www.pwc.com

Governance in the Age of Blockchain Distributed Ledger Technology

Table of contents

Introduction 1

Governance in the age of Blockchain 2

Blockchain environments 4

Implications for risk functions 5

PwC Blockchain risk and controls framework 6

Summary 9

Contact us 10

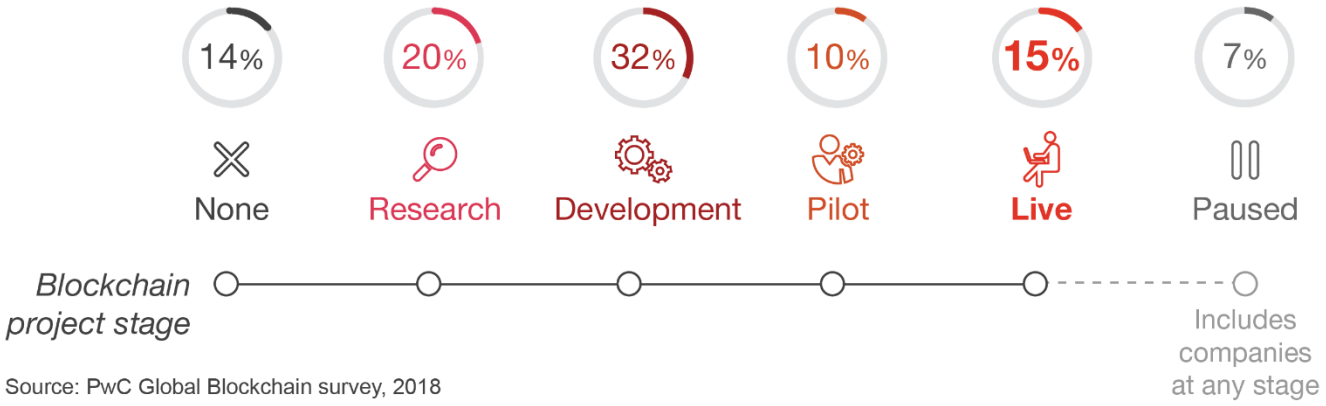
Introduction

Blockchain is an exciting and dynamic technology that promises to enhance, transform — and, yes, disrupt — industry. In fact, it's one of what we at PwC refer to as the "Essential Eight" among more than 150 emerging technologies we expect to make significant global impact.

Blockchain has rapidly grown from curiosity to investment. In PwC's recent Global Blockchain Survey of 600 business and technology leaders in 15 countries, over half reported blockchain R&D in progress and 15 percent noted live blockchain implementations.

As all risk and governance professionals know, any new technology has trust implications. blockchain is no different. In this paper, we explore how our profession is evolving to accommodate emerging technologies and share our perspective on a risk and controls framework that can help enable crucial governance and validation while establishing trust in blockchain business applications.

How Far Along are Companies with Blockchain?



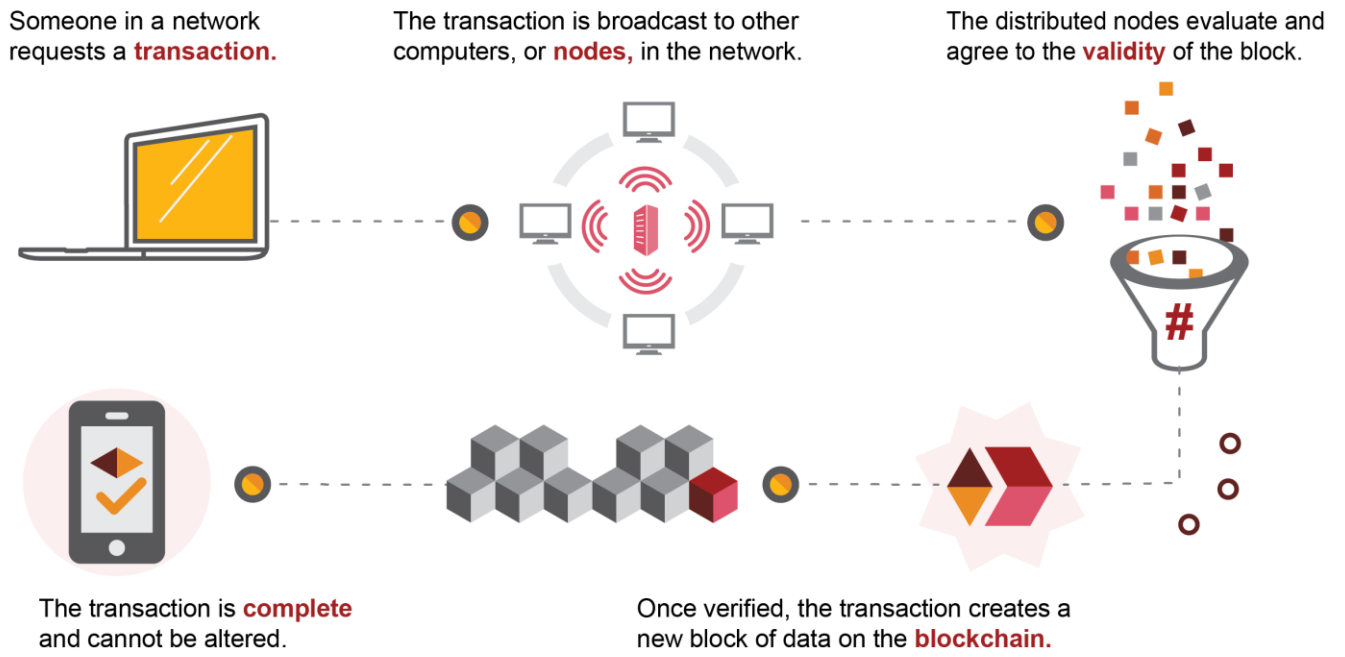
Source: PwC Global Blockchain survey, 2018

Governance in the age of Blockchain

Blockchain applications have gone live in some organizations. But before companies can deploy blockchain applications at scale, they will have to learn to navigate a new world of digital risk. One little-talked-about but critical factor in blockchain's widespread adoption is governance — and bridging the gap among innovators, technologists, regulators, business leaders, and governance teams remains a challenge. Enterprises need a comprehensive controls framework for blockchain to ensure their deployments will meet governance, risk management, and controls requirements.

How blockchain works

Blockchain is a data structure that uses a distributed system of databases (called "ledgers") instead of a traditional central database. Everyone in a blockchain network is considered a "node," and each has a copy of the ledger. All nodes are connected via peer-to-peer networks and everyone checks each other for consistency. Each individual use case determines the ledger's records (or "blocks"), which are "immutable," meaning that blocks cannot be changed once verified and added to the chain. Many types of transactions can be conducted and confirmed on a blockchain.



Take, for example, blockchain used to manage a supply chain. In pre-blockchain supply chains, products are tracked using a patchwork of barcodes, radio frequency identification (RFID) tags, and relational databases that must be constantly checked and updated. This method was groundbreaking a decade ago, but it looks primitive next to the capabilities that blockchain-based solutions could bring. Today's inventories are managed by periodic spot checks, manual counts, and other time-consuming, error-prone methods. When products and services come together in a region with a complex tax structure, such as Europe's VAT system, managing the supply chain and ensuring compliance becomes even more complicated — and the chances of inventory mistakes and financial errors increase.

With blockchain, tracking and monitoring raw materials as they go into production becomes easier and more accurate. A new record (block) is created in the blockchain ledger for each new piece of raw material. This block can track the source, price, location of the item, quality, and any other identifying information. As the item works its way through the production process and becomes part of a finished product, new blocks are created that accounts for these changes.

When you combine a blockchain-based supply chain management system and high-performance computing tools that can analyze all the data quickly, everyone in the process, including producers, vendors, and customers, can have visibility into the product at every point in the production process — from raw materials and production to distribution and retail. This makes it easy not only to track and measure inventory, but also to calculate taxes, initiate product recall processes, and so on. Lifecycle management becomes easier and more accurate.

One of blockchain's key features is that the ledger is both distributed *and* shared — in this case among the various parties in the supply chain. Both the producer and the receiver of an item share access, and are thus kept up-to-date on the location and condition of any product in real-time, allowing for more accurate business decision making. Every record in the blockchain is cryptographically linked with the one prior. Information recorded in the chain can never be altered (even by a system administrator), significantly reducing the possibility of fraud. This becomes crucial in cases where raw materials are especially susceptible to counterfeiting. blockchain ultimately gives manufacturers a higher level of confidence in the origin, authenticity and quality of their products.

Supply chain is just one example of many potential blockchain use cases. Companies are exploring its use for settling financial transactions, managing real estate and land registrations, ensuring the reliability and completeness of healthcare records, and developing self-executing legal documents called "smart contracts" that could be managed without third-party oversight. No matter the use case, however, governance challenges are consistent.

Blockchain environments

Before we dive into blockchain governance, it's also useful to understand the environment that the blockchain will operate in. In general, there are three types of blockchain implementations, each of which impacts governance and control.

Blockchain Implementation Types

Governance and control environment responsibility

Permissionless

Anyone can participate. Operated and administered by community

Community

Federated Blockchains

Used, operated and administered by multiple participants under a consortium leadership

Shared among multiparty

Private Blockchains

Used, operated, and administered by a single entity

Centralized party

1. **Permissionless:** This is an open blockchain network that anyone can join and participate in. The community operates and administers the blockchain, and one or more participants can provide consensus. Any user can join a permissionless network, i.e., exchanging digital currency on a public currency exchange.
2. **Federated (Permissioned):** Since this blockchain model requires permission to join, read, write to, operate and administer, it's also called "permissioned." Multiple participants administer the blockchain under consortium or group leadership. There may be restrictions on how participants can contribute to the system state or consensus of transactions.
3. **Private:** In a private blockchain, only a centralized entity or single participant has permission to write to the blockchain. Platform architects must decide how to assign permissions to participants based on certain criteria.

Today, as companies begin to embrace blockchain, most start with permissioned or private blockchains, where they know all of the participants and can better manage the rollout of new emerging technology-based applications. Their governance approach needs to be tailored accordingly - something that is more manageable given they are working with known trading partners. As they grow into public, permissionless blockchains, the governance model can evolve to address the new risks that are more specific to working with anonymous partners.

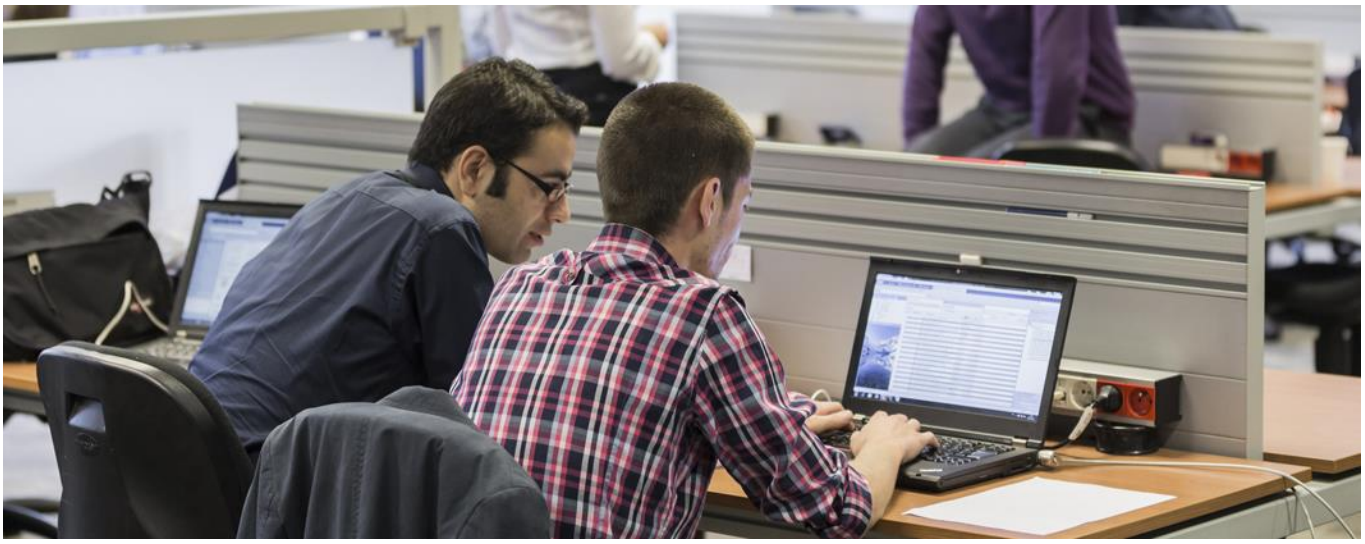
Implications for risk functions

Our blockchain-enabled supply chain might sound like an executive's dream come true. But it's an uncharted way of doing business that will bring new challenges. Primarily, issues revolve around the fact that blockchain was never designed with an audit trail or control environment in mind — it was built as a pure technology solution. As a result, enterprises have to build in governance if they want to validate blockchain applications from a risk management point of view. There is a common misperception that immutability of the blockchain means there is no need for governance or internal audit. This is not true. The blockchain itself may be sound, but the entire workflow that runs on top of the blockchain still requires governance and validation just like any other business process. There are several variants of blockchain technology that organizations can chose to enable a specific use case, which will dictate the platform, protocol, consensus and encryption mechanisms that each have a distinct set of risks.

Traditional audit approaches don't work with blockchain. Why? blockchain does not lend itself to point-in-time, retrospective, sample-based analysis. Applying these traditional audit approaches to blockchain applications requires an exponential increase of both resources and time, simply because "crawling" through the distributed chain of information would be tremendously tedious. In addition, the exponential increase in transaction volume blockchain enables renders a traditional sample-based analysis ineffective and impractical. Lastly, it is necessary to audit blockchain to validate the technology's strengths and whether it is functioning as intended.

We see three key issues that impact governance for blockchain applications: transparency, risk, and controls. One or all of these issues could stall your blockchain innovation efforts. There is neither work-flow **transparency** nor a standard audit trail in a blockchain. From a **risk** perspective, no industry or enterprise consortium has widely explored or adopted a framework for evaluating risk. And, when considering **controls,** lack of knowledge of the technology creates a skills gap that may lead some to believe that auditing a blockchain environment is impossible.

PwC has a spent a lot of time considering how to address these challenges. We believe blockchain governance can only be achieved through continuous audit using a risk framework specifically designed for blockchain.

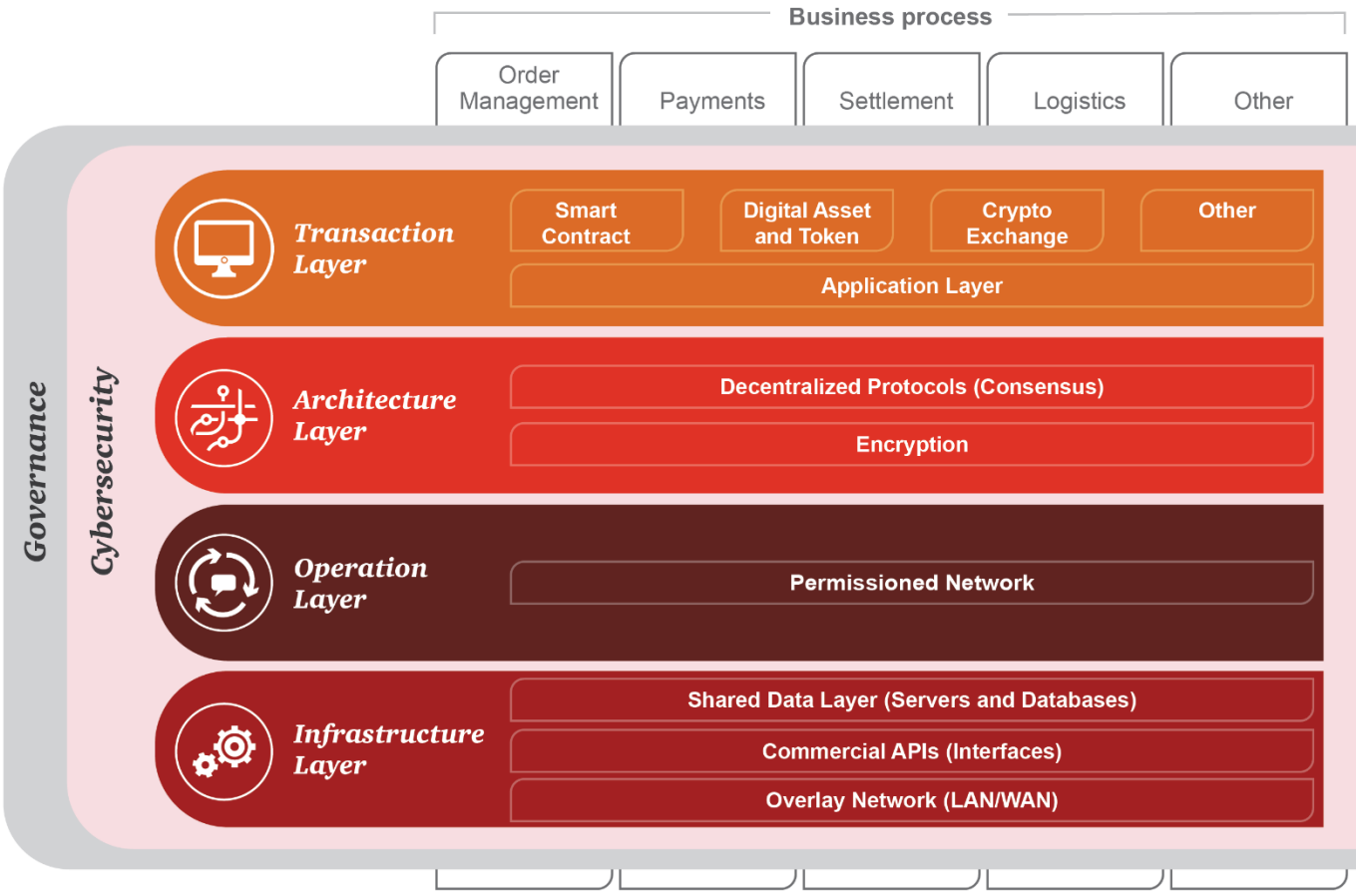


PwC Blockchain risk and controls framework

We designed a Blockchain Risk and Controls Framework to help address risk expectations across three lines of defense: operations, enterprise risk management, and internal audit. The framework aligns with blockchain technology stacks to help companies evaluate risk position and monitor and communicate effectively, keeping stakeholders – including executive boards and risk, audit, operational, and other committees – informed, engaged, and confident. The framework can be applied across all industries, blockchain implementation type, or transformation phase.

The framework identifies six risk domains with supporting subcategories that outline blockchain system considerations in light of best practices and any applicable internal and external stakeholders' requirements. It addresses overarching governance and cybersecurity concerns, illustrating the need to assess any blockchain implementation in context with the rest of the enterprise.

PwC Blockchain Risk and Controls Framework



The following describes each domain, including considerations that should be addressed in each:

- **Governance & oversight:** Explore the blockchain technology best suited to your needs. Agree on why blockchain fits the use case, and how you will establish a control environment and achieve governance.
- **Cybersecurity:** Consider how to address participants' data security and privacy needs. How will cyber threats be detected, managed, and contained?
- **Infrastructure layer:** Evaluate risks associated with core components of the environment in which your blockchain will operate. How will you scale supporting infrastructure? Can you effectively protect interfaces and APIs?
- **Architecture layer:** Focus on risks specific to the blockchain technology you're using. For example, how will you define and achieve consensus? What type of encryption will you use? Will it scale?
- **Operational layer:** Introducing additional parties or users can introduce new operational risks. How will participants be invited, onboarded, managed, and retired on your blockchain network?
- **Transactional layer:** You may deploy decentralized applications (dApps) on your blockchain to enable select business processes. How will you assess the dApp-enabled workflow, validate transaction procedures and address any relevant regulatory requirements?

Taken together, these six areas form a foundation that can support the strategic development, design, build, and implementation of blockchain use cases.

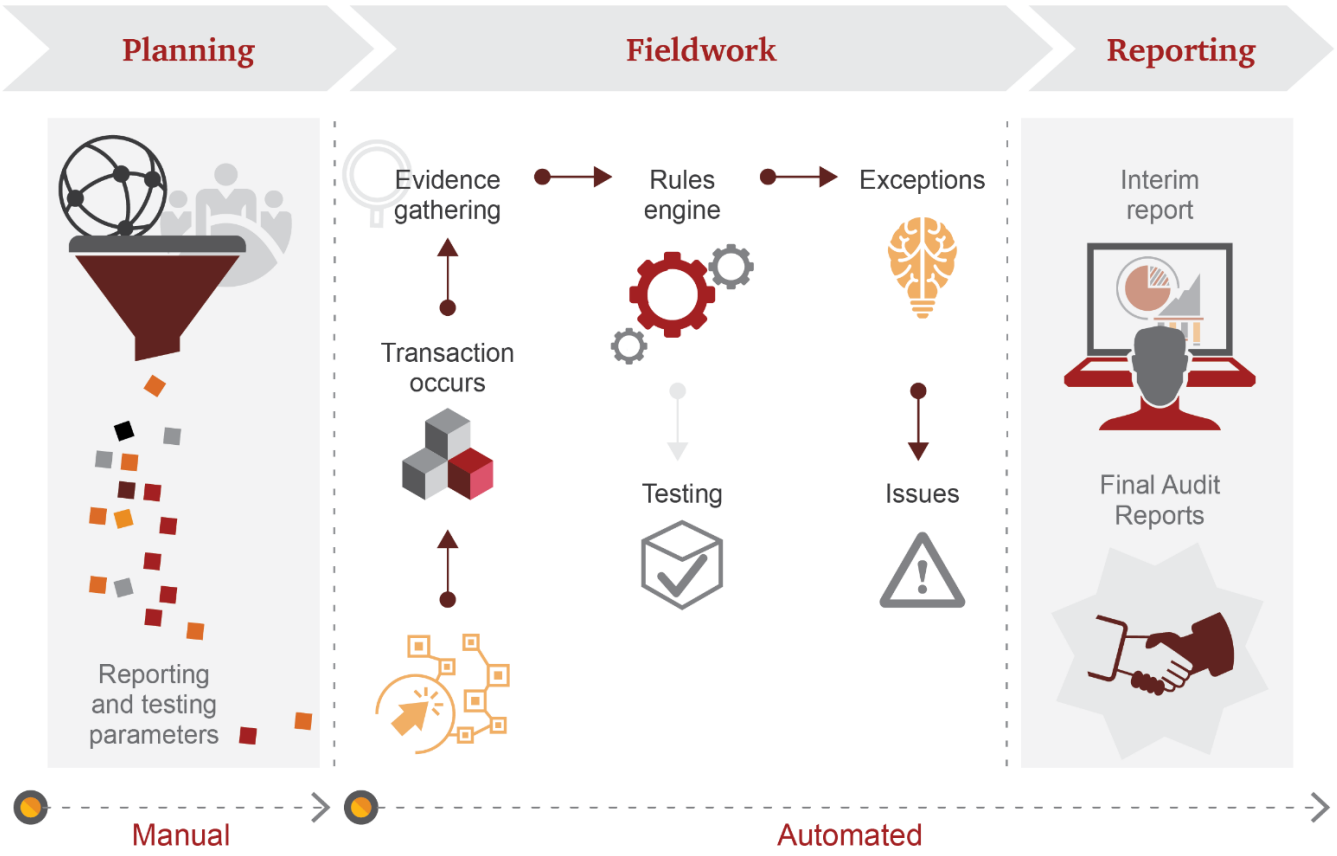
Blockchain in practice – Digital continuous audit

In the past, traditional audit techniques have been used widely to validate business processes and instill confidence and trust. For years, auditors have managed risk and offered opinions on internal controls based on manual, point-in-time (typically annual), sample-based auditing techniques. As technology has progressed, computer-assisted audit technologies have improved audit efficiency. With continued advancement, new approaches have emerged to improve the process further, allowing auditors to review a full population of data continuously. We see industry continuing to move toward continuous audit, a real-time auditing technique that relies on machines to monitor and test for anomalies in the transactional flow and provide a mechanism to report and issue opinions on processes and subprocesses. The combination of continuous audit with a blockchain risk and controls framework is moving us toward digital continuous audit, which will provide unlimited potential to manage risk and ensure governance.

Our approach to continuous blockchain audit and monitoring is designed to help manage risk in real time. This is particularly important in light of the scale of transactions that blockchain enables. It establishes a proper governance model that can ultimately be automated to build continuous trust.

Providing transparency in a blockchain requires a fundamental shift in how we think about audit and control. It must go from retrospective (forensic, point-in-time) efforts to real-time auditing where the underlying foundations of audit and control become embedded in each discrete transaction.

A Continuous Auditing Approach for Blockchain



We advocate a continuous auditing methodology for blockchain, comprised of the following key activities:

- **Planning:** During planning, assess the overall blockchain system and control environment relative to all stakeholders' needs using the framework described above. This assessment will help establish the scope of the continuous audit by aligning the controls to each of the framework categories, including the frequency, approach, and testing method. Define testing and reporting parameters for continuous testing and reporting at the workflow and process level to validate transactions as they occur.
- **Fieldwork:** Once the system is operationalized and deployed, transactional information must be sent through a rules engine that hosts and applies the test procedures as transactions are occurring in a continuous fashion. Testing results are classified into either observations or passed categories. The auditor uses continuous audit workflows to further classify observations as either an exception/deviation or no exception/deviation. For the exceptions noted, the auditor uses another set of workflows to raise an issue.
- **Reporting:** Once the audit testing and other fieldwork activities are concluded, the auditor can produce an interim audit report that includes rating and details at the process and Subprocess level to achieve continuous reporting and monitoring, depending on the desired cadence. After the interim reporting cycle is complete, the auditor produces a final audit report that includes ratings and opinions at the process and subprocess levels.

Continuous auditing practices applied within our ***Blockchain Risk and Controls Framework*** can help establish robust governance for blockchain and achieve significant increases in efficiency, effectiveness and levels of confidence.

Summary

Blockchain is coming. In fact, in a growing number of industries, blockchain is already here. As blockchain matures and even more creative uses of the technology emerge, the issue of governance and trust comes to the forefront. To establish an effective, efficient governance model for blockchain, implement an audit methodology and framework, often with supporting continuous audit software, specifically designed for this groundbreaking technology. We designed the PwC blockchain Risk and Controls Framework with this in mind.

To learn more about PwC's Blockchain Validation Solution, visit www.pwc.com/blockchain-validation.

Related content:

- Understanding blockchain risks, controls and validation
- Confidence in the future: How tomorrow's technologies can help the finance function of today
- Building blocks: How financial services can create trust in blockchain

Contact us

Chris Curran
New Ventures, Chief Technologist
214-754-5055
chris.curran@pwc.com

George Galindo
Partner, Risk Assurance
713-296-0315
george.a.galindo@pwc.com

A. Michael Smith
Partner, Blockchain Assurance Leader
646-471-9580
a.michael.smith@pwc.com

Emad Khan
Internal Audit, Compliance & Risk Management Solutions (ICRS)
646-335-4412
emad.khan@pwc.com

Charlie Latch
New Ventures, Business Development
214-616-3281
charlie.latch@pwc.com