Retail Payments Risk Forum
A CATALYST FOR COLLABORATION

Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks

Douglas King

Retail Payments Risk Forum Working Paper
Federal Reserve Bank of Atlanta
October 2015
Revised February 2016

Abstract: To date, much of the attention directed toward Bitcoin has focused on its use as a preferred payment method by criminal enterprises because it allows users to transact pseudonymously. But Bitcoin offers more than just pseudonymity. It is a fast, low-cost, and secure payment solution that can also be used for many legitimate purposes. As investment and interest in the Bitcoin ecosystem have grown since its 2009 start, new businesses have emerged seeking to advance Bitcoin as a mainstream payment solution. The pseudonymous nature of Bitcoin transactions heighten Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Act compliance risks, making it especially challenging for these new businesses to establish banking relationships.

This paper examines the current regulatory environment for Bitcoin-related businesses as well as measures these businesses can adopt to mitigate the BSA/AML risks inherent in the Bitcoin protocol. It also presents a framework for financial institutions (FIs) to consider for managing the risks associated with banking these companies. This paper is not a replacement, update, or supplement to BSA/AML guidance requirements provided in November 2014 by the Federal Financial Institutions Examination Council (FFIEC). By making a commitment to BSA/AML compliance, Bitcoin-related businesses can both better position Bitcoin as a mainstream payment system and enhance the ability of FIs to successfully bank them.

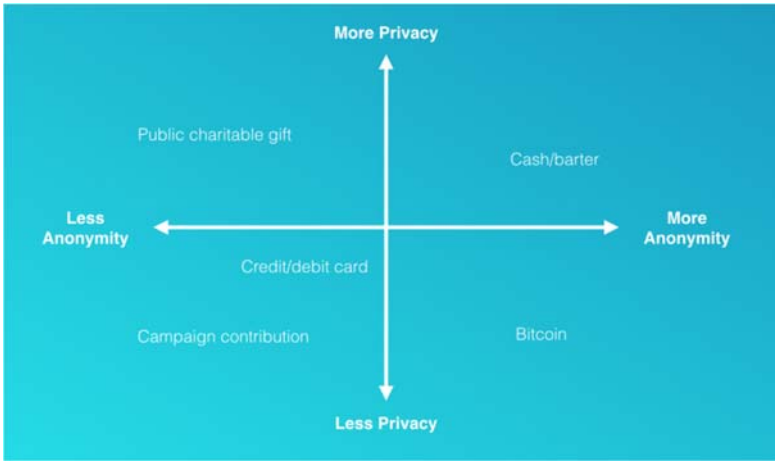
Introduction

Properly balancing risk and reward is vital for financial institutions (FIs) to thrive. When determining whether or not to provide financial services to a prospective customer, FIs need to assess the potential profitability against the various types of risk the prospective customer poses. Types of risks for FIs to consider include strategic, compliance, reputational, financial, and operational risks.

By their very nature, some industries are inherently riskier than others. Companies operating in high-risk industries might find it challenging to develop banking relationships because some FIs decline to do business with them. While these industries may pose an elevated risk as a whole, companies operating within them can take steps to manage the risks. An example of one such industry is virtual currencies and, more specifically, the industry and companies developing around the Bitcoin ecosystem.

A particular risk associated with Bitcoin transactions is complying with regulations related to the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) Act. Bitcoin transactions offer a level of anonymity similar to cash transactions. However, unlike a cash transaction, which is private between entities, a Bitcoin transaction is recorded on a publicly visible, distributed electronic ledger known as the *blockchain*. Despite this transparency, no personally identifiable information (PII) is captured in a Bitcoin transaction, so users can easily obscure their digital identities. In essence, a Bitcoin transaction is pseudonymous. This feature has enabled some people to use Bitcoin to conduct illegal transactions and launder money, and it could be leveraged to fund terrorism.

Figure 1: Privacy and Anonymity Matrix[1]



Although the Bitcoin protocol has been used for commerce supporting illegal transactions, a number of companies, recognizing the BSA and AML risks associated with Bitcoin, are working to bring Bitcoin into the mainstream. These companies offer a range of services to enable individuals and businesses to transact with the Bitcoin protocol and offer the promise of safe, secure, and fast payment transactions. Some of these companies have developed banking relationships while others have had trouble establishing such relationships given the potential BSA/AML risks.

Companies giving individuals access to the Bitcoin ecosystem and enabling individuals and businesses to accept bitcoins as a form of payment can mitigate these risks. This paper describes the different participants in the Bitcoin ecosystem, their current BSA/AML compliance obligations, and BSA/AML considerations for FIs as part of an enhanced due diligence process in light of their related risks.

I. The Bitcoin Ecosystem

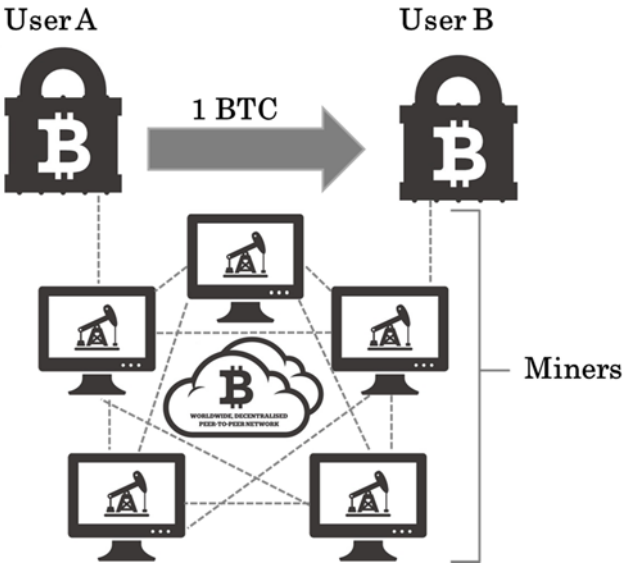
Overview

The Bitcoin protocol is based on a distributed, peer-to-peer network. Two types of participants are vital to this network: *users*, or the individuals or entities that initiate and receive transactions, and *miners*, the individuals or entities that validate transactions.[A] Without users, there would be no Bitcoin transactions. And without miners, there would be no way to validate transactions on the network.

But the Bitcoin ecosystem has grown to include many participants beyond users and miners. These include wallet providers, exchanges, ATM manufacturers and operators, and payment processors. The additional participants play important roles in the ecosystem. They provide access to bitcoins, store bitcoins, and enable businesses to accept bitcoins in exchange for goods and services.

[A] For a more complete description of Bitcoin, including a more technical overview of a Bitcoin transaction, see "Bitcoin: Technical Background and Data Analysis." Anton Badev and Matthew Chen. October 7, 2014.

Figure 2: A Simplified Bitcoin Transaction



Users

Bitcoin users initiate and receive transactions. They can be individuals, companies, or even connected devices that interact with one another via the Internet. Given the anonymity that Bitcoin offers, researchers have struggled to fully identify and understand who the specific users are. Generally, Bitcoin users can be segmented into three different groups: *transactors*, *investors*, and a hybrid of the two.

Bitcoin transactors obtain bitcoins for the purpose of purchasing goods or services or exchanging in person-to-person transactions. For these users, bitcoin usage is limited by the number of retailers and individuals who accept bitcoins in exchange for goods and services. According to reports in early 2015, approximately 100,000 merchants worldwide accept bitcoins.[2] Some larger online merchants are Overstock, Newegg, and Expedia, but the majority tend to be smaller, online-only retailers.

Bitcoin investors obtain bitcoins for speculative purposes. These users do not intend to spend their bitcoins. Rather, they intend to buy and sell them much like a traditional investor trades in company stocks or commodities.

The hybrid bitcoin users both treat bitcoins as an investment and use them to conduct commerce.

Miners

Miners are individuals or entities who validate transactions. A transaction on the Bitcoin network takes approximately 10 minutes. Transactions are collected and turned into a list, called a *block*. Miners use computing power to run the data from the block through a "secure hash algorithm" to create a hash, or a random sequence of letters and numbers. This hash is then added to the blockchain, Bitcoin's distributed public ledger. Each time a miner successfully adds a hash to the blockchain (and effectively validates the transactions of that particular block as well as prior blocks), the miner is awarded newly created bitcoins.

The difficulty of mining is correlated to the number of miners vying to add each new hash to the blockchain as well as the number of bitcoins in circulation. As the popularity of mining has grown and the bitcoins in circulation have increased, the computing power and energy required to solve the secure hash algorithm has also increased. This has led to the formation of mining pools, or groups of individuals who combine their computing power to improve their chances of successfully adding a hash to the blockchain.

Wallet Providers

Just as individuals store physical currency in wallets, bitcoin users also use wallets to store their digital keys, which provide access to bitcoins. Unlike traditional physical wallets, these wallets are digital.

Wallet providers offer options that are software-based (desktop or mobile), cloud-based, or hardware. A cloud-based wallet—such as the Coinbase, Circle, and Xapo wallets—serves as the custodian of a user's private and public keys. Providers generally perform some level of identity verification and act as a gateway for the user to access the Bitcoin protocol.

Software-based and hardware wallet providers do not take custody of the users' keys and generally offer less transparency. They compete for users by offering wallets with added security, ease of use, and additional methods of making bitcoin users' digital keys more private and anonymous.

Exchanges

Bitcoin exchanges allow individuals and other entities to transfer fiat currency into bitcoins, and vice versa. Bitcoin exchanges act as brokers that attempt to match two offsetting transactions (buy order and sell order) involving the acceptance of one type of currency and the transmission of another. Exchanges do not hold an

inventory of bitcoins and fiat currency to fulfill exchange orders; they simply match a buyer to a seller and vice versa. The exchanged funds and bitcoins belong to the buyers and sellers, not the exchange.

To use an exchange, individuals must deposit fiat currency or bitcoins into an account. For most exchanges, individuals' accounts are linked to bank accounts at traditional financial institutions. Once funds are available in the exchange account, account holders can purchase bitcoins through a market order, an instant order to purchase bitcoins at the lowest market price, or through a limit order, a prescribed order to purchase bitcoins at a set price. Bitcoins can also be sold in a similar fashion through these exchanges.

ATM Manufacturers and Operators

Another avenue for obtaining bitcoins is through Bitcoin ATMs. Toward the end of 2014, there were nearly 90 Bitcoin ATMs located in the United States, representing approximately 30 percent of all such ATMs worldwide.[3] There are approximately 20 manufacturers and 30 different models of Bitcoin ATMs with different features and functionality across the globe. Six manufacturers control approximately 90 percent of the installations worldwide.[4] Bitcoin ATMs differ from traditional ATMs and are not manufactured by the same companies. Bitcoin ATMs can be either one-way machines, allowing users only to purchase bitcoins, or two-way machines, allowing users both to purchase and sell bitcoins.

ATM operators purchase the machines from the manufacturers and own and operate the ATMs as a business. Unlike an exchange, which acts as a broker matching bitcoin buyers and sellers, an ATM operator trades bitcoins for fiat currency or vice versa. The ATM operator must maintain an inventory of bitcoins and fiat currency to transact with customers. ATMs come with a variety of features and functionality that assist with mitigating BSA/AML risks, but it is the ATM operators who ultimately decide which features on the machines to enable.

Payment Processors

Just as traditional payment processors facilitate card-based and ACH transactions for businesses, Bitcoin payment processors enable businesses to accept bitcoins as payment for goods and services. These processors can facilitate bitcoin transactions through multiple channels, including e-commerce, mobile, and brick-and-mortar point of sale. Some processors enable multiple channels, others focus exclusively on an individual channel.

Based on contractual agreements between the processors and businesses, the processor can pass the bitcoins through to the business's wallet or they can pass fiat currency through to the business, usually based on a real-time exchange rate between bitcoin and fiat currency. In this case, the business never receives or maintains bitcoins from the sale of goods or services; the processor maintains ownership of the bitcoins.

II. History of BSA and AML Regulations

The Bank Secrecy Act, also known as the Currency and Foreign Transactions Reporting Act, was signed into law by President Richard Nixon on October 26, 1970.[5] This legislation was enacted to help U.S. government agencies detect and prevent money laundering. More specifically, the BSA established requirements for recordkeeping and reporting of specific transactions, including the identity of an individual engaged in the transaction, by banks and other FIs.

The reporting requirement instruments are Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), Currency or Monetary Instrument Reports (CMIRs), and Foreign Bank and Financial Accounts Reports (FBARs).

FIs must file CTRs for transactions by, or on behalf of the same person, totaling $10,000 or more during any one business day (deposit, withdrawal, exchange, or other payment or transfer). Exemptions are made for certain types of businesses that routinely have transactions that would generally meet the filing requirement but these transactions are considered part of their normal course of business and the reporting would not necessarily aid law enforcement authorities.

SARs are to be filed when depository institutions, money service businesses (MSBs), and several other types of businesses defined by FinCEN detect a known or suspected violation of Federal law or a suspicious transaction related to money laundering activity or a violation of the BSA. (MSBs are nonbanking entities that are subject to federal reporting requirements. They are also licensed and regulated at the state level and have additional regulatory compliance obligations on a state-by-state basis.) Transactions that trigger the filing of a SAR include transactions of $5,000 or more that may involve money laundering or violate the BSA. SARs must also be filed for any known or suspected criminal violations involving transactions in aggregate of $5,000 or more when a suspect can be identified. If the institution cannot link transactions to a specific suspect or suspects, then the aggregate value of transactions rises to $25,000 for filing a SAR.

CMIRs must be filed by every party involved in the physical movement of currency or certain other monetary instruments in an aggregate amount exceeding $10,000 into or out of the United States.

FBARs must be filed by every citizen of the United States with an interest in, or authority over, one or more banks, securities, or other financial accounts in a foreign country if the aggregate value of such accounts exceeds $10,000 in any given year.

Since being signed into law in 1970, the BSA has had an additional 11 separate legislative acts and numerous amendments to these regulations.[B] Of note, FinCEN and the Federal Reserve Board amended the BSA regulations in January 1995.[6] Among several changes, this amendment expanded BSA reporting requirements for MSBs. In 2011, FinCEN issued additional guidance expanding the definition of entities required to register as MSBs to include, but not to be limited to, providers of prepaid access, money transmitters, and sellers of prepaid access.[7]

After the terrorist attacks on September 11, 2001, the U.S. Patriot Act (Patriot Act) was signed into law on October 26, 2001.[8] Section 3 of the Patriot Act amends the BSA to further address the prevention, detection, and prosecution of international money laundering and terrorist financing. One of the more substantial changes the Patriot Act brought to the financial services industry was the deepening of the "know your customer" (KYC) process. Specifically, the Patriot Act requires FIs to establish appropriate, specific, and, when necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering or terrorist financing.

In 2003, multiple federal regulatory agencies adopted a rule requiring that all FIs develop and adhere to a customer identification program (CIP).[9] At a minimum, an FI's CIP must include three components: (1) procedures to verify the identity of any individual seeking to open an account, (2) records of the information used to verify the individual's identity, and (3) an indication that the FI verified that the individual does not appear on any lists of known or suspected terrorist or terrorist organizations.

It is important to note that under new regulatory guidance released in November 2014 by the Federal Financial Institutions Examination Council (FFIEC), FIs are strongly urged to flag suspicious customers' accounts.[10] To the extent that a Bitcoin-

[B] For a detailed history of the BSA and subsequent legislative acts, see "A New Framework for Partnership, Recommendations for Bank Secrecy Act/Anti-Money Laundering Reform." Appendix C. American Bankers Association. October 16, 2008.

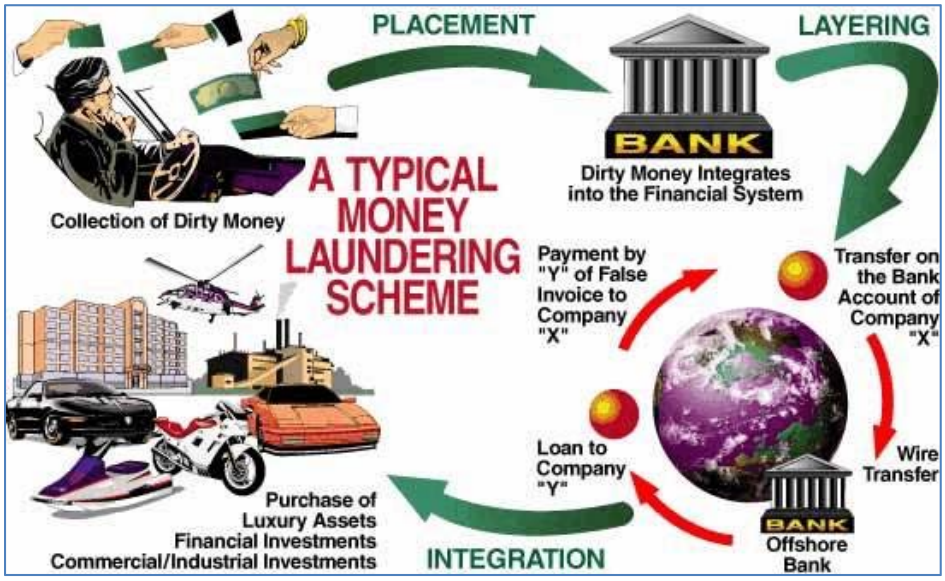
related business customer (or any customer) of an FI facilitates money laundering or terrorist financing for any of its customers, the FI could be subject to BSA/AML-related fines and other disciplinary actions. In 2014, a total of $351 million in fines for AML violations were levied by regulators.[11] This makes it imperative for FIs to be intimately familiar with their direct banking relationships and to understand those relationships' customers and the types of transactions that they are facilitating.

III. Using Bitcoin to Facilitate Money Laundering and Terrorist Financing

The Financial Crimes Enforcement Network (FinCEN) describes money laundering as the process of making illegally gained proceeds (that is, "dirty money") appear legal (that is, "clean").[12] This process is actually a three-stage process and involves the:

1. **Placement** of illegally gained proceeds into the financial system.
2. **Layering** of these proceeds by conducting multiple financial transactions to make detection difficult.
3. **Integration** of these proceeds into the legitimate economy (such as investments in assets or business ventures, purchases of goods and services).

Figure 3: The Money Laundering Cycle[13]



The Bitcoin system can be used to facilitate each step of the money laundering process. Instead of placing dirty money into the banking system, a money launderer, using either a Bitcoin exchange or ATM, can purchase bitcoins using

dirty fiat money and place those bitcoins into a wallet. It should be noted that in most cases, fiat money that is placed into an exchange has first been placed into the traditional banking system, which complicates this laundering process. Once the bitcoins are in a wallet, they can be transferred and layered among multiple wallets until they are ultimately used to purchase goods or services, which could be facilitated by a payment processor or exchanged back into fiat currency through a Bitcoin exchange or ATM.

Some companies have launched products and services aimed at making the money laundering process via Bitcoin more difficult. Exchanges such as Coinbase and Kraken, cloud-based wallet providers, and some ATM operators generally require various levels of identity verification based on transaction velocity and size. These types of companies are often the primary points of access for individuals to Bitcoin. Through BSA/AML programs, they can play an integral role in identifying and mitigating illicit fund flows through Bitcoin.

However, other companies have launched products and services designed to make the money laundering process easier and even openly advertise on the Internet. Two examples are Dark Wallet, which mixes together multiple users' payments in an attempt to make transactions untraceable to individuals,[14] and Bit Launder, an online program used specifically for further anonymizing bitcoin.[15]

In another money laundering scenario, instead of using dirty fiat money to directly purchase bitcoins, dirty money could be used to purchase computer-related hardware to start a Bitcoin mining operation. As this miner earns bitcoins through the mining process, these coins could be layered and placed as described above.

In the two money laundering scenarios just described, each participant in the Bitcoin ecosystem (see section II) has a role in facilitating a money laundering transaction, although some may be unknowingly doing so. Section V discusses the current BSA/AML regulatory compliance obligations for Bitcoin-related companies and Section VI suggests considerations for FIs in managing the BSA/AML risks associated with them.

IV. The Current Regulatory Landscape and Guidance For Bitcoin-Related Participants and Companies

Overview

As is often the case with emerging payments, regulations and regulatory guidance related to Bitcoin and other virtual currencies lag product development. Regulatory agencies face the difficult task of fully understanding these emerging payments and then deciding whether existing or new regulations and guidance are applicable or needed to mitigate the associated risks without hampering innovation. To date, FinCEN and the Internal Revenue Service (IRS) have been the only two federal agencies to take an official position on Bitcoin and other virtual currencies.[c] Also, many state banking agencies have issued warnings to consumers about the risks involved with Bitcoin and virtual currencies. Several states, including New York and California, have been pursuing a regulatory or legislative environment specific to virtual currency companies as they struggle with how best to modernize their money transmission statutes.

Federal

On March 18, 2013, FinCEN issued its initial virtual currency guidance.[16] This interpretive guidance clarified the applicability of the BSA regulations to participants engaged in creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. Rather than focusing on a particular virtual currency, FinCEN opted to refer to virtual currencies generically and defined three participants within its guidance: *users*, *exchangers*, and *administrators*.

FinCEN defines a user as "a person that obtains virtual currency to purchase goods or services." However, this definition does not apply only to transactors, one of the three types of users identified in Section II of this paper. In an administrative ruling, FinCEN applies their definition of user to also include investors, stating that when a "company invests in a convertible virtual currency for its own account, and when it realizes the value of its investment, it is acting as a user of that convertible virtual currency within the meaning of the guidance."[17]

[c] Taxation regulations are outside the scope of this paper. If interested in the tax regulations pertaining to virtual currencies and virtual currency transactions, including Bitcoin, see IRS Notice 2014-21 contained in *Internal Revenue Bulletin 2014-16* (April 14 , 2014), accessible at irs.gov/irb/2014-16_IRB/ar12.html.

An exchanger is defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." Finally, an administrator is defined as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency." Since Bitcoin is decentralized and no entity issues or has the authority to remove bitcoins from circulation, no participant within the Bitcoin ecosystem fits FinCEN's definition of an administrator.

FinCEN concluded that exchangers and administrators, unless a limitation to or exemption from the definition applies, are MSBs, specifically money transmitters, and subject to MSB registration, reporting, and recordkeeping regulations as required by the BSA. FinCEN concluded that users are not MSBs.

Since issuing its initial generic virtual currency guidance in March 2013, FinCEN has issued four administrative rulings in response to participants seeking comment on whether they would be required to register as MSBs.[18,19,20,21] These rulings have provided additional details specific to the Bitcoin ecosystem, including which participants are considered MSBs according to FinCEN. The following table summarizes how FinCEN's guidance and administrative rulings apply to participants in the Bitcoin ecosystem.

Bitcoin Participant	Applicable FinCEN Definition	MSB Registration Status
Users	User	Not Required
Miners	User	Not Required[D]
Wallet Providers[E]	N/A	Not Required
Exchanges	Exchanger	Required
ATM Manufacturers	N/A	Not Required
ATM Operators	Exchanger	Required
Payment Processors	Exchanger	Required

[D] This assumes that the miner uses mined bitcoins for its own purpose and not for the benefit of any other entity. However, a user wishing to purchase goods or services with bitcoin it has mined, which pays the bitcoin to a third party at the direction of a seller or creditor, may be engaged in money transmission and required to register as an MSB.

[E] FinCEN has not issued an administrative ruling specific to wallet providers. Wallet providers can simply provide a user with the means to maintain bitcoins. Alternatively, wallet providers can enable additional functionality that ultimately allows for the transmission of real currency for virtual currency, with the potential to be considered an exchange.

State

Beyond registration as an MSB at the federal level, almost all states require that money transmitters obtain a license to operate within the state. (South Carolina and New Mexico are the only states without licensing requirements.) Operating within a state doesn't necessarily mean that a business needs to have a physical presence in state. Most state regulatory bodies require that any money transmitter that services or solicits a state's citizens obtain a money transmitter license in that state. Hence a money transmitting business with a physical presence in one state but with customers or potential customers in every state will be required to obtain a license in every state that has licensing requirements.

While most of the states have licensing requirements, the requirements are not uniform. In fact, the licensing requirements and related fees can vary significantly between states and some states might choose not to license certain types of money transmitter businesses whereas other states might. It is critical that Bitcoin-related businesses understand the licensing requirements in each state where its products or services could be used and obtain the necessary licenses as required by each state.

Rather than attempting to fit Bitcoin and other virtual currency-related businesses into the category of money transmitters, some states are in the process of creating unique licensing requirements. The New York Department of Financial Services recently adopted a BitLicense requirement for virtual currency businesses that sets specific rules and regulations for these businesses. In California, legislation is pending that would require any virtual currency business to obtain a specific virtual currency license that would be different from the state's traditional money transmitter license.[22] As of yet, the California Department of Business Oversight has not determined how to subject virtual currency businesses to the state's Money Transmission Act or any other banking-related state laws.

V. BSA/AML Considerations for Financial Institutions When Evaluating Bitcoin-Related Companies

General Considerations

An FI's due diligence efforts should be heightened for Bitcoin-related businesses, just as they are for other high-risk industries and businesses. This type of due diligence, referred to as *enhanced* due diligence, requires that FIs go above and

beyond traditional due diligence requirements as outlined by the FFIEC in its BSA/AML Examination Manual. A thorough understanding of both the federal and state-by-state rules and regulations of MSBs and virtual currency companies is paramount for any FI entering into a relationship with a Bitcoin-related business. The FI should understand the Bitcoin ecosystem, the different types of participants, and registration requirements to ensure that their customers are properly registered with federal and state authorities.

The decision to bank Bitcoin-related businesses should be well thought out and become a part of the FI's strategic plan. As part of this plan, the FI should incorporate a vetting process with its board and executives so they are fully aware of the risks associated with banking these types of businesses. Once a decision to bank these businesses is made, an FI should integrate updated policies related to these businesses and their unique BSA/AML requirements into its BSA manual.

Account Opening Procedures

FIs should complete a full risk assessment of a Bitcoin-related business prior to the account opening. This assessment should include a detailed evaluation of the BSA/AML risks and cover the following items.

Registration & Licensing

Before opening an account with a Bitcoin-related business, an FI should confirm the business is properly registered, if required, with FinCEN as an MSB as well as with any states requiring registrations or special licensing.

Based on the most up to-date FinCEN guidance, Bitcoin exchanges, ATM operators, and payment processors must register with FinCEN as MSBs. It could be necessary for a wallet provider to also register with FinCEN should they allow the exchange of real currency for virtual currency. In fact in May 2015, FinCEN ruled that Ripple Trade, a wallet application for a different virtual currency than bitcoin, had to register as an MSB.[23] State registration and licensing requirements vary by state and are currently very fluid.

BSA/AML Compliance Program

For businesses that provide users with access to Bitcoin, it is important that FIs monitor their role in mitigating BSA/AML risks that are inherent in this particular payment system. While some of the businesses have regulated federal and state requirements, these requirements should be viewed as a minimum standard. Any business that provides access to a virtual currency,

Bitcoin included, should have a BSA/AML compliance program in place so that its FI can properly address regulatory requirements. An FI should ensure the existence of a BSA/AML compliance program with any Bitcoin-related business, especially those required to register with FinCEN.

The compliance program should be led by a dedicated BSA/AML compliance officer. Having this individual supported by a dedicated staff of professionals could further demonstrate a business's willingness to comply with BSA/AML laws and regulations. As part of the BSA/AML compliance program, KYC procedures must be in place as well as a CIP that includes an analysis of flow of funds and geographic regions served.

FIs should be aware of the unique KYC and CIP challenges that several of the Bitcoin-related businesses face. Exchanges and wallet providers currently operate in an electronic-only environment and do not offer any brick-and-mortar locations, which means they have to manage their KYC program and CIP electronically, and possibly by mail or phone. Alternatively, they could outsource certain functions to providers with brick-and-mortar resources.

ATM operators generally use the actual ATM to manage their KYC program and CIP. This requires that the ATM is able to capture the relevant customer information and documentation that regulations and their own compliance program require. FIs wishing to bank ATM operators should have an understanding of an operator's portfolio of ATMs, including the manufacturers of their ATMs and their KYC and CIP capabilities.

The KYC procedures of Bitcoin payment processors should include an underwriting process for any merchant account. As part of this underwriting process, the processor should consider a merchant's business type, geographic locations, customer types, length in business, experience with other forms of payments, and financial health. It is important that the payment processor understand a merchant's motivation for enabling bitcoin transactions. It could be a red flag for the processor if a merchant has lost the ability or is unable to process card or other electronic transactions. This could be the result of the merchant selling illegal items or having a large volume of chargebacks, returns, or customer complaints stemming from deceitful sales tactics or poor product quality.

In addition to ensuring that Bitcoin-related businesses have KYC and CIP procedures in place, FIs should also ensure that they have a transaction monitoring program in place as part of their BSA/AML compliance program.

> In a May 2015 settlement with the Justice Department and FinCEN, a virtual currency business (not Bitcoin-related) was assessed a $700,000 penalty for failing to follow AML rules. As part of the settlement, the company agreed to build analytical transaction monitoring tools for monitoring transactions across the protocol. [24]
>
> While not a regulatory requirement, a transaction-monitoring program would benefit from some level of automation, either rules-based or statistical profile-based, identifying potentially suspicious transactions that might require a more detailed manual review. A rules-based automated program would identify transactions that meet certain predefined criteria while a statistical profile-based program would identify transactions that appear unusual given the transactional history. Once a program is in place, it should be periodically evaluated to determine its effectiveness and efficiency, and then enhanced to compensate for any deficiencies.

Due Diligence Reviews

Once an FI enters into a business relationship with a Bitcoin-related business, ongoing due diligence of that business will need to confirm that the account opening was appropriate. Given the higher-risk nature of these businesses and the need for enhanced due diligence, annual reviews may not be sufficient but should be viewed as a minimum threshold for ongoing due diligence reviews. Regardless of the frequency of reviews, it is a best practice to incorporate an onsite visit at least annually.

As part of these reviews, FIs should ensure that the customer has obtained or maintained the proper FinCEN and state-level registration and licensing requirements, especially given the fluidity of these requirements. Although an FI's account agreement with the customer requires the business to promptly notify the FI of any substantial changes in its business operations, it should still monitor for any changes to the BSA/AML compliance program and customer profiles or behaviors during these reviews. If the customer has an independent review of its compliance program, which is recommended, the FI should obtain and assess the results of that review.

Within its account agreement with a customer, an FI may want to consider including the right to audit the customer's BSA/AML compliance program and procedures as part of its ongoing enhanced due diligence process. This audit will allow an FI to test its customer's BSA/AML procedures as they choose.

Ongoing Transaction Monitoring

While FIs need to ensure that Bitcoin-related businesses incorporate transaction monitoring as a part of their BSA/AML compliance program, FIs should also have transaction monitoring procedures in place to monitor the activities of their customers. This monitoring program should be risk-based to identify high-volume or high-value transactions that should be analyzed for further review. Transactions that seem out of the ordinary for specific clients, such as international transactions for a client that generally only transacts domestically, should also be analyzed. While these transactions could be legitimate, they could also point to money laundering or other illegal activities and an analysis of these transactions could determine whether a SAR should be filed.

While not directly a BSA/AML issue, FIs should be aware that Office of Foreign Assets Control (OFAC) monitoring is currently a major challenge for Bitcoin-related businesses and their FI partners. Since only a public key, and no PII, is needed to send a transaction to another party, knowing where and to whom a transaction is going is very difficult. The Bitcoin protocol isn't currently designed to collect and provide this type of information for transactions. Companies within the ecosystem are developing and contemplating solutions to address this issue, and FIs should continue to monitor and understand what these companies are doing to ensure OFAC compliance such as IP address tracking and identification.

Information Sharing

Section 314(b) of the Patriot Act provides a safe harbor and liability protection for a wide range of FIs that have chosen to share information with another.[25] Given that FIs along with the different businesses described within this paper all play a role in the lifecycle of a Bitcoin transaction, information sharing between and among these entities could be critical to identifying suspicious activity. FinCEN's July 2014 SAR Stats Technical Bulletin outlines the unique vantage point the different entities bring to a Bitcoin transaction and "encourages the use of information sharing under 314(b)."[26]

VI. Conclusion

The Bitcoin protocol carries the promise of allowing for fast, low-cost, and secure payment transactions. However, its pseudo-anonymous structure also brings with it a number of risks, including the facilitation of money laundering and illegal transactions.

Given these BSA/AML-related risks and others associated with Bitcoin transactions and its highly publicized history of facilitating payments for illegal transactions, the Bitcoin ecosystem is considered high risk by many regulatory agencies and financial institutions. With some FIs in a risk-reduction mode, many are opting to avoid this industry as a whole. However, within this high-risk category, there remain many legitimate uses for bitcoin and businesses that facilitate these legitimate transactions.

The Bitcoin ecosystem has evolved to include a number of different businesses that help consumers and businesses access it. Along with allowing access, these businesses are also in a position to mitigate inherent risks that are at the core of Bitcoin's pseudo-anonymous payment protocol. Some state and regulatory agencies have identified this aspect of these businesses and have applied existing, or are in the process of developing, rules and regulations with which these businesses must comply.

FIs interested in banking Bitcoin-related businesses should have a full understanding of the Bitcoin ecosystem, the role of the different participants, and the unique BSA/AML circumstances involving this ecosystem. A robust BSA/AML enhanced due diligence process is necessary when evaluating Bitcoin-based businesses.

Beyond regulatory requirements, Bitcoin-related businesses can adopt certain processes and practices that have the ability to even further legitimize the Bitcoin transactions that they are enabling. By focusing on a commitment to BSA/AML compliance through a robust compliance program, Bitcoin-related businesses can better position themselves for banking relationships with FIs. In return, this dedication to compliance ultimately places FIs in a better position to successfully bank them.

References

[1] Ludwin, Adam. 2015. "How Anonymous is Bitcoin? A Background for Policymakers." *Coindesk*, January. Retrieved from coindesk.com/anonymous-bitcoin-backgrounder-policymakers/, accessed on April 6, 2015.

[2] Cuthbertson, Anthony. 2015. "Bitcoin Now Accepted by 100,000 Merchants Worldwide." *International Business Times*, February. Retrieved from ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613, accessed on May 18, 2015.

[3] Wong, Joon Ian. 2014. "6 Charts That Show Massive Bitcoin ATM Growth in 2014." *Coindesk*, December. Retrieved from coindesk.com/6-charts-show-massive-bitcoin-atm-growth-2014/, accessed on June 8, 2015.

[4] CoinATM Radar Blog. 2014. "How to Buy Bitcoins with Bitcoin ATM," October. Retrieved from coinatmradar.com/blog/how-to-buy-bitcoins-with-bitcoin-atm/, accessed on May 14, 2015.

[5] *See* Public Law 91-508 (Oct 26, 1970). Retrieved from gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf, accessed on May 19, 2015.

[6] *See* Amendment to the Bank Secrecy Act Regulations Relating to Recordkeeping for Funds Transfers and Transmittals of Funds by Financial Institutions, 60 Fed. Reg. 220 (Jan 3, 1995) (to be codified at 31 C.F.R. pt. 103).

[7] *See* Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45404 (July 29, 2011) (codified as amended at 31 C.F.R. pts. 1010 and 1022).

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat.272.

[9] *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25109 (May 9, 2003) (to be codified at 31 C.F.R. pt. 103.121).

[10] Federal Financial Institutions Examination Council. 2014. "Bank Secrecy Act / Anti-Money Laundering Examination Manual," November.

[11] Nguyen, Bao. 2015. "Regulators Issued Fewer AML Fines in 2014, but Packed a Bigger Punch," February. Retrieved from krfs.com/news/regulators-issued-fewer-aml-fines-in-2014-but-packed-a-bigger-punch/, accessed on June 11, 2015.

[12] Financial Crimes Enforcement Network. "History of Anti-Money Laundering Laws." Retrieved from fincen.gov/news_room/aml_history.html, accessed on May 18, 2015.

[13] United Nations Office on Drugs and Crime. "The Money Laundering Cycle." Retrieved from unodc.org/unodc/en/money-laundering/laundrycycle.html, accessed on May 18, 2015.

[14] Greenberg, Andy. 2014. "Dark Wallet Is About to Make Bitcoin Money Laundering Easier Than Ever." *Wired.com*, April. Retrieved from wired.com/2014/04/dark-wallet/, accessed on June 9, 2015.

[15] bitlaunder.com/bitcoin-tumbler, accessed on June 9, 2015.

[16] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." FIN-2013-G001 (March 18, 2013).

[17] "Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity." FIN-2014-R002 (January 30, 2014).

[18] "Application of FinCEN's Regulations to Virtual Currency Mining Operations." FIN-2014-R001 (January 30, 2014).

[19] Id. 12

[20] "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform." FIN-2014-R011 (October 27, 2014).

[21] "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System." FIN-2014-R012 (October 27, 2014).

[22] AB-1326 Virtual Currency. California Legislature 2015-2016 Regular Session. leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326

[23] Casey, Michael J. 2015. "BitBeat: Day after FinCEN Bombshell, Ripple Labs Addresses Concerns." *Wall Street Journal*'s *Money Beat* blog, May. Retrieved from blogs.wsj.com/moneybeat/2015/05/06/bitbeat-day-after-fincen-bombshell-ripple-labs-addresses-concerns/, accessed on June 22, 2015.

[24] Tracy, Ryan. 2015. "Treasury Penalizes Ripple Labs, in First Action Against Virtual Currency Exchange." *Wall Street Journal*, May. Retrieved from

wsj.com/articles/treasury-penalizes-ripple-labs-in-first-action-against-virtual-currency-exchange-1430864628, accessed on June 22, 2015.

[25] Financial Crimes Enforcement Network. 2013. "Section 314(b) Fact Sheet," October. Retrieved from fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf, accessed on June 2, 2015.

[26] Financial Crimes Enforcement Network. 2014. "SAR Stats Technical Bulletin," July. Retrieved from fincen.gov/news_room/rp/files/SAR01/SAR_Stats_proof_2.pdf, accessed on July 20, 2015.