Cryptocurrency Compliance and Regulatory Risk

FEATURED EXPERTS

Kevin Batteh, Partner, Delta Strategy Group

Alan Cohn, Principal, ADC/Strategy.Works, LLC

John Collins, Affiliate, Berkman Klein Center at Harvard University

Philip Gradwell, Chief Economist, Chainalysis

Kimberly Grauer, Senior Economist, Chainalysis

The rise of cryptocurrencies — including bitcoin, monero, litecoin and ethereum, to name a few — and initial coin offerings (ICOs) as funding mechanisms for startups have created new compliance and legal challenges for banks and financial institutions. As the flows of capital into digital-currency exchanges continue to grow and ICOs proliferate, opportunities for the financial sector will, too. Concurrent with those two trends will be a greater stress on money-laundering controls and transparency regulations. In this article, RANE highlights some of the emerging issues and risks identified by experts.

TRACKING CRYPTOCURRENCY TRANSACTIONS

Philip Gradwell of **Chainalysis** says that banks and financial institutions need to understand who are transferring funds, as well where that money is going, in order to properly understand the risk that arises from transacting in cryptocurrency with counterparties. "Not all bitcoin transactions are equal from a compliance perspective," he says. "For instance, a bitcoin purchased on localbitcoins.com is likely to be used on a darknet market, while a bitcoin purchased on a regulated exchange, such as Coinbase, tends to be used for legal means." ***Part of a bank's responsibility, thus, is "understanding who the crypto counterparty is.*** Financial institutions and banks are at different stages of that process and not necessarily understanding the risks," he adds.

Gradwell notes that in traditional money transfers by financial institutions, a notification, such as a SWIFT message, is generated when funds enter one organization's accounts. (The Society for Worldwide Interbank Financial Telecommunication facilitates money transfers via messages that include such information as the sending bank's information, the parties involved in the transfer, and codes that describe how funds will be collected.) ***Still, it's difficult for a bank to see where customers send their cryptocurrency "unless they are watching the bitcoin network."*** With blockchain transactions, real-world identities can be determined at the points where individuals convert digital currency into fiat currency — the "on- and off-ramp," as **Gradwell** calls it. "The crucial thing is you need to connect the identities." This, he notes, isn't an either/or proposition: "The transactions can be monitored, separately, in both systems, and the exchanges are where these two systems come together."

A recent report by Chainalysis found that the amount of bitcoin heading into dark web transactions, once accounting for an estimated 30 percent of the cryptocurrency's use, is now down to 1 percent. ***Yet that comes from the boom in cryptocurrency among financial speculators, rather than a decline in criminal activity.*** "Exposure to the darknet is going up in absolute numbers," **Gradwell** says.

"It's not quite as scary as it's made out to be, particularly when bitcoin has moved into the mainstream," says **Alan Cohn** of **ADC/Strategy.Works, LLC.** For instance, ***transactions in bitcoin or ether are increasingly being handled by exchanges that have registered with FinCEN*** as money services businesses (MSBs) that conduct not only know-your-customer (KYC) inquiries but enhanced due diligence, as well.

"The industry is built upon the idea that power structures should be decentralized," John Collins notes. "The idea that they would suddenly centralize themselves around self-regulation is unrealistic."

THE EVOLUTION OF AML PROCESSES

Anti-money laundering (AML) processes are emerging for cryptocurrency exchanges. **Cohn** notes that compliant cryptocurrency exchanges, as well as the majority of crypto exchanges, verify the identity of the person presenting funds, as well as the entity from which they are coming. If it all checks out, the transfer is executed. ***"For the provenance of the funds, what's interesting in cryptocurrency is that you actually have two mechanisms for checking,"*** he says. "You still have the ability to check the ID of the presenting party, to say, 'Who is this person?'" But in addition, blockchain's distributed-ledger structure makes it possible to "look directly at the provenance of the funds."

There remains a challenge, however, of connecting digital wallet addresses to identifiable persons. Bitcoin transactions — which are pseudonymous, not necessarily anonymous — occur between publicly searchable wallet addresses that are all unique, **Cohn** explains. "There are entities that assist financial institutions and law enforcement in understanding how to use public records and also to check the provenance of the funds." Yet further analysis is also possible, allowing interested parties to examine the chain of custody for funds or to identify wallets linked to criminal investigations, along with links to those associated with dark web, and possibly illegal, activity. Blockchain analysis can also determine a digital wallet's proximity to known entities tied to illicit transactions, further shedding light on whether an individual is operating as a mule or a front. ***The knowledge that bitcoin is traceable provides some level of deterrence for bad actors,*** **Kimberly Grauer** of **Chainalysis** says. "Bringing bitcoin into the mainstream will deter money launderers."

Gradwell also notes banks' evolving policies. There's a comfort level that needs to occur before financial-services firms go all-in on cryptocurrency, he says. "A lot of banks have publicly said, 'We won't touch any funds generated from bitcoin,'" yet acceptance has continued to grow and many banks are putting processes in place. "I imagine the sector is going to take a more nuanced approach in the future." Banks will come to know that funds from bitcoin can come from a legitimate place, though "it takes a bit of understanding before they can build the risk analysis around it."

At the same time, licensed exchanges are growing, **Gradwell** says. And with a leader like Coinbase posting $1 billion in revenue last year, the pressure could increase on financial institutions to speed up their digital-asset operations.

INSTITUTING KYC PROTOCOLS

Once a cryptocurrency business registers with FinCEN, they're able to provide the regulator with information about individuals moving funds. "This is what the transactional analysis yields — and this either matches what the parties have represented, or it doesn't match," **Cohn** says. "It provides another layer of ability to check identity." In addition, there are

blockchain-based digital identity platforms that can provide KYC information, and that financial institutions could require customers to use in order to access their platforms." That allows institutions to have "some certainty around who the individual is" that's transacting in bitcoin or another digital asset with a high degree of certainty.

Analytical services also allow organizations to integrate checks on both the ID of the individual and the provenance of the funds, **Cohn** says. Those same services can also provide a gauge of what their exposure is to questionable elements. **Cohn** notes that the Treasury Department has estimated that 99.9 percent of money-laundering attempts are successful in the traditional banking system, yet "the tools that exist for understanding identities and provenance in the cryptocurrency world are significant." That goes for dealers and brokers, money-transfer firms, or depository trusts.

"The overall message is: Don't think that there's no visibility into this world," **Cohn** says. "In fact, the more you transact in this area, the more visibility you have."

CREDIT RISKS IN CRYPTOCURRRENCIES

An overwhelming majority of cryptocurrencies is used for investment rather than transactions, notes **John Collins** of **Red Flag Consulting. Collins** ***calls out the volatility inherent in digital assets that aren't pegged to any fiat currency.*** "Why would I buy something with a cryptocurrency today that could double tomorrow?" he says. Conversely, accepting payment in bitcoin presents a devaluation risk. "I think in terms of a global payment system, the technology certainly is not able to scale to that level — yet."

Collins says there's more discussion about cryptocurrency as a new asset class now than there was three or four years ago, which could shift the nature of a predominantly speculative market. Yet transactional use carries risk. "A problem in this industry is the same problem they've always had: Primarily reputation," **Collins** says. "You're not seeing a lot of retailers or brick and mortars accepting these cryptocurrencies or assets as payment, unless your retail is on a darknet market. ***All of those things — the terrorism financing, money laundering — all of that stuff continues to be an issue in the minds of the public because they don't see a lot of transactions in the course of their daily lives."***

There are also credit risks in the trading of bitcoin. ***In particular, people are borrowing on credit cards to finance trade at exchanges, which can sometimes be leveraged.*** However, **Gradwell** says, "These credit risks are real but do not yet have seem to have significantly materialized, despite large fluctuations in price." Yet, these risks remain and could become increasingly significant. **Gradwell** responds, "There is a very live debate on how to manage these risks in the industry."

SHIFTING REGULATION AND COMPLIANCE CHALLENGES

From the standpoint of compliance, the biggest challenge for blockchain is bringing the entire supply-chain ecosystem into alignment, **Kevin Batteh** of **Delta Strategy** says. For instance, the specific context of supply-chain management — e.g., you want to track a product from the time it was grown and bailed on a farm in Mississippi until it is unpacked at a manufacturing facility in China — would require having all the people along the way (port authority officials, shippers, etc.) be part of the process and have verified ID and the ability to use the technology. "Fundamentally, you have to have a good identity solution," he adds. "How can we verify that Kevin Batteh is Kevin Batteh?" That will require buy-in from everyone along the supply chain — a list that include state actors, foreign governments, private and public companies, etc.

From the standpoint of compliance, the biggest challenge for blockchain is bringing the entire supply-chain ecosystem into alignment, Kevin Batteh argues. "Fundamentally, you have to have a good identity solution."

One of the most pressing issues for banks in the cryptocurrency space will be ***failing to ramp up compliance processes fast enough***. "Just knowing how much money is going into exchanges is something banks need to understand," **Gradwell** says. "People are sending and receiving money from exchanges regardless of the bank policy toward crypto. (Banks) may not realize they have a compliance problem."

Gemini — the cryptocurrency exchange launched by Cameron and Tyler Winklevoss — proposed the creation of a Self-Regulatory Organization for the industry. "It's a smart idea," **Collins** says, though he adds that he's "very skeptical" of the cryptocurrency industry signing on anytime soon — even at established exchanges. "The industry is built upon the idea that power structures should be decentralized," he notes. "***The idea that they would suddenly centralize themselves around regulation is unrealistic.*** Coordination in any competitive industry is tough, but this is one is particularly difficult."

Regulation risk appears to be most volatile in Asia, with officials in Japan and South Korea struggling to deal with cryptocurrencies' popularity boom. "Volume grew phenomenally fast, and a lot of the regulatory news comes at a much higher cadence in those regions," **Grauer** points out. "Regulators in those countries are saying, 'This is a pace of retail investing that we are uncomfortable with. It's happening at a speed we need to get out in front of.'"

Investors also should be wary of regulatory events in Europe, she argues. In February 2018, the European Securities and Markets Authority (ESMA) announced it would begin monitoring the development of financial innovation, specifically including cryptocurrency and blockchain technology. The UK's Financial Conduct Authority (FCA), in its 2018/2019 business plan, also identified cryptocurrencies as one of its priorities for the year ahead.

"It's not quite as scary as it's made out to be, particularly when bitcoin has moved into the mainstream," says Alan Cohn. "Don't think that there's no visibility into this world. In fact, the more you transact in this area, the more visibility you have."

STATE VS. FEDERAL REGULATIONS

All states have money transmitter licensing requirements, and a business's designation is a state-by-state determination, depending on activity, says **Batteh**. For instance, a wallet service in New York will have to comply with a licensing requirement, while an exchange must register in all 50 states. Further complicating the issue, each state also has its own securities laws — which may or may not trigger Blue Sky Laws designed to protect investors against fraudulent sales.

Other US regulators that have opined on cryptocurrencies include the Commodities Futures Trading Commission (CFTC), the Internal Revenue Service (IRS), the Consumer Financial Protection Bureau (CFPB), Financial Crime Enforcement Network (FinCEN) and the Department of Justice (DOJ).

Currently, both the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC) appear to want some piece of jurisdiction over exchanges, "States will balk at that, especially New York," **Collins** says. So far, New York is the only one that has stepped up to create a cryptocurrency-specific regime outside of its money transmission statute. "Most other states decided to either modify money-transfer statutes, or took current law and interpreted them to cover cryptocurrency," **Collins** says. Cryptocurrency exchanges operate under state money-transmission laws, which "were not created to be able to handle exchange operations."

Because of the way bitcoin was created — by anonymous individuals carrying out the mining and dispersion of those tokens — ***the ruling so far on such digital assets as bitcoin and Litecoin is that they are treated as commodities,*** which would put those assets in CFTC's wheelhouse, **Collins** says. That said, the CFTC doesn't have authority to regulate exchanges, only to deal with observable fraud and market manipulation.

INITIAL COIN OFFERINGS (ICOSs)

Cryptocurrency startup firms have increasingly turned to a previously unregulated crowdfunding mechanism known as ***initial coin offerings (ICOs)***. In the process, investors will buy "tokens" — similar to shares in a public company. "People are selling them as a way to fund their idea or platform. People buy them expecting the value of those coins to rise, either because the product does well or because people want to buy them at a higher price on a secondary market" **Collins** adds.

In December, SEC Chairman Jay Clayton remarked on initial coin offering (ICO) markets noting that, "as they are currently operating, there is substantially less investor protection than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation."

In the statement, Clayton also said that ICOs raised questions for investors and market participants, offering a few to consider:

- Is the product legal? Is it subject to regulation, including rules designed to protect investors? Does the product comply with those rules?
- Is the offering legal? Are those offering the product licensed to do so?
- Are the trading markets fair? Can prices on those markets be manipulated? Can I sell when I want to?
- Are there substantial risks of theft or loss, including from hacking?

"The answers to these and other important questions often require an in-depth analysis, and the answers will differ depending on many factors," Clayton added.

"Just knowing how much money is going into exchanges is something banks need to understand," Philip Gradwell points out. "People are sending and receiving money from exchanges regardless of the bank policy toward crypto. (Banks) may not realize they have a compliance problem."

ABOUT THE EXPERTS

Kevin Batteh, Partner, Delta Strategy Group

Batteh is an attorney and government affairs expert working in the field of derivatives regulation and policy, as well as a senior advisor to a number of blockhain and digital currency (e.g., bitcoin and Ether) related companies. He began his career as a complex litigation associate at a Fortune 100 law firm. In 2003, after five years of private practice, he joined the CFTC as a trial attorney in the Division of Enforcement where he investigated and prosecuted cases of fraud and market manipulation in Federal District Courts across the country.

Alan Cohn, Principal, ADC/Strategy.Works, LLC

Cohn is co-chair of Steptoe & Johnson LLP's Blockchain and Digital Currency practice and Principal of ADC/Strategy.Works, LLC. He also serves as counsel to the Blockchain Alliance, a public-private forum established by a broad coalition of companies and organizations to help combat criminal activity on the blockchain. He counsels companies that handle virtual currencies, blockchain and distributed ledger technology companies, and investors in these technologies on strategy, policy, legal, and compliance issues.

John Collins, Affiliate, Berkman Klein Center at Harvard University

Collins's focus at the Berkman Klein Center is on developing global public policy frameworks around financial technology, with a specific focus on digital currencies and blockchain technology. He formerly served as Head of US Operations for Red Flag Consulting, a strategic advisory and communications firm, and he is former Head of Policy for Coinbase, the world's most well known digital currency company. Collins led the United States Senate's first oversight work into bitcoin and blockchain technology in 2013, culminating in the first Congressional hearing on the subject. He has worked with policymakers, industry leaders, academic thinkers, and media from the local to the supranational level. He has been featured in national and international media, including the New York Times, Washington Post, Wall Street Journal, CNBC Europe, NPR, and Politico, among others.

Chainalysis

Founded in 2014, Chainalysis provides investigation software and financial data for digital currencies, Blockchain technologies. With offices in New York and Copenhagen, the firm assists client in the adoption of digital currencies through a software platform that increases transparency between financial institutions, governing bodies, and users. Chainalysis software has assessed over $20 billion in transactions and the firm's research has been recognized in Forbes, The Wall Street Journal, and other media outlets. The firm works with global financial institutions, like Barclays and Bitcoin exchanges to enable every stakeholder to assess risk in this new economy.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.