COSMOS
Navigate the Compliance Universe

CEP Magazine - May 2019
Blockchain's compliance potential

By Jacqueline and Tony Niderost

Jacqueline Niderost (jacquedn@gmail.com) is a strategic advisor for Gerson Lehrman Group in Phoenix, Arizona, USA. **Tony Niderost** (tony@niderost.org) is a technical adviser and subject matter expert to investment firms and is based in Scottsdale, Arizona, USA.

By now many people have heard of blockchain, but not everyone knows what it is, even though it is the big buzzword these days. It may seem complicated, and I'm sure the technical implementation details are. However, from a brass tacks perspective, rest assured it is not an insurmountable concept to grasp. In fact, think of it as nothing more than a transaction ledger that happens to be tamper-proof, with multiple copies that ensure the majority of others holding their copy of the ledger agree it is correct and the source of truth.

In case you lose your copy of the ledger, you can just grab one of the copies and make yourself another copy of your own. They are always all up to date with the right version. Additionally, there is no central intermediary, such as a bank in the case of monetary transactions. However, you do need a majority consensus of the participants to make a given transaction valid.

In reality, blockchain is simply a combination of several concepts that have existed for years, such as transparency, decentralization, distributed ledgers, and immutability.

One of the major uses of blockchain that has gained the attention of the public over the last several years is Bitcoin. In fact, Bitcoin would not exist without such a structure. Bitcoin is a cryptocurrency that can be traded, used for purchase, etc., in the way that other forms of currency can be used as well. And guess what? You need a ledger to track transactions and ensure they are transparent (everyone can see it who needs to), you can't change recorded transactions (immutability), and you don't want to depend on a central authority such as a bank or a broker (decentralized).

Although blockchain gained attention in the financial sector, use cases have started to expand to other verticals. Compliance is no exception. Compliance can use this technology to accelerate adoption of their programs while gaining efficiencies within their company.

Getting started with blockchain within compliance

Assess if this is truly the solution for your business

As tempting as it is, avoid the hype! Some common things to consider when making the decision to use the technology or not:

- Do stakeholders in your company need/require access to data via a shared common database? Within many companies, groups may solve the data issue by building their own, but later this creates data silos within the organization.
- Are there third parties involved in your business that conduct regular transactions? Should all third parties be trusted? (Think suppliers, background verification for partners, employees.)

- Do stakeholders of the data have conflicting organizational objectives? One group may want to work with a third party because they are less expensive, while compliance may have serious concerns about how the third party poses a broader risk to the organization.
- Are there uniform rules/policies governing various aspects of your business, including ongoing third-party management?
- Is cryptography required, and is there a desire to use it for data privacy within your company?
- Is there a business need to track business decisions, approvals, and additional facts about working with certain third parties? This data should also remain immutable and transparent at all times.

If you are ready to move forward with blockchain, below are next steps to guide you through to implementation.

Identify the compliance functions moving to blockchain

Although it is tempting to move everything onto the blockchain, some common functions that could benefit from the technology are:

- **Supply chain management:** Track the origin of supplies, including movement of items throughout the supply chain, and have a trusted record of truth for stated changes.
- **Trade compliance:** Track the steps that have occurred between you and your clients/partners and ensure regulations are followed.
- **Third-party management and ongoing risk assessment:** Ensure you are working with partners that will not present undue risks to your business, or if they do, you are able to track the questionable transactions or contracts that can hurt your business.
- **Know your customer, anti-money laundering, and due diligence:** These are often duplicated efforts due to lack of data sharing across an enterprise, leading to fragmented and inaccurate data about your client/customer.

With blockchain, a record of truth with a clear audit trail can be shared with anyone in the organization. If a customer's information is updated, you could trigger an alert to notify those who subscribe and show the addition to the record. In short, you have a "clean" record of who you work with to lessen the chance of inadvertently being involved with people or companies associated with criminal activities.

Blockchain is still evolving; prepare for pushback

Best practices with implementation and ongoing management are still being defined. And yes, blockchain did gain prominence on the dark web, so a compliance function using it as core technology may appear to be questionable, to say the least.

However, the fact that it did start to gain prominence on the dark web should give you comfort, because operating in that environment required the key capabilities of an immutable, transparent record of truth, as well as providing anonymity (e.g., Bitcoin).

One of the big questions to ask yourself is, "What if there is a problem or a hack? Who do you go to in a public blockchain?" Since there is no central authority, this can make resolving a problem challenging. However, this should not preclude you from moving to the technology. However, the advice we would give is to proactively

define what troubleshooting would look like for your organization. Who else can proactively think through risks and associated remediation plans better than a compliance officer? This could mean hiring or training a person within your organization who is accountable when issues emerge, as well as integrating blockchain training as a requirement. And the blockchain should be closed (more on open and closed blockchains in a bit).

Consider the anonymous capabilities of blockchain. This can be used for compliance capabilities such as confidential employee compliance reporting (e.g., whistleblowing). One major hurdle for an effective whistleblowing program is that even though compliance officers state everything is "anonymous," employees are still left to wonder if it truly is. Personally, I have witnessed someone coming forward in an organization only to quietly move on. Perhaps it is an urban legend within an organization, but once the legend is out there, it can cause people to be hesitant about future whistleblowing activity.

Business process automation can also use blockchain, so you can have a record of the events that have been triggered and applied. Developed properly, this reduces the need for manual follow-up, potentially lost email reminders, and delays with getting contracts approved.

Determine what type of topology you need to implement

You will need to choose what type of topology you need to implement in order to support your business requirements. A topology is simply how to structure and configure the foundation for a blockchain. Blockchains can be open or closed, with the difference being who is allowed to join the network, track identities, execute the consensus protocol, and maintain the shared ledger.

- **Public:** This would allow all participants to join the blockchain without identity verification required.
- **Private:** Only designated individuals can join the blockchain.
- **Open:** This is similar to "public" but refers to the ability to read data on the blockchain. In this case all participants have access.
- **Closed:** Only designated individuals have access to read data on the shared ledger.
- **Permissionless:** Identity is not required and permissions of individuals participating (yes Bitcoin is the example again!) are absent.
- **Permissioned:** This helps enforce identity and role-based permissions and is a method to track identities.

Within either open or closed blockchains, you can choose to go permissionless or permissioned. Because public blockchains typically don't hold identity information (although it can be customized to do so), they are usually permissionless. Again, Bitcoin is an example. You have to make a choice between whether or not the blockchain is permissioned or permissionless. A permissionless blockchain allows anyone to join and add records to it. They would be able to browse and see all of the transactions as well.

In a permissioned environment, you need to know the identity of the party that would access the blockchain. From their identity, you can specify what privileges they have. For instance, you may want to grant read-only access to everyone, but only specific roles/individuals can add records. Again, note the "add records" statement, because blockchains do not let you delete records; you can only append to them. Overall, you need to determine, working with those knowledgeable in the field, what it is that you are trying to implement and what works best for your specific requirements.

From a corporate compliance standpoint, you will likely go with a closed blockchain. If it is a closed blockchain, it

usually means that you don't want everyone to see or do anything with the shared ledger. Therefore, designing and implementing such a mechanism, based upon managing identity and permissions against that identity, is required. It also helps to answer the "Who's going to fix this?" question as far as troubleshooting or disputes go.

Third-party risk rating and due diligence will most like remain private, and your organization will have read access. If someone resides within the compliance function, they would require read access, because their assessments would be considered the source of truth.

Supply chain and trade may only require a public blockchain, because external partners would require read and write access. However, you would want to consider your permission needs to evaluate how public data should be.

The capabilities for HR support can be especially useful. Imagine the ability to have multiple parties providing information on an employee and being able to add records knowing that they cannot be tampered with post facto.

Setting up nodes within your organization

Being a distributed platform, it is critical to identify participants who would have copies of the transactions, as well as who is responsible for mining the blocks when appropriate. If it is a private implementation within your enterprise, the distributed nature of the transactions can provide failover capabilities that are inherent with blockchain. The further out from your business site (site/data center/geographically separate nodes), the better the fault tolerance.

Prepare for implementation

Do your research on vendors to assist with implementation, especially if your IT department does not have the expertise just yet. A good place to start your research is LinkedIn. There are numerous blockchain think-tank engines, member groups, and training sites appearing regularly.

People are actively working to break through on this as a business topic and emerge as the leader. The good news is that now is the time for you to emerge as a leader for managing compliance differently. As with any new business venture, plan and budget accordingly.

One aspect that is worth noting is, what will be your contribution to the compliance and blockchain communities? What can your peers learn from you? We start advancing the technology when we start to talk about it. Therefore, ensure your voice is heard, and let's start doing compliance differently one step at a time!