Challenges Faced when Auditing a Digital-Currency Financial Institution

Written By: Marion Keyes, CAMS-Audit
I. Executive Summary

“Digital currency”\(^1\) is a currency with no physical form that is not controlled by a central bank. Instead, a person or entity “owns” digital currency by having entries in a massive distributed public ledger called the “blockchain.” The entries in the blockchain connect a specific unit of digital currency to the owner of the digital currency by means of public and private keys. The owner of the digital currency then accesses and utilizes their digital currency by means of a digital wallet that is placed online, on a computer, or on a smartphone. The blockchain itself is not controlled by any entity and cannot be found in any given place; rather, it resides on servers around the globe. This is loosely similar to the application protocol HTTP (hypertext transfer protocol) that resides on servers around the globe and thereby creates the “World Wide Web.”

The most widely known example of digital currency is the “bitcoin,” created in January 2009 by the mysterious Satoshi Nakamoto, whose true identity has yet to be verified. To date, the promises of bitcoin proponents have mostly been realized in alternative payment systems where bitcoin has provided almost nonexistent transaction fees, nearly instantaneous processing times and accessibility to the billions of persons who do not have banks, but who do have cellphones. Tarnishing this outstanding feature of bitcoin are two things: (i) public perception that bitcoins are used by criminals to launder money and commit other financial crimes; and (ii) the very real threat of hackers who have shut down and/or collapsed several high-profile exchanges. With respect to the public perception that Bitcoin is becoming the medium of exchange for criminals, the U.S. dollar will likely hold that top spot for some time to come. Put another way, the problem is not that bitcoins are inherently bad; rather, it is that “bad guys” have discovered bitcoins’ incredible power and value well in advance of the common man on the street. With respect to hackers shutting down exchanges, it is critical to understand that the blockchain, itself, is not being hacked. The problem lies with the lax and/or substandard security polices of the exchanges that have been hacked. This paper will explore several of the more pressing issues faced when auditing a digital currency financial institution.

---

\(^1\) The vast majority of digital-currency entrepreneurs balk at the term “virtual currency” as it: a) implies that the currency is not real; and b) is generally used to refer to units of value in closed systems – such as a gaming platform – whereby the “currency” has no value outside of the closed system.
II. Culture of Noncompliance

From the perspective of auditors, it is important to know that the digital currency space has more than its fair share of financial rebels.\textsuperscript{2} It is very difficult to put this group of persons into a box and then neatly label the box; nonetheless, many digital currency entrepreneurs oppose any sort of government intrusion into their economic affairs, creating a “culture of noncompliance” in many digital currency financial institutions.

This problem is further compounded by the fact that “many, if not most, of the digital-currency financial industry entrepreneurs come from a technology background with no real understanding of the compliance requirements for financial institutions.”\textsuperscript{3} Marco Santori, a leading digital currency attorney stated: “[a] lot of digital-currency companies don’t know what compliance obligations they are subject to, and that makes it difficult for young companies with limited resources to build out a compliance program that gets them banking … and helps them create a culture of compliance.”\textsuperscript{4} Santori goes on to say that “many digital-currency businesses put compliance second, when businesses in traditional finance tend to, and have to, put compliance first.”\textsuperscript{5}

Nonetheless, this culture of noncompliance is rapidly changing. Driven partly by high-profile criminal convictions and steep civil fines, digital currency financial institutions are beginning to understand that the “board of directors and

\textsuperscript{2} “The digital-currency industry tends to attract financial rebels; those who do not want to play by the rules and within the current system.” TELEPHONE INTERVIEW WITH DIGITAL-CURRENCY ATTORNEY BRUNO BORDIGNON, Senior Partner, Duncan Cotterill (New Zealand), January 14, 2015 (hereinafter “Bordignon Interview”); “Bitcoin does tend to attract a disproportionately large number of libertarians.” TELEPHONE INTERVIEW WITH BENJAMIN ULLRICH, President, Denver Bitcoin Center, January 12, 2014, (hereinafter “Ullrich Interview”).


\textsuperscript{5} Santori Interview.
management should create a culture of compliance to ensure staff adherence to the [financial institution’s] ... AML policies, procedures, and processes.”

Furthermore, as digital currency financial institutions reach out to traditional financial institutions in order to set up various bank accounts, they are quickly figuring out that traditional banks do not want to have anything to do with a digital currency financial institution that has a substandard compliance program. “Right now in banks and most financial institutions almost a third of their personnel are dedicated to compliance, and that tells us something: it tells us that these institutions can’t service an industry unless they’re going to service it in a compliant manner.”

Finally, as Arthur Levitt, the former SEC chairman aptly said: “… a company that has transparency and passes regulatory scrutiny is going to do much better than a company that is fighting regulators … So I don’t buy the libertarian argument that we don’t need any regulation.”

III. Lack of Regulation

A common theme heard from many leaders in the digital currency industry is that regulators have not done their job and have failed to provide adequate regulations for the digital currency industry. “One of the primary reasons why digital-currency financial institutions don’t have adequate compliance is that the governmental regulators don’t fully comprehend the new technology. In addition, the regulators are attempting to apply existing regulations to a wholly-new environment that doesn’t necessarily fit the paradigm of digital currency.” Furthermore, the “regulators” are not a single homogeneous body; rather, each

9 Bordignon Interview.
regulatory body has its own idea of what digital currency is, and is not. In one example, the U.S. Department of the Treasury has two different classifications for digital currency that differ depending on whether you are speaking with the IRS or the Financial Crimes Enforcement Center (FinCEN) (both agencies within the Department of the Treasury).\(^8\)

As a result, even when a digital currency financial institution wants to be compliant, it will have a hard time actually being compliant because there are gaps—perceived and/or real—in what exactly it is supposed to be doing. As Michael Parsons, a noted thought leader in the digital currency space, stated: “the problem with many digital-currency startups is that they don’t know what to do, if they have to do it, and they haven’t allocated enough money to do it.”\(^11\)

A number of thought leaders within the digital currency space have suggested the following path towards addressing this problem: (i) government regulators have to both understand digital currency and realize that it is not going away; (ii) digital currency financial institutions need to reach out to government regulators to help them understand this new paradigm; and (iii) both regulators and digital currency financial institutions need to come together to create a roadmap to compliance that addresses the needs and concerns of both sides.\(^12\)

IV. Scoping and Planning

“The scoping and planning process generally begins with an analysis of ... prior examination reports and workpapers ... independent reviews and audits.”\(^13\) Unfortunately, and largely due to the fact that digital currency financial institutions are very new, there are usually no prior examination reports, workpapers, independent reviews, or audits.

This issue will resolve itself over time as the digital currency financial industry matures and individual digital currency financial institutions have one or more previous audits under their belts.

\(^{10}\) “The Internal Revenue Service treats digital currency as a commodity so that it can be taxed, while FinCEN treats it as a currency so that it can be regulated. These are both in the Department of the Treasury.” Ullrich Interview.

\(^{11}\) Parsons Interview.

\(^{12}\) Parsons Interview; Bordignon Interview; and Santori Interview.

\(^{13}\) FFIEC Examination Manual, at 15.
V. AML Risk Assessment

It has been this author’s experience that digital currency financial institutions severely underestimate the magnitude of the risks associated with digital currency and digital currency financial products. They downplay their risk exposure in order to reduce their compliance burden. If that is the case, it is the auditor’s duty to bring this to the board and senior management’s attention.¹⁴

When talking about product and service risk, “[c]ertain products and services offered by [financial institutions] may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents.”¹⁵ A non-exhaustive list of high-risk products and services given in the Federal Financial Institutions Examination Council (FFIEC) Examination Manual includes: electronic banking, foreign correspondent accounts, services provided to third-party payment processors or senders and foreign exchange.¹⁶ All of the items on this list are products/services handled by most digital currency financial institutions. The highly transferable nature of digital currency creates a multitude of opportunities for the anonymous funding of money launderers and terrorists; thus placing almost all digital currency transactions squarely into the high-risk category.

With respect to customer and entity risk, “[a]lthough any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks.”¹⁷ The specific customers and entities identified by the FFIEC Examination Manual include: foreign financial institutions, nonbank financial institutions, senior foreign political figures, nonresident aliens and accounts of foreign individuals, foreign corporations, domestic entities located in higher risk geographic locations and cash-intensive businesses (such as ATMs). Perhaps the biggest risk that digital currency financial

institutions face is that of due diligence/know your customer (KYC). It is very
difficult to know where digital currency originates and where it is going. Who is
the real beneficiary of an account? Like traditional financial institutions, digital
currency financial institutions that have foreign correspondent accounts have
similarly difficult times monitoring the customer of the customer.

Geographic risk is very difficult to eliminate in a digital currency financial
institutions. “Identifying geographic locations that may pose a higher risk is
essential to a [financial institution’s AML] compliance program.” Such countries
generally include: countries subject to the Office of Foreign Assets Control (OFAC)
sanctions, jurisdictions determined to be of “primary money laundering concern”
by FinCEN, jurisdictions and countries actively being monitored by FATF because
of deficiencies with their AML programs, and offshore financial centers. Unlike
traditional money transfer systems, digital currency can move from one part of the
globe to another in a matter of seconds, without the need of a middleman.

In order to achieve auditing success, both auditors and digital currency financial
institutions have some hard work ahead of them with respect to risk analysis.
With respect to auditors, it is never easy to “rock the boat” and inform clients that
they have serious risk issues that would likely create significant changes to a
client’s compliance and business operations. Nonetheless, it is the auditor’s duty
to present these hard facts to their clients. Perhaps one method is to create a
roadmap to full compliance and suggest intermediate steps that will give younger
digital currency financial institutions a clear vision (and a plan) of what they
should accomplish as soon as they have the resources to do so.

VI. Customer Identification Program

“The CIP must contain risk-based procedures for verifying the identifying
information that must be obtained from each customer. At a minimum, the
financial institution] must obtain the following identifying information from each
customer before opening the account: name, date of birth for individuals, address,

---

18 “The ability to commit money laundering is greater with digital-currency
products and services than with traditional products and services. This is partly
due to the fact that the recipients of digital-currency transfers are largely
anonymous.” Bordignon Interview.
[and] identification number.”21 Here, the prevalent culture of noncompliance will usually make itself known. Many digital currency financial institutions will go out of their way to explain why they are not subject to this, or why their financial institution does not require, for example, an identification number from a customer. Instead, a number of digital currency financial institutions will attempt verification through non-documentary methods. Some of these methods are quite novel and ingenious, but they do not give the same level of satisfaction (that you, in fact, know who your customer is) as government-issued identification.

In addition, many digital currency financial institutions rely on third-party service providers to conduct their CIP. “However, as with any other responsibility performed by a third party, the [financial institution] is ultimately responsible for that third party’s compliance with the requirements of the [financial institution’s] CIP.”22

“The cornerstone of a strong … AML compliance program is the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing.” It is the opinion of this author that the majority of the customers of a digital currency financial institution should be subject to “enhanced due diligence” based on the product/service, customer, and geographic risks associated with digital currency. “Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the [financial institution’s] reputation, compliance, and transaction risks.”23 “The objective of a CDD should be to enable the [financial institution] to predict with relative certainty the types of transactions in which a customer is likely to engage.”24

If a customer poses a higher risk, the financial institution should consider obtaining, both at account opening and throughout the relationship, the following information on the customer: purpose of the account, sources of funds and wealth, identification of the beneficial owners of the account, occupation or type of business, financial statements, banking references, domicile, proximity of the customer to the financial institution, description of the customer’s primary trade area and whether international transactions are expected to be routine,

21 FFIEC Examination Manual, at 54.
22 FFIEC Examination Manual, at 58.
23 FFIEC Examination Manual, at 64.
24 FFIEC Examination Manual, at 63.
descriptions of the business operations, the anticipated volume of currency and total sales, a list of major customers and explanations for changes in account activity. 25 It is neither usual nor customary in the digital currency financial institution industry to expect or receive this amount of information from customers; customers who are likely more libertarian than the digital currency financial institution in question. Furthermore, the directors and owners of digital currency financial institutions are fearful that any attempt to require this depth of information will result in a decrease in revenue due to a loss of customers.

Again, as with the issue of risk analysis (above), if an auditor is able to provide a roadmap to compliance success, along with intermediate steps to reach this goal, then it is perhaps more likely that a digital currency financial institution will, over time, achieve full compliance.

VII. Internal Controls

“Internal controls are the [financial institution’s] policies, procedures, and processes designed to limit and control risks and to achieve compliance with [regulatory AML requirements]. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the [financial institution].” 26 “One perceived problem with digital currencies is that there is no one actively monitoring transactions.” 27 “Initially the market first came out with guidance that certain types of digital currency companies needed to be regulated as money services businesses (MSBs) … The original focus was registering as a MSB, the next focus was on establishing policies and procedures, then the next great focus was know your customer (KYC). What was left over was the transaction monitoring component. There are systems for monitoring transactions but they’re built against traditional financial services and therefore aren’t as suitable for digital currency services. There’s a technology gap there that exists, but again that’s a technology gap that probably will be filled over a period of time.” 28

26 FFIEC Examination Manual, at 33.
Though the technology gap will be filled over time, technology can only take the digital currency financial institution part of the way towards compliance success. It is perhaps wise for digital currency companies to begin wrapping their minds around the idea that they will need to budget significantly more resources to their compliance programs. Internal controls are only as good as the personnel monitoring them. Put another way, digital currency financial institutions will need to hire and retain a sufficient number of compliance experts to make sure that their internal controls function properly, are current and address all of the business lines of the institution.

**VIII. Independent Testing**

“Independent testing (audit) should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the [financial institution] to conduct independent testing every 12 to 18 months, commensurate with the ... AML risk profile of the [financial institution].”

29 Assuming that the risk profile of the digital currency financial institution is high, then the audit function would ideally be conducted on an almost continuing basis; as occurs in most large banks. Realistically, though, the vast majority of digital currency financial institutions who conduct independent testing will hire outside auditors or consultants due to their relatively small size and budgets.

“... The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.”

30 Again, due to the relative youth of the digital currency financial institutions being audited, the fact that they have even done a previous audit is noteworthy; it is far less likely that they will have a written “internal audit charter.”

“Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is

---

29 FFIEC Examination Manual, at 34.
30 IIA Standards, Section 1000, “Interpretation.”
incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.”

For most digital currency financial institutions, the audit function is a required “check-the-box” type of activity that occurs on an annual basis. The idea that audit should be an ongoing activity has not been ingrained into the average digital currency financial institution. This is partly due to the fact that most digital currency financial institutions are very young and are severely focused on the immediate needs of achieving profitability and launching various product lines. Over time, the issue of having an adequate internal audit function will hopefully resolve itself as the digital currency financial industry matures and as individual digital currency financial institutions undergo audits and thereby realize their importance.

IX. AML Compliance Officer

“The appointment of [an AML] compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.” Due to the fact that this is a very new industry largely populated by technology start-up companies, a) they oftentimes do not allocate sufficient funds to compliance, and instead, focus their time and money on launching their products/services; b) they oftentimes randomly appoint a corporate attorney, senior company officer or director who has next to no compliance education or experience to take on this role; and c) the compliance officer is oftentimes usually directly connected with the business lines of the company, i.e., they are not independent.

Here, the auditor may be faced with the unpleasant but necessary task of informing the board of directors and senior management that the person chosen to be the compliance officer is not competent for the position. Unfortunately, and

31 IIA Standards, Section 1311, “Interpretation.”
33 “In the beginning, most digital-currency financial institutions do not have a Chief Compliance Officer who has the adequate expertise, authority, or time to properly do their job. This quickly changes, however, when outside investors enter the picture and provide funding.” Bordignon Interview.
even if the person chosen for this position can receive the required education (for example, by receiving a CAMS certification from the Association of Certified Anti-Money Laundering Specialists), it is still not clear whether or not they would have the required experience to adequately manage a compliance program for a digital currency financial institution. Again, this issue will hopefully resolve itself as the industry matures and more experienced compliance experts take on roles within the digital currency financial industry.

X. Training

It is this author’s experience that compliance training programs—when they exist at digital currency financial institutions—are not actually implemented. When they are implemented, there is a definite lack of record keeping as to what was the training material, who was the training audience, dates of the training, etc.

This is perhaps the easiest compliance issue to fix, mostly because it will not require large expenditures of capital or resources to accomplish. As the Nike commercial says, “Just Do It.”

XI. Conclusion

With time and experience, digital currency financial institutions will mature and the problems discussed herein will diminish and hopefully disappear. In the meantime, it is the auditor’s duty to give their unvarnished opinions, findings and conclusions to the auditee.

As regulators wrap their collective minds around this new financial paradigm, they will surely levy fines upon and perhaps even imprison those who are not compliant. This will likely assist the efforts of compliance officers and auditors, when they bring their concerns to the board of directors and senior management. After all, it is hard to avoid or dismiss an issue when a fellow entrepreneur or colleague in the digital currency industry is sitting in jail for noncompliance. Finally, knowledgeable and well-informed legislators and regulators will hopefully enact legislation and regulations that assist those digital currency financial institutions that desire to be fully compliant by giving them a clear roadmap to success.
XII. Works Cited


b) INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING (STANDARDS), § 2120 “Risk Management” (The Institute of Internal Auditors, issued October, 2008, revised October 2012).