Cryptocurrency – A Business Opportunity or Mistake?

Compliance and Ethics

Financial Services

Technology, Privacy, and eCommerce

Cheat Sheet

- **Blockchain's appeal.** It allows anyone to bypass the use of any intermediaries, reducing the costs and time needed to settle a transaction.
- Accepting cryptocurrency**.** Start by setting up a public cryptocurrency wallet address and making it available to consumers.
- **Compliance programs.** All financial institutions using blockchain must implement an anti-money laundering (AML) program and follow sanctions protocols.
- **Transaction monitoring.** The right technology can protect an institution’s finances and reputation, which can easily be damaged by scandals.

As general counsel for a US-based nationwide bank, your CEO has asked you whether your bank can use cryptocurrency payment networks to speed up payment activities and other bank-permissible functions. Your CEO has also mentioned in passing that one of your biggest customers, a worldwide retailer, for which you acquire payments would also like to be able to accept payments in cryptocurrencies.

You’ve heard of cryptocurrencies (who hasn’t, with Bitcoin trading at US$46,000?). But you aren’t sure of all the legal ramifications of the proposed activities, so you begin to research cryptocurrencies

and what would you need to do to make this happen.

Cryptocurrencies 101 — What are they?

The current financial system is built on trust and trusted intermediaries — trust in banks and other financial institutions, and the governments responsible for issuing fiat currency. Cryptocurrencies emerged as an alternative to the need to place this trust into financial institutions and governments.

One of the most innovative aspects of cryptocurrency is the creation of a new type of ledger system where it is possible to rely on the validity of data stored across a decentralized network of participants with no relationship to each other, and no grounds for anyone to trust them.

The P2P/decentralized feature means there is no central authority responsible for making decisions relating to the state of the ledger and the participants in the network. Everyone and anyone can participate, identities are not vetted, they just have to be running software that enables them to connect to the network and enforces the rules of the network.

Private keys are one of the most important concepts in cryptocurrency; if a public address is the equivalent to a bank account number, private keys are like a debit card PIN. They are the alphanumeric sequence that generates an address you can send funds to, and they unlock funds received to enable sending them onward. Because private keys are what controls the ability to withdraw or send funds out of an address, it is often said, “whoever has the keys, has the coins.”

Using cryptocurrency payment networks

To understand the benefits of using blockchain technology as payment rails, it is worth considering how fiat currency travels through the financial system. Depending upon the location of the sender and receiver of funds, fiat currency may go through the whole chain of financial institutions (what are known as correspondent banks) before it reaches its final destination (i.e., the beneficiary’s account).

The term correspondent bank refers to a financial institution that provides services to another financial institution, usually in another country. It acts as an intermediary or agent facilitating wire transfers, conducting business transactions, accepting deposits, and gathering documents on behalf of another bank.

Having multiple financial institutions involved in the transactions increases the amount of time it may take for funds to become available. It also increases the cost of conducting that transaction. This is why using blockchain technology as payment rails is so appealing; in theory it would allow a financial institution to bypass the use of any intermediaries, reducing the costs and time needed to settle a transaction.

Through a series of interpretive letters, the Office of Comptroller of Currency (OCC) made it clear that while financial institutions must be aware of the potential risks when conducting activities using blockchain technology (as further discussed in this article), they are allowed to validate, store, and record payment transactions using blockchain technology. They can thereby transact stablecoin payments on behalf of their customers and provide banking services to lawfully operated cryptocurrency businesses.

"Stablecoin" is a type of cryptocurrency whose value is tied to another asset class such as fiat

currency or gold to stabilize the price.

How to accept payments in cryptocurrencies

Technically speaking, accepting payments in cryptocurrencies is as simple as setting up a public cryptocurrency wallet address and making it available to the consumers. Cryptocurrency wallet addresses are anywhere between 25 and 36 characters and can be converted into a QR-code, which can be scanned by the consumer when sending payment.

Once the payment is made and validated, the transaction is posted on the blockchain public ledger. The ledger shows a payment from the consumer's public address to your public address. Legally speaking, accepting payments in cryptocurrencies without involving any intermediary (e.g., a payment processor or a bank) brings up a whole host of potential issues.

Among them: banking, money transmission, securities, licensing, anti-money laundering compliance, sanctions compliance, fraud/ransomware/human trafficking/illicit activity, transaction monitoring, consumer protection and tax, to name a few.

> Legally speaking, accepting payments in cryptocurrencies without involving any intermediary (e.g., a payment processor or bank) brings up a whole host of potential issues.

A threshold question is often how to characterize a particular cryptocurrency from a regulatory perspective. Whether a cryptocurrency is considered a security, commodity, and/or currency drives the applicable regulatory requirements. For example, if a cryptocurrency is deemed a security, it may implicate state and federal registration requirements or require certain persons transacting in the cryptocurrency be registered as broker dealers. Our discussion focuses on cryptocurrencies similar to Bitcoin, which is not regarded as security. Additional considerations may be implicated depending on the specific classification and attributes of a particular cryptocurrency.

Licensing

In 2013, the US Financial Crimes Enforcement Network (FinCEN) issued guidance that applies basic principles of the Bank Secrecy Act (BSA) to anyone that creates, obtains, distributes, exchanges, accepts, or transmits cryptocurrencies. FinCEN's guidance asserted that only financial intermediaries (e.g., administrators or exchangers) acting on behalf of customers were subject to the registration, record keeping, and reporting requirements of the BSA as money transmitters (a

category of “money services businesses”).

FinCEN’s regulations define the term “money transmitter” as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term “money transmission services” means “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”

The definition of a money transmitter does not differentiate between real currencies and cryptocurrencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.

In addition to MSB registration requirements on the federal level, many states require licensing on a state-level, so long as an entity is either located in the state or does business with residents of the state. For example, the New York State Department of Financial Services created a BitLicense, a business license covering commercial cryptocurrency activity in the state of New York. The BitLicense covers diverse uses of cryptocurrency like custodial services, currency transmissions and issuance, and exchanges.

Some companies handling cryptocurrencies have organized as trust companies in different states or are seeking national charters. In Wyoming, the legislature passed a law that created a new type of state bank charter that enables companies to become special-purpose depository institutions (SPDIs, pronounced “speedies”), handling both US dollars and digital currencies.

Crypto tip: Companies can set up wallets of their own

With this in mind, your bank’s customer (a worldwide retailer) could technically set up a public wallet address of its own and, without your bank’s involvement, start accepting payments in cryptocurrency. Since it would be accepting cryptocurrencies on its own behalf (and not on behalf of any customers), there would be no need for it to be licensed as an MSB. However, for reasons that will become apparent shortly, that might not be the best way to go.

If, however, your bank’s customer decided to accept payments in cryptocurrency through your bank, your bank’s federal full depository charter would cover any licensing requirements on the federal level. While your federal full depository charter should generally preempt state licensing requirements, some states (e.g., New York) may argue that the scope of your charter does not cover the appropriate obligations and does not meet its licensing requirements for cryptocurrency activities.

Anti-money laundering compliance

All financial institutions and MSBs (including money transmitters) must conduct a comprehensive risk assessment of their exposure to money laundering and implement a risk-based anti-money laundering (AML) program. FinCEN regulations require all financial institutions and MSBs to develop, implement, and maintain a written program that is reasonably designed to prevent it from being used to facilitate money laundering and the financing of terrorist activities.

An AML program must include:

- Written know-your-customer (KYC) policies, procedures, and internal controls;
- Designated compliance officer responsible for assuring day-to-day compliance with the program and BSA requirements;
- Ongoing training for appropriate personnel;
- Independent review/audit to test the program; and
- Risk-based procedures for conducting appropriate ongoing customer due diligence.

In addition, all financial institutions and MSBs are subject to certain record-keeping and reporting requirements pursuant to the BSA, such as suspicious activity and currency transaction reporting.

Recently, FinCEN proposed regulations that would require financial institutions and MSBs to submit reports, keep records, and verify the identity of customers participating in transactions above a certain threshold, including cryptocurrency wallets not hosted by a financial institution. Also known as "unhosted wallets," these wallets are typically hosted by a financial institution in certain foreign jurisdictions identified by FinCEN as a jurisdiction of a primary money laundering concern, including Myanmar, Iran, and North Korea.

The proposal also includes an aggregation requirement if the financial institution or MSB has a knowledge that a transaction is one of multiple involving a single person within a 24-hour period that aggregate to value in or value out above a certain threshold.

Crypto tip: Know Your Customer (KYC) information helps

If your bank's customer decided to accept payments in cryptocurrency without your bank's involvement, it would technically not be subject to these requirements. However, meeting other requirements (which are explored below) may be more difficult, if not impossible, without some basic KYC information being obtained and retained. If your bank's customer decided to accept payments in cryptocurrency through your bank, your bank's existing AML program, with some adjustments, would likely meet all requirements.

Sanctions compliance

All US persons are prohibited from doing business with any individuals or entities who are listed on the Specially Designated Nationals and Blocked Entities List (SDN List) of the US Department of the Treasury's Office of Foreign Assets Control (OFAC). OFAC is an agency within the US Department of the Treasury (USDT) that is responsible for implementing financial sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, weapons of mass destruction traffickers, and other threats to the national security, foreign policy, or economy of the United? States, including human rights abuses and interference with democratic processes.

OFAC requires all US citizens to "block" (i.e., freeze) the assets of the individuals and companies who are engaging in transactions with:

- Countries that are subject to US economic sanctions (i.e., blocked countries);
- Certain companies and entities that act as agents for such countries (i.e., blocked parties); and
- Certain individuals who act as agents for such countries (i.e., SDNs).

To avoid civil and criminal penalties from OFAC for non-compliance, organizations should have a compliance program in place.

One of the most challenging aspects of sanctions compliance when dealing with cryptocurrencies is the fact that although transactions between wallets are generally public and relatively transparent, there may be limited information about the owner of the wallet (usually just a cryptocurrency wallet address). This impedes scrubbing the data against any information available in sanctions lists.

Within the past year or so, OFAC has started using blockchain analytics to track down and blacklist cryptocurrency addresses used by malicious actors who are now being added to the SDN list. In addition to scrubbing data against any sanctions lists, it's critical to check and verify the location of a customer by checking Internet Protocol (IP) addresses associated with the used devices to ensure it isn't associated with one of the sanctioned countries or regions.

Crypto tip: Don't run afoul of sanctions

If your bank's customer decided to accept payments in cryptocurrencies without your bank's involvement, it would be responsible for ensuring that it does no business with any sanctioned individual, party, region, or country. If it decided to accept payments in cryptocurrencies through your bank, your bank's existing processes for sanctions compliance could be deployed to meet these requirements.

Transaction monitoring

It is no secret that due to its pseudo-anonymity and the fact that cryptocurrency transactions require no use of an intermediary (e.g., a bank), cryptocurrencies are used by criminal enterprises for fraud, human trafficking, ransomware, and other illicit activities. And because criminals were early adopters of cryptocurrencies, their initial embrace has continued to shape its overall reputation despite data that suggests the proportion of cryptocurrency-related crime is falling. It is, however, still an issue that requires continuous monitoring of transactional risk.

At its most basic level, transaction monitoring usually involves deploying technology that detects and analyzes unusual transactions in real-time and/or on a daily basis. Such an analysis allows businesses to verify the source and destination of funds and the possible connection of those funds to money laundering.

Transaction monitoring protects an institution's finances and reputation, which can easily be damaged by becoming a focal point of a fraud/human trafficking/other illicit activity type of scandal, as well as allowing an institution to spot suspicious transactions and fulfill its reporting obligations. Monitoring transactions in cryptocurrencies is a little different, however, and it requires the use of blockchain analytics tools.

Identifying the entities connected to addresses often requires proprietary analytical techniques to map transactions and addresses to real-world entities. Chainalysis, a company that provides blockchain analytics tools and services, does this in two steps:

1. Group addresses exhibiting a particular type of transactional behavior into clusters ("clustering"), and

2. Identify the real-world entities (businesses or services, not individuals) that control a group of addresses (“identifications”).

In addition to analyzing transactions in real-time to prevent future payments, an institution may also need to review past transaction activity when cryptocurrency transaction activity becomes suspicious in hindsight due to new information that is uncovered. Continuous monitoring solutions will check to see if their platform previously processed transactions with a now-suspicious or newly sanctioned entity, even if an institution would have had no way of knowing the information previously. If reviews showed their platform did transact with that now-suspicious/sanctioned entity, the institution would need to report those transactions through the appropriate channels.

> A financial institution that does not continuously monitor for newly identified risk in old transactions could find itself in trouble with regulators.

It is worth noting that for some regulated entities, such as financial institutions, this does not just apply to sanctioned entities, but to any entity whose cryptocurrency transaction activity becomes suspicious in hindsight due to new information being uncovered.

For instance, if a cryptocurrency wallet was identified as belonging to a ransomware operator, a financial institution would need to identify any old transactions occurring between that ransomware wallet and addresses hosted by their platform.

A financial institution that does not continuously monitor for newly identified risk in old transactions could find itself in trouble with regulators, who are themselves adopting the same blockchain analysis platforms financial institutions themselves rely on, and can therefore spot historic suspicious activity financial institutions fail to report.

To make it less time-consuming, continuous monitoring solutions usually use automatic alerts that notify financial institutions real-time of any suspicious cryptocurrency transactions. Furthermore, to better focus on critical alerts, most monitoring solutions use customizable alert thresholds that are set based upon an institution’s policies, priorities, and risk tolerance.

Crypto tip: Blockchain analytics is needed for monitoring

If your bank’s customer decided to accept payments in cryptocurrencies without your bank’s involvement, it would be responsible for monitoring its own transactions and deploying blockchain analytics. If it accepted them through your bank, your bank’s transaction monitoring would need to be upgraded to include blockchain analytics data.

Tax

In 2014, the IRS declared that “virtual currency,” such as Bitcoin and other cryptocurrency, is to be treated as property (not as currency) for federal tax purposes and the general principles applicable to transactions involving property apply to transactions involving virtual currency.

A taxpayer that receives virtual currency for goods or services must include the fair market value of the virtual currency, as of the date of receipt, in his or her gross income. A taxpayer also realizes gain or loss on the sale or exchange of a virtual currency, which includes the use of virtual currency to pay for a service and the exchange of virtual currency for another virtual currency. Consequently, every individual or business that owns cryptocurrency generally needs to, among other things:

- Keep detailed records of cryptocurrency purchases and sales,
- Pay taxes on any gains that may have been made upon the sale of cryptocurrency for cash,
- Pay taxes on any gains that may have been made upon the purchase of a good or service with cryptocurrency, and
- Pay taxes on the fair market value of any mined cryptocurrency as of the date of the receipt.

The recent infrastructure bill includes new provisions aimed at cryptocurrency, highlighting evolving initiatives as the government looks to the cryptocurrency industry as a new source of tax revenue.

Because of the risks in this area, many businesses and individuals find that working with a software provider, such as Lukka or other crypto tax software programs, can reduce the risk and uncertainty that comes with the data and reports that are required to be kept and filed with the IRS as it pertains to crypto.

Crypto tip: There are still IRS requirements

Again, to the extent that your bank’s customer decided to accept payments in cryptocurrencies without your bank’s involvement, it would be responsible for ensuring that it complies with all IRS record-keeping and reporting requirements. If it decided to accept payments in cryptocurrencies through your bank, your bank’s existing processes for tax compliance could be deployed to meet these requirements.

A new financial landscape

Cryptocurrencies and cryptocurrency technology present both challenges and opportunities for financial institutions. The regulatory framework around cryptocurrencies continues to evolve as regulators and lawmakers seek to regulate a new financial landscape. It is imperative to understand the legal and other risks for banks and other financial institutions to address new and evolving requirements and mitigate risk. Armed with knowledge and the proper tools, you can show your CEO that cryptocurrencies and related technologies are a mitigable risk with immense opportunity.

Adriana Dulic

Chief Compliance Officer

Epoch Payment Solutions

Adriana Dulic is chief compliance officer at Epoch Payment Solutions where she is responsible for planning, organizing, and leading the implementation of a wide range of legal policies and regulatory compliance, including anti-money laundering, sanctions, privacy, data security, and consumer protection. She is a Certified Anti-Money Laundering Specialist (CAMS), Certified Global Sanctions Specialist (CGSS), and a Certified Information Privacy Professional (CIPP/US and CIPP/E). She is also a member of the board of directors and co-chair of the Association of Certified Financial Crime Specialists' Austin chapter.

Amanda Wick

Chief of Legal Affairs

Chainalysis

Amanda Wick is the chief of legal sffairs at Chainalysis, Inc, which provides data, software, services, and research to government agencies, exchanges, financial institutions, and companies in over 60 countries. Previously, she served as a senior policy advisor at the Financial Crimes Enforcement Network (FinCEN) where she advised on issues involving cryptocurrency, money laundering, and human trafficking. Before that, she served nearly 10 years as a federal prosecutor for the US Department of Justice where she specialized in cryptocurrency money laundering, asset recovery, and BSA/AML issues.

Eric Sibbitt

Partner

Paul Hastings

Eric Sibbitt is partner in the Securities & Capital Markets and co-chair of the Fintech & Payments practices of Paul Hastings and is based in the firm's San Francisco office. Sibbitt represents major trading platforms and other market intermediaries, leading innovators, and prominent investors in navigating the regulatory complexity presented by blockchain and new financial technologies and legacy regulation.