Creating Assurance in Blockchain

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Blockchain—a distributed ledger technology that underpins bitcoin and is also being tested by a variety of companies to track ownership of assets without a central authority—is everywhere. Supporters claim it to be everything from a panacea for the high overhead costs associated with financial services back-office functions to the future of how money—and other transactions—will get processed. To describe blockchain as a solution in search of a problem, critics have cited a lack of successful production deployments; the challenges associated with audit, taxes and compliance; and a sketchy regulatory picture. As is often the case, the truth about the usefulness of blockchain likely lies somewhere in between, but what is indisputable is that the audit problem is holding up more extensive commercial deployments.

"Audit problem" is not necessarily a recognized industry term, but it is how this author describes the problems and challenges associated with actively deploying live blockchain instances. Use of the "audit problem" terminology is based on seeing more proofs of concept (POCs) than one can imagine being held up just before deployment because some combination of internal and external audit, compliance, risk, and legal is asking the ultimate question: Is there proof that it is working safely and securely? Countless POCs are ready to go live right now, but will not go live because companies are struggling with how to deal with the assurance needs of the control organizations. It is not a surprise that in most cases, audit and assurance were not top of mind during development, and when companies start to consider them, they confront the challenge of how to meet the expectations of those control groups.

亦有中文简体译本
www.isaca.org/currentissue

Now, to be clear, it is not that blockchain cannot be audited; it is that the way of thinking about audit and the overall concept of transaction assurance must, of necessity, be different. Before delving into assurance, though, it is important to revisit blockchain at a high level to begin to understand what is causing the challenge. Most blockchain POCs are designed to achieve benefits that fall loosely into one of three categories: reduce costs and create process efficiencies, create an ecosystem with higher-than-standard levels of trust, or facilitate digital currency exchange. Other slightly different classification schemes may exist, but they are immaterial for the purposes of this discussion.

What is important is that, regardless of classification, trust and efficiency are the main value drivers for any use case. So, in essence, a certain key aspect of assurance is derived from the technology itself, and that aspect is trust. Additionally, that outcome is achieved through a method that leads to reductions of processes, intermediaries and the like. So if the technology itself produces the essence of assurance, how can that benefit be maximized without adding back in

A. Michael Smith
Has more than 25 years of experience in IT auditing, cybersecurity, privacy and regulatory requirements in the IT space. He is responsible for PricewaterhouseCooper's IT internal auditing services practice in the US for financial services companies, and he has led projects in all financial services sectors. His primary area of focus is designing strategies for deploying technology audit in large financial services organizations. Prior to joining PwC, Smith was the global director of technology audit for the Bank of New York Mellon.

many additional layers of administration in an effort to "prove" it?

To take that idea a step further, the technology also creates an irrefutable transaction record and irrefutable transaction integrity. Those are two more of the characteristics of assurance that are traditionally produced by the audit process—meaning that in the absence of blockchain, the integrity of a transaction's historical record and the validity of the transaction itself come from extensive processes and controls. In financial services, this might occur via administration-heavy activities such as corporate trust, asset servicing and global custody; however, in any industry, there might be such controls as reconciliations, confirmations, identity and access management. It is important to remember that this represents just the first step in the assurance process, because those processes and controls have to be "proven" by audit, which traditionally is performed in the form of forensic, point-in-time analysis (by sample) of historical transaction activity. Once that has been completed satisfactorily, the concept of assurance has been created, which enables the use of the data for purposes of tax reporting, compliance reporting, risk analysis and so on.

The fact that blockchain technology creates this concept of assurance by its nature significantly reduces the need for those processes and controls. However, it is still necessary to prove that it is, in fact, creating the needed assurance, and optics—or transparency into the technology—are needed to demonstrate that it is. This is where one can begin to see the need to transform the way of thinking about audit and assurance: Instead of creating assurance through a burdensome administrative process, it is possible to now prove assurance and provide transparency to reflect it. Some might view that as a challenge, but it is, rather, an opportunity to fully embed audit and assurance into technology and make them by-products of each transaction's inherent nature.

In other words, to enable assurance on a blockchain instance, one must begin with the technology itself. An exhaustive assessment of the underlying cryptography, key management and security around the blockchain engine is the recommended first step. The actual nature and extent of the procedures to be performed will be determined by the characteristics of the business use case, the needs of the anticipated assurance-related stakeholders (e.g., internal audit, tax, compliance), and the version of blockchain being used.

That is an important point to make with regard to what blockchain really is. The term "blockchain" refers to a form of applied cryptography that is open-sourced and available to anyone. Because that is the case, there are many blockchain vendors, each of which has unique performance characteristics and add-ons (some even have reporting capabilities), which underscores the importance of understanding that what is being solved is a change in philosophy and not a specific, one-size-fits-all solution. Once it has been confirmed that the technology is functioning as intended, it is then a simple matter of creating the necessary reporting to meet stakeholders' transparency and optics expectations.

"The term 'blockchain' refers to a form of applied cryptography that is open-sourced and available to anyone."

Ongoing review to ensure the sustainability of the assurance solution will also be necessary, but the nature, timing and extent of that review work will again be determined by the technology used, the business-use case and the evolving ecosystem in which the instance is deployed. There are also fantastic opportunities for audit to provide add-on value once transaction-level assurance has been confirmed and implemented. The reason is that doing it properly requires a higher-than-average understanding of the overall business process or processes that affect the individual-use case for

the technology itself. Now that they have become freed from having to perform labor-intensive forensic analysis, those in audit can focus on broader process issues and business efficiency issues; they will also be closer to changes in the blockchain deployment as both its use and the business case evolve over time. That evolution will facilitate a nimbler and more strategic approach to audit, which, in turn, will lead to more value for the organization.

Conclusion

As previously noted, where blockchain will end up is anyone's guess, but from an audit perspective, it is a great opportunity to start embracing the evolving concept of real-time, or continuous, auditing. Many factors are already directing the profession in that direction, not the least of which are transaction volume and increased reliance on technology. However, in this case, the technology itself mandates such an approach. The faster that technology evolves and the more rapid development and higher levels of automation (e.g., robotic process automation) are embraced, the more the pressure on audit to evolve will increase dramatically. By adopting the mind-set and following the concepts outlined in this article, the audit function will be well prepared to begin its journey toward becoming truly strategic and best-in-breed—and more than ready to deal with blockchain, at whatever its stage of evolution.