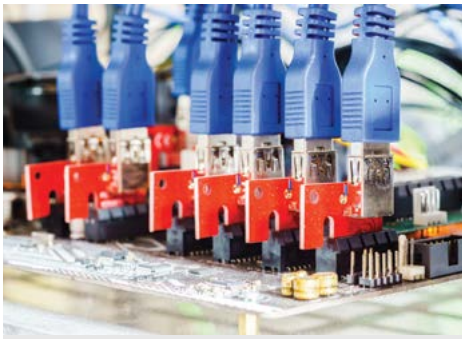
NOVEMBER 2017
www.bdo.com

AN ALERT FROM THE BDO FINANCIAL SERVICES PRACTICE

ASSET MANAGEMENT INSIGHTS

DIGITAL CURRENCY FUND PREPARATION FOR INITIAL YEAR AUDIT AND TAX COMPLIANCE

By Ignacio Griego, Sam Seaman, Jeff Barrett, Maurice Liddell



2017 has been an exciting ride in the world of digital currency, with historic returns attracting a slew of portfolio managers and investors to the space.

From Floyd Mayweather to Lloyd Blankfein to Jaime Dimon, everyone seems to have different opinions, but a theme everyone can agree upon is that the space is evolving at a rapid pace and participants are having a challenging time keeping up. Prior to 2017, many who chose to invest in the digital currency space chose to do so by directly investing in bitcoin and ether. The eye-popping returns during 2017 have attracted a wider group of investors, many with deep pocket books, looking to gain exposure to this new asset class by investing in or creating pooled private vehicles to invest in various new digital currencies and ICOs. During the year, it has been reported by various sources that over one hundred new digital currency funds have launched.

In addition to the challenges these funds will face in properly identifying investment opportunities and staying abreast of the dynamic market, the vast majority of these funds will also be dealing with financial statement audits and issuing tax returns for the first time. Within the digital currency space, this proves even more challenging compared to traditional investment funds because prior year precedents have not been set and there is a lack of authoritative guidance from audit and tax regulators.

With the aim of helping to improve the efficiency of year-end audit and tax services, we have summarized below key areas that digital currency funds and their service providers should be discussing during the planning phase of the engagement:

AUDIT

Currently, there are only a handful of assurance practices with experience auditing digital currency funds. Given the unique characteristics of these funds, having a foundation in both digital currency as well as investment funds will be key. Since this is a new space for most assurance practices, client acceptance can be a longer process compared to other new clients in traditional industries. Key areas to discuss with the auditors which can help in streamlining the client acceptance process and overall audit include:

BDO's Asset Management Practice serves over 350 firm relationships, representing in excess of 700 audits. Our team has extensive experience providing audit, tax and consulting services with a focus on investment funds, management companies, and broker-dealers. Our clients range in size from start-ups to large institutional funds with strategies utilizing equity, debt, commodities, derivatives and alternative investments.

Read more ▶

- **Entity structure** – Ensure your auditors have the ability to review draft fund legal documents before finalization. Key fund attributes such as fund risks, management and incentive fee structures, contribution and withdrawal details including timing and in-kind transactions, general fund liquidity features, different investor classes, fund level expenses, and partner allocation methodology will be areas of focus. Additionally, funds domiciled outside of the U.S. should discuss with their auditor additional reporting requirements that could be triggered.

- **Valuation policy**- A fund should develop its valuation policy addressing key points of Topic 820 Fair Value Measurement. While some funds may work with their administrator to help develop their valuation policy, management bears ultimate responsibility for determining the fair value of its investments. Although many exchanges exist throughout the world which may serve as a pricing source, there are several important points a fund should address in its valuation policy when analyzing the market, including:

  - **Valuation:** Topic 820 defines fair value as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants. Since a fund may trade a single currency on multiple exchanges, it will need to identify the principal market or, in the absence of a principal market, the most advantageous market. The FASB defines the principal market as the market with the greatest volume and level of activity for the asset or liability. The FASB defines the most advantageous market as the one that maximizes the amount that would be received to sell the asset or minimizes the amount that would be paid to transfer the liability, after taking into account transaction and transportation costs. When identifying its principal (or most advantageous) market, the fund should ensure it has access to this market at the measurement date. Because different access may exist among different funds, this needs to be considered from the perspective of the reporting fund. A fund should take into account all information that is reasonably available as it attempts to identify markets it can access.

    A fund's valuation policy should also address key aspects of the fair value hierarchy, including determining if quoted prices are available, if adjustments need to be made to the quoted prices, and whether the market is considered active. If quoted prices are adjusted, it will be important for the fund to denote in its valuation policy when it feels adjustments are appropriate and apply a consistent policy in the treatment of these situations.

    A fund should have proper monitoring controls in place to determine whether quoted prices from a specific exchange or source can be relied upon. Funds can consider discussing: Has diligence been performed on the pricing source to reflect upon how pricing is derived, or do the pricing sources have SOC reports explaining the process? Do significant spreads exist when comparing pricing sources? Many funds have chosen to compare their principal market pricing source with other pricing sources to demonstrate reasonableness.

  - **Custody and existence:** Proving existence and ownership is another area that if not discussed early and vetted properly, could create challenges during the audit. The portfolio should be examined and discussed with the auditor to determine which, if any positions, are held at a custodian. If a custodian is in place, auditors will typically confirm balances at a certain date. Understanding what balances and activity the custodian will confirm, whether the auditor can place reliance upon reports and confirmations received, and whether the auditor plans on performing additional procedures to test existence and ownership, will be key in reducing last-second fire drills. This will prove even more important for positions not held at a custodian and for positions that may have special privacy features. Ensuring the auditors are aware of these positions early will provide them with additional time to properly scope the verification of existence and ownership. When determining whether to invest in a new form of digital currency, fund portfolio managers should consider the above and actively discuss these points with their auditor. If the auditor is unable to develop a procedure to verify existence and ownership for a large position, the result could be a qualification to or potentially even a disclaimer of opinion. Important internal control considerations related to custody are discussed in further detail on pages 3 and 4.

- **Financial reporting** – Communication between the auditor and administrator during planning is another important focus point. Auditors should provide and discuss their document request list with the fund and administrator during planning to ensure all year-end reports requested will be available and in the proper format. Reviewing detailed schedules, including portfolio holding reports, partner allocations, realized gain/loss reports, and draft footnote disclosures prior to year-end is a best practice to improve year-end efficiency. The necessary time should be spent to ensure generic investment fund financial statement footnote language is tailored to properly address the unique aspects of a digital currency fund, including but not limited to the fund's valuation policy, custody arrangements, realized gain/loss and cost identification

Read more

policies, unique risks of digital currency funds (many of which are typically outlined in fund legal documents), and subsequent events such as forks, significant valuation changes, and key regulatory developments.

- **Timeline** – Ensure a timeline is established and agreed upon between fund management, the administrator and the CPA firm. The timeline should span both audit and tax and include when the administrator will deliver NAV packages and financial statements to management and the CPA firm, when the CPA firm will deliver draft FS and K1s to management and the administrator, and when final financial statements and K1s will be released. If CPA offices in offshore jurisdictions such as the Cayman Islands will be involved, those team timelines should also be included.

TAX CONSIDERATIONS

For federal tax purposes, virtual currency is treated as property. In Notice 2014-21 the IRS confirmed property tax treatment and explicitly stated that virtual currency is not treated as currency that would generate foreign currency gain or loss.

The character of gain or loss depends on whether the virtual currency is a capital asset in the hands of the taxpayer.

Virtual-currency investors will recognize capital gain or loss on the sale or exchange of virtual currency. Short-term and long-term rates will apply based on the holding period of the currency.

Conversely, virtual-currency "miners" will recognize the FMV of the currency as ordinary income on the day of receipt. It should be note that "mining" virtual currency constitutes a trade or business and net earnings may generate self-employment tax.

INTERNAL CONTROL ENVIRONMENT

No one would argue that the digital currency marketplace is inherently dependent upon both privacy and digital asset protections that are almost entirely dependent upon various technology platforms. The independent posture from government oversight and peer-to-peer transactional nature of digital currency is also driving discovery of cutting edge IT governance models toward more widely accepted "reliance." Conceptually, "reliance" provides a foundational connectivity between providers, investors and regulation.

The related service providers, including those managing crypto tools internally, include different solutions and intra-party procedures to meet the exploding transactional volumes across the globe. The challenge persists that not all solutions and how they are being utilized are standardized or maintained the same way. This presents an industry and entity challenge evaluating either underlying technologies.

Further, the use of technologies combined with management processing procedures (end users), like transactional dual-validation and call backs (akin to wire transfer processing), create a far more complex IT governance approach. These combined approaches are designed to ultimately protect stakeholders. Stakeholders include entity management, transaction and storage service providers (wallets and miners) and related investors. Global banks and regulatory bodies are currently discerning industry standards from issues like jurisdiction to regulatory certification to fulfil their respective "public protections" duties.

> **"Simply, the 'reliance' positon depends upon independent validation and testing both from literal security perspective (transactions) and a technical industry perspective (asset existence) through the use of the SOC 1 "IT review report" and SOC 2 report."**

The SOC 1 and SOC 2 reports are only as reliable as the defined scope and considered the current standard for evaluating a third-party technology provider including FinTech providers (i.e. wallet custodians, exchanges) and more traditional SaaS providers such as accounting platforms (Oracle, NetSuite, SFDC, SAP & other hosted environments). Today, SOC 1 and SOC 2 reports help management assess whether IT controls are operating effectively or not depending on if the SOC 1 and SOC 2 reports were issued with an "unqualified" opinion or not. This report alone should not be the basis for a constructive "reliance" approach to the entity, such as a technology service provider or an entity utilizing the technology under scope of review. It should be noted that while SOC 2 reports ordinarily take a deeper dive into information technology matters and may be of interest to management, clients, prospects, and regulators from a confidentiality, security, processing integrity, availability and/or privacy of the data perspective; SOC 1 is the report that addresses internal controls over financial reporting (ICFR) and may be of interest to management, clients, and regulators from a transaction processing perspective.

Note: The AICPA plans to issue an attestation guidance related to the supply-chain industry, such as digital currency, in the next year or so.

The reliance on a third-party review of these emerging technologies (encryption keys, processing procedures, and perimeter protections) may not be totally possible. Only experienced service providers with fully reviewed and assessed technology environments combined with a holistic point-to-point control environment should be considered to minimize the outsized risk of breach. However, the industry and technology

Read more ▶

governance have improved dramatically as significant lessons have been learned from past breaches.

There are several factors that determine if stakeholders, and more specifically, financial statement auditors (and management) can place "reliance" upon such "SOC 1" or "SOC 2" reports and "opinions." For management of investment funds, individual crypto currency investors of all types, and technology service providers (including custodians and exchanges), the independent external SOC 1 or SOC 2 report is the only standard in practice today. Every SOC 1 or SOC 2 report is only as good as the scope of the review (IT controls population included versus the total population of topics).

The SSAE 18, SOC 1 Type 2 and SOC 2 Type 2 reports help stakeholders dependent on technologies being provided as a service to understand the internal controls of the service organization.

All constituencies from investment funds and wallet service providers are continuously facing a barrage of risk and control considerations. Although international technology and security standards exist, the emerging crypto regulatory constructs are yet to adopt widespread "transactional and asset protection" standardizations.

Some practical steps to understanding "reliance" for various stakeholders include the following:

1. In situations where management does not use third-party service providers (to review or provide technologies) **such as instances where crypto wallets and transactions are performed in-house**, serious consideration and discussion of key controls should certainly be conducted. The areas management should be prepared to disclose include cash management, financial reporting and trading activity, along with the controls over storage of encryption keys, and transactional walkthrough processing, while providing supporting documentation to the audit team.

2. Stakeholders, such as prime brokers, custodians, fund administrators and other service providers may provide SOC 1 and SOC 2 reports to management outlining the internal control environment and results of the examination (including control deficiencies). This may include comments on limitation of scope and indications that opinion is "qualified." Users of the SOC 1 and SOC 2 reports are responsible for following up with the service provider on any identified exceptions, etc.

3. Discuss any report received with the financial statement audit team. In particular, if the report describes any changes to the processing environment or issues in internal control processes.

4. Evaluate complementary user entity controls (CUECs), if any are noted in the SOC 1 or SOC 2 reports. CUECs are controls that the service provider (service organization) assumed the entity will implement in designing its internal control related to the services it provides to the entity.

5. Evaluate complementary subservice organization controls (CSOCs), if any are noted in the SOC 1 or SOC 2 reports. CSOCs are controls that the service organization assumed its vendors (subservice providers) will implement in designing its internal control related to the services it provides to the entity. For example, if the service organization that provides crypto wallet services utilizes Amazon Web Services (AWS) for its cloud, the service organization has very likely assumed that the physical, environmental and logical controls related to the infrastructure that AWS provides are managed by AWS, and relies on AWS' controls as it relates to the security, confidentiality, privacy, and availability of the infrastructure.

6. Management can provide an updated SOC 1 report to the audit team to assist in the assessment of the internal control environment and related representations. Please note, if the SOC 1 report does not cover the full period under audit, typically the fiscal year, management can request a "bridge letter." The bridge letter is a memo that the service organization management provides representing if any changes were made during the stub period (of fiscal period) since the last date of the examination and before the start of the next annual examination period. SOC 1 reports may not follow calendar or even necessarily match up to entity financial statement fiscal years.

7. Consider the required management procedures that 'wrap around' the use of technology and related safeguards that control the use and disposition of technology and related transactions. More specifically, how does management's responsibility, such as compensating control procedures, combined with service provider technologies, ensure safeguard of assets, transactions, and protection of value.

8. Implement vendor risk management procedures, whereby prior to selecting a vendor the entity management performs a thorough evaluation of the vendor keeping in mind the relevant industry risks, including viability of the vendor being considered. Exhaustive security questionnaire has come to be common place given the environment we live in, which may be addressed by the SOC 1 and/or SOC 2 report if the scope of those questions are covered in the SOC 1 and/or SOC 2 reports.

Read more ▶

Providers and management stakeholders should consider the enterprise risk management capabilities and the capacity to safeguard assets. Financial statement auditors and the service providers should be consulted and provided an opportunity to consider risks toward providing insight into the degree of marketplace capabilities.

The digital currency and crypto marketplace will continue to grow and thrive where independent verification is provided to develop confidence in a technology dependent on an alternative investment miracle. The path to success and marketplace prominence will be through independent testing and congruency with emerging regulatory standards.

We hope this overview will be useful in guiding digital currency funds through first-year planning discussions with their service providers to facilitate a smooth and successful delivery of audited financial statements and tax returns. If you would like to discuss any of the topics raised in this alert in more detail, please feel free to reach out to any of the BDO team members below or to your local BDO practice leaders.

HOW DO I GET MORE INFORMATION?

IGNACIO GRIEGO
Assurance Partner
San Francisco
415-490-3182
igriego@bdo.com

KEITH MCGOWAN
Assurance Partner
New York
212-885-8037
kmcgowan@bdo.com

JONATHAN SCHMELTZ
Tax Partner
New York
212-885-8170
jschmeltz@bdo.com

SAMUEL SEAMAN
Tax Partner
San Francisco
415-490-3157
sseaman@bdo.com

BHARATH RAMACHANDRAN
Assurance Partner
Boston
617-239-4161
bramachandran@bdo.com

MATHEW DEMONG
Tax Partner
Boston
617-422-7575
mdemong@bdo.com

NICK MAROULES
Assurance Partner
Chicago
312-730-1332
nmaroules@bdo.com

JOE PACELLO
Tax Partner
New York
212-885-7375
jpacello@bdo.com

DARIN SCHINDLER
Tax Partner
Pittsburgh
412-281-7618
dschindler@bdo.com

BDO'S FINANCIAL SERVICES PRACTICE

BDO's Financial Services Practice provides assurance, tax and advisory services to asset management entities, primarily Hedge Funds, Private Equity Funds, Broker Dealers and Mutual Funds. The practice services over 600 advisors nationwide with funds ranging from start-up funds to those with billions under management.

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

People who know Asset Management, know BDO.