T. F. (2011). Creating and developing a corporate knowledge ecosystem. *Annual summit on business and entrepreneurial studies (ASBES 2011) proceeding 486*. 17–18 October 2011, Grand Margherita Hotel Kuching, Sarawak, Malaysia.

Genesereth, M. R., & Ketchpel, S. P. (1994). Software agents. *Communications of ACM*, *37*(7), 48–53.

Kozlowski, S., & Vasarhelyi, M. A. (2014). *An audit ecosystem: A starting point with definitions, attributes and agents*. Working paper. Newark, NJ: Rutgers Business School.

Krahel, J. P. (2012). *On the formalization of accounting standards*. PhD dissertation, Rutgers, The State University of New Jersey.

Nachira, F., Dini, P., & Nicolai, A. (2007). *A network of digital business ecosystems for Europe: Roots, processes and perspectives*. Introductory Paper. European Commission, Bruxelles..

Nwana, H. S., & Ndumu, D. T. (1999). A perspective on software agents research. *The Knowledge Engineering Review*, *14*(2), 125–142.

Papazoglou, M. P. (April 2001). Agent-oriented technology in support of E-business enabling the development of "Intelligent" business agents for adaptive, reusable software. *Communications of the ACM*, *44*(4), 71–77.

Pranata, I., Skinner, G., & Athauda, R. (2011). A community based authentication and authorisation mechanism for digital ecosystem. *5th IEEE international conference on digital ecosystems and technologies (IEEE DEST 2011)*, 31 May–3 June 2011, Daejeon, Korea.

Sacha, J., Biskupski, B., Dahlem, D., Cunningham, R., Dowling, J., & Meier, R. (2007). A service-oriented peer-to-peer architecture for a digital ecosystem. *2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2007)*. 21–23 February 2007, Cairns, Australia.

Troubleyn, E., Moerman, I., & Demeester, P. (2013). QoS challenges in wireless sensor networked robotics. *Wireless Personal Communications*, *70*, 1059–1075.

Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. *Auditing-A Journal of Practice & Theory*, *10*(1), 110–125.

Weiner, N. (1948). *Cybernetics; or control and communication in the animal and the machine* (pp. 194). Oxford: John Wiley.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, *21*(1), 7–31.

Zuiderwijk, A., Janssen, M., & Davis, C. (2014). Innovation with open data: Essential elements of open data ecosystems. *Information Polity*, *19*(1, 2), 17–33.