Cryptocurrency Compliance:
An AML Perspective

Authored By:
Sherri Scott
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Blockchain for Blockheads</td>
<td>3</td>
</tr>
<tr>
<td>RegTech</td>
<td>5</td>
</tr>
<tr>
<td>Sanctions</td>
<td>7</td>
</tr>
<tr>
<td>Transaction Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Exponential Growth</td>
<td>7</td>
</tr>
<tr>
<td>How to Audit FIs Servicing the Cryptocurrency Industry</td>
<td>8</td>
</tr>
<tr>
<td>Conclusion - Unity in the Financial Intelligence Community</td>
<td>10</td>
</tr>
<tr>
<td>Exhibit A: The Association of Accounting Technicians (AAT) Reference Document</td>
<td>11</td>
</tr>
<tr>
<td>Exhibit B: Bitcoin Reference Guide</td>
<td>12</td>
</tr>
<tr>
<td>Exhibit C: Money Service Business (MSB) Compliance Checklist</td>
<td>13</td>
</tr>
<tr>
<td>Exhibit D: Currency Crimes - Federal Money Laundering Laws</td>
<td>15</td>
</tr>
<tr>
<td>Exhibit E: Examination Procedures</td>
<td>16</td>
</tr>
</tbody>
</table>
Executive Summary

October 31, 2017, marks the 9th anniversary of Bitcoin's introduction to the world, and there is yet a consensus to be made on how to regulate the cryptocurrency industry. Chances are unlikely that little ghouls and boys will receive bitcoins while Trick-or-Treating this year. It is likely that future gifts will involve e-cards containing cryptocurrency.

The U.S. Statue of Liberty is globally recognized as a symbol of freedom. Home of the infamous 9/11 attacks and the heart of the U.S. where the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 was conceived. Better known to anti-money laundering (AML) professionals as the ten-letter abbreviation we hold dear to our hearts, the “USA PATRIOT Act”—An Act of Congress that was signed into law by President George W. Bush on October 26, 2001.1

Today, Lady Liberty also symbolizes the birthplace of cryptocurrency regulation. The New York State Department of Financial Services (NYDFS) was an early adopter and embraced the financial technology (Fintech) industry. The NYDFS finalized the first regulatory framework in the nation and created BitLicenses, which are now being actively awarded to Virtual Currency Exchanges (VCEs). The Office of the Comptroller of the Currency (OCC) is now challenging the State regulator in a game of Double Dutch as they play jurisdictional jump rope. Which agency will win the argument over legal charter authority?

While consistent regulation is lacking, virtual currency exchanges (VCEs) are being denied fair banking services because they are being “de-risked” by financial institutions (FIs). The discrimination from fair banking services VCEs are facing is comparable to the medical marijuana industry. Unlike its high-risk counterpart, Fintech innovators operate in a field that is federally legal. We will embark on a journey through a brief history of cryptocurrency, the tides of regulation, and the storms to come.

Blockchain for Blockheads

An anonymous entity known as Satoshi Nakamoto published a white paper2 titled “Bitcoin: A Peer-to-Peer Electronic Cash System” through a cryptography mailing list on October 31, 2008. The concept is simple: reduce consumer costs by eliminating the banking system from peer-to-peer transactions. The infamous white paper solved the problem of double spending by having an open ledger verified by a consensus of independent individuals. The Association of Accounting Technicians (AAT) put together visual representations that describe both Bitcoin the protocol and the system for spending bitcoins, which can be found on their website4 as well as Exhibit A.

Individuals can download free software to create a virtual wallet (VW). The VW is similar to an investment account held at a brokerage firm. Funds are transferred into the account and remain in the form of fiat money (government designated currency) until invested/converted into cryptocurrency. Each VW has a unique identifier, analogues to an account number or email address. The owner generates a secret key, equivalent to a long alphanumeric pin number, which is unique to each VW and necessary to complete a transaction.

1 Wikipedia Website https://en.wikipedia.org/wiki/Patriot_Act
2 Image Source << https://www.pinterest.com/pin/384424518169643559/ >>
Virtual currency exchanges manage virtual wallet accounts and are responsible for obtaining customer information and performing due diligence to the same standard of expectation required by any money services business (MSB). The virtual wallet is initially funded by transferring fiat money from an account held at a financial institution, or transferring cryptocurrency from another virtual wallet. Although VCEs do not accept cash deposits, customers can deposit cash into a virtual wallet through a cryptocurrency Automated Teller Machine (ATM). Mining is another method used to obtain cryptocurrency. Mining is a reward that can be earned when an individual or entity participates in the process of verifying the legitimacy of transactions on the public ledger.

**Figure 1: How Cash Turns Into Cryptocurrency**

![Image of a diagram showing how cash turns into cryptocurrency](Image)

The transactions are completely transparent with values flowing from one unique identifier to another and are maintained on a public ledger for all to see. Transfers are timestamped and confirmed by a consensus of independent miners. Transactions that occurred during the same interval are grouped together and recorded in chronological blocks of time. Details such as the time, amount, unique identifier of the sender and unique identifier of the receiver are eternally documented. From inception, when first mined, to transfer, and ultimately converted to fiat currency, all movement is noted in the chain of history. This is how the term “blockchain” was born.

According to CoinMarketCap.com, 927 virtual currencies totaling $100,114,992,312 are in existence today. Bitcoin dominates 41 percent of the $100 billion market. Most alternate virtual currencies created with blockchain technology are based off some derivative of bitcoin. According to Coin ATM Radar there are currently 1,323 virtual currency ATMs operating in 56 countries. Coinbase reports that over 46,000 businesses accept virtual currencies, such as PayPal, Dell, Dish, Expedia, Overstock.com, USAA, and Bloomberg, to name a few. A general breakdown of bitcoin denominations can be found in Exhibit B.

A global leading tax administrator and the Treasury Department’s trillion dollar revenue earning bureau, the Internal Revenue Service (IRS), weighed-in on the issue in March 2014. The IRS classifies virtual currency that has an equivalent value in fiat money (bitcoin being one of them) as a “convertible virtual currency” (IRS 2014-21). For U.S. federal tax purposes, convertible virtual currencies are treated as “property” and are subject to existing tax principles for property transactions. Individuals that mine bitcoins are responsible for legally claiming the fair market value as gross income at that point in time, regardless of when the funds held in a virtual wallet are converted into fiat money. Depending on whether or not the property is a capital asset, the gain or loss in value will be determined at the point in time when the property held in the virtual wallet is converted fiat money.

Continued innovation and virtual intelligence is rapidly evolving. Blockchain technology can be used for far more than peer-to-peer transfers of virtual currency. Blockchain technology can be used to securely transfer electronic data and is being considered as a solution for many industries, such as healthcare and insurance. In addition, an article published by The Economist listed “5 applications for blockchain in your business” as follows:

1. Smart contracts
2. Cloud storage
3. Supply-chain communications and proof-of-provenance
4. Paying employees

---

5 CoinMarketCap.com Figures as of 2nd Quarter 2017 Website [https://coinmarketcap.com/all/views/all/](https://coinmarketcap.com/all/views/all/)
6 Coin ATM Radar Figures as of 2nd Quarter 2017 Website [https://coinatmradar.com/](https://coinatmradar.com/)
5. Electronic voting
RegTech

It does not take a boxing enthusiast to appreciate the epic regulatory bout occurring between the New York State Department of Financial Services (NYDFS)\textsuperscript{11} and the Office of the Comptroller of the Currency (OCC).\textsuperscript{12} Conflict regarding regulatory jurisdiction of the virtual currency exchanges continues to escalate.

Responsible for promoting uniformity and consistency in the supervision of financial institutions, the Federal Financial Institutions Examination Council (FFIEC)\textsuperscript{13} is an interagency body that houses the combined agency Bank Secrecy Act (BSA)/anti-money laundering (AML) examination manual.\textsuperscript{14} In addition to training state and federal examiners, the FFIEC creates federal examination standards for the supervision of FIs.

**Federal Financial Institution Regulators**

- Board of Governors of the Federal Reserve System (FRB):\textsuperscript{15} state-chartered/federal reserve member
- Federal Deposit Insurance Corporation (FDIC):\textsuperscript{16} state-chartered/non-member federal reserve
- National Credit Union Administration (NCUA):\textsuperscript{17} state-chartered credit unions/federal credit unions
- Office of the Comptroller of the Currency (OCC):\textsuperscript{5} state-chartered/federal reserve member
- Consumer Financial Protection Bureau (CFPB):\textsuperscript{18} FIs and NBFI s operating in the U.S.

Virtual currency exchanges qualify as money transmitters (MTs), a subcategory of money service businesses (MSBs), under the BSA 31 U.S.C. § 5312(a)(2)\textsuperscript{19} and 31 C.F.R. §§ 1010.100(t), 1010.100(ff).\textsuperscript{20} The FFIEC Examination Manual\textsuperscript{21} lists an MSB as a non-bank financial institution (NBFI). In accordance with state legislation, an MSB is required to obtain licensure with the state(s) where it is incorporated and/or conducting business. In addition, MSBs are required to register with FinCEN. The author of this paper compiled a compliance checklist that can be used for VCEs, Exhibit C, based on current MSB regulatory requirements.

In March 2013, FinCEN published FIN-2013-G001,\textsuperscript{22} Guidance on the Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual currencies. FinCEN confirmed initial BSA interpretations and announced government recognition of VCEs as MTs that fall under the MSB classification. This meant that any entity conducting business as a virtual currency exchange better immediately register with FinCEN and ramp up efforts to create a sound AML compliance program.

This position was further evidenced two years later with the first enforcement action against a VCE when FinCEN and the U.S. Attorney’s Office for the Northern District of California (USAO-NDCA) slapped Ripple Labs, Inc\textsuperscript{23} with a $700,000 civil monetary penalty (CMP). A blatant disregard to report suspicious activity and implement an effective AML program, Ripple Labs, Inc. and its subsidiary, XRP II, LLC (formerly XRP Fund II, LLC), were facing criminal charges. To avoid a criminal investigation, Ripple Labs, Inc. signed a settlement agreement\textsuperscript{24} with the USAO-NDCA. Ripple bounced back a year later and was awarded the second BitLicense by the NYDFS.

Confused bitcoin miners received confirmation about whether or not they were required to register with FinCEN nearly a year later. FinCEN Administrative Ruling FIN-2014-R007\textsuperscript{25} made it clear that individuals mining for personal use, and entities that buy and sell as an investment, need not register.

**Note:** Information regarding federal money laundering laws can be found in Exhibit D.

\textsuperscript{11} New York State Department of Financial Services [http://www.dfs.ny.gov/](http://www.dfs.ny.gov/)
\textsuperscript{12} Office of the Comptroller of the Currency [https://www.occ.gov/](https://www.occ.gov/)
\textsuperscript{13} Federal Financial Institutions Examination Council (FFIEC) [https://www.ffiec.gov/](https://www.ffiec.gov/)
\textsuperscript{15} Board of Governors of the Federal Reserve System (FRB) [https://www.federalreserve.gov/](https://www.federalreserve.gov/)
\textsuperscript{16} Federal Deposit Insurance Corporation (FDIC) [https://www.fdic.gov/](https://www.fdic.gov/)
\textsuperscript{17} National Credit Union Administration (NCUA) [https://www.ncua.gov/Pages/default.aspx](https://www.ncua.gov/Pages/default.aspx)
\textsuperscript{18} Consumer Financial Protection Bureau (CFPB) [https://www.consumerfinance.gov/](https://www.consumerfinance.gov/)
\textsuperscript{23} FinCEN Ripple Labs, Inc. CMP [https://www.fincen.gov/sites/default/files/shared/Ripple_Assessment.pdf](https://www.fincen.gov/sites/default/files/shared/Ripple_Assessment.pdf)
\textsuperscript{24} Ripple Labs, Inc. Settlement Agreement [https://www.justice.gov/file/421636/download](https://www.justice.gov/file/421636/download)
The NYDFS began VCE inquiries in 2013, proposed and finalized regulations by June 2015, and started issuing BitLicenses in September 2015. Two quarters later in March 2016, the OCC publication on responsible innovation appeared to show a willingness to support VCEs through agency collaboration:

“Supervision of the financial services industry involves regulatory authorities at the state, federal, and international levels. Exchanging ideas and discussing innovation with other regulators are important to promote a common understanding and consistent application of laws, regulations, and guidance. Such collaborative supervision can support responsible innovation in the financial services industry.”

In October 2016, Michael Benardo from the FDIC RMS Cyber Fraud and Financial Crimes section published a PowerPoint deck, which stated “States are grappling with how to deal with virtual currency” and noted “No federal licensing requirements...” Two months after Bernardo’s presentation and more than a year after the innovation publication, the OCC came out with a proposed solution. The agency laid out the framework for a national charter option for VCEs. In December 2016, the OCC published a paper titled “Exploring Special Purpose National Bank Charters for Fintech Companies.” Fintech companies would have the opportunity to obtain a Special Purpose National Bank (SPNB) charter from the OCC. The paper describes a system where Fintech companies would be regulated the same as FIs, thus promoting uniform enforcement of safety and soundness laws. Since Fintech companies do not take cash deposits, the OCC indicated that VCEs would not be FDIC insured; therefore, not subject to FDIC examinations. New York-based VCE, Gemini, partnered up with neighboring Signature Bank and is able to provide its customers up to $250,000 of FDIC insurance for the cash value in an account (does not cover funds converted to cryptocurrency).

**SPNB Charter Application Minimum Expectations**

- Robust business plan
- Governance structure
- Capital
- Liquidity
- Compliance—Risk management
- Financial inclusion

Maria Vullo, NYDFS superintendent, responded to the proposal citing the state’s jurisdiction and opposition to the SPNB charter. Although the OCC did not formally respond to the concerns addressed by the NYDFS, Comptroller Curry made the agencies stance well known with public comments at a LendIT conference, ironically held in NYDFS stomping grounds.

A year after introducing the SPNB concept, the OCC presented a draft supplement to the Comptroller’s Licensing Manual for the Fintech charter. Superintendent Vullo, with the support of Governor Cuomo, swiftly responded with a formal letter to Comptroller Curry. A timeline of events is located in Exhibit B. The outcome of this Fintech feud will shape the industry and how it is regulated moving forward.

---

26 NYDFS Timeline Website: [http://www.dfs.ny.gov/about/press/pr1509231.htm](http://www.dfs.ny.gov/about/press/pr1509231.htm)
35 Image Source << [https://www.pinterest.com/ledgerwallet/bitcoin-editorial-cartoons/]>
Sanctions

Swedish investment firm, Brave New World Investments, does not need to legally comply with U.S.-based sanctions against Iran. Cryptocurrency allows the investment firm to maintain an Iranian equity account to conduct business while Swedish FIs remain unwilling to provide them with banking services.\(^\text{36}\)

How does one determine if a numbered account correlates to a sanctioned entity? The true beneficial ownership of existing anonymous numbered accounts remains a challenge. The blockchain does not store Internet Protocol (IP) addresses or any information that can be used to identify the account owner. Entities are able to block IP addresses, Virtual Private Network (VPN) proxies, etc., from being used on their proprietary systems. Unfortunately, there are several ways to conceal an IP address and circumvent VPN blocks.

Beneficial ownership can only be confirmed on customer accounts. All transactions stored on the blockchain are from one numbered account to another. In most cases, the identity is only known for one side of that transaction. The downside is that a bad actor can easily open another account within minutes.

The Office of Foreign Asset Control (OFAC) has the ability to publish VW numbers associated with Specially Designated Nationals and Blocked Persons List (SDNs). The FIs and VCEs need to implement systems that can screen an SDN account list containing blocked VW account numbers prior to finalizing a transaction. In some cases, the funds attempted to be transferred to the sanctioned entity should be neutralized pending the results of a timely investigation.

Transaction Monitoring

Numbered accounts require transaction monitoring. Although anonymity may prevent an FI or VCE from determining the party on the other end of a transaction, it cannot prevent algorithms from identifying patterns and behaviors that are indicative of money laundering. The same thresholds and red flags apply as they would for any other high-risk line of business. A bonus of the blockchain is that the history is cemented in a public ledger for all to see. Once a numbered account is associated with criminal activity, data derived from the blockchain can be compiled to formulate powerful intelligence for law enforcement. These systems need to be well thought out and in place before opening an account.

Exponential Growth

The third BitLicense was awarded this year to the largest VW provider and the most popular VCE in the world, Coinbase. Last year the firm opened 635,000 new accounts, according to Wikipedia.\(^\text{37}\) On top of IRS requests for customer account information, Coinbase users experienced ID verification failures in March of this year.

With VCEs not accepting cash deposits, sources must be transferred from an existing FI account, deposited through a virtual ATM, or transferred from another VW. This process alleviates CTR filings by the VCE; however, it does not eliminate the need to file SARs. Failing to implement and adhere to an adequate AML compliance regime will result in a massive blow to a non-compliant VCE, and possibly the FI that services the entity. In addition to being hammered with a CMP and fines from FinCEN, humiliation could ensue in the form of a consent order.


How to Audit FIs Servicing the Cryptocurrency Industry

Size does not matter when it comes to compliance. Regulatory expectations are the same regardless of the size and complexity of any financial institution that wishes to provide banking services to virtual currency exchanges. Employees of financial institutions should utilize the checklist located in Exhibit C. The term MSB, not VCE, is used throughout the checklist. FinCEN declared that virtual currency exchanges are a type of MSB in March 2013, when it published FIN-2013-G001. Through transference, this makes the use of the checklist valid for any financial institution wishing to evaluate its relationship with a virtual currency exchange.

Auditors of financial institutions that provide banking services to virtual currency exchanges should refer to Exhibit E. In this instance, the terms “MSB” and “NBFi” can once again be substituted for VCE, as per the same FinCEN guidance referenced in the previous paragraph. These examination procedures were pulled directly from the FFIEC Examination Manual. For all the other FIs that choose not to frolic in Fintech fun, you are not off the hook! Education and training is necessary to prevent and/or identify bad actors attempting to use your systems.

FIs that bank VCEs need to consider all potential risks. Unfortunately, it sometimes takes severe yet honest audit exceptions and/or an enforcement action to force an FI to remedy compliance program weaknesses and provide the compliance department with necessary resources.

Scope
Determining the audit scope and estimated hours/pricing for an emerging industry is challenging. The scope must be clearly stated and hours estimated. A price for hours exceeding expectations should always be included in the statement of work. Audits typically involve stumbling on issues that neither party wishes to encounter.

Audit Considerations
- Board minutes
  - Strategic plan
  - Board approved budget
- Adverse media (i.e., enforcement actions, pending lawsuits, etc.)
- Significant changes (i.e., balance sheet composition, beneficial ownership/control)
- Prior audits and findings
- Reports of examination (ROEs)
  - CAMELS Ratings
    - Capital adequacy
    - Assets
    - Management
    - Earnings
    - Liquidity
    - Sensitivity to market risk

Board Minutes/Budget
The Board of Directors (the Board) must be actively involved in the decision to provide banking services to the cryptocurrency field. The risk appetite should be clearly documented and commensurate with the strategic plan. Check the Board minutes to ensure the topic was adequately addressed and that the Board is fully aware of the risks, including personal liability. The Board needs to be aware of the dangers of being negligible.

Engaging in high-risk industries requires healthy CAMELS ratings and consultation with regulators prior to offering banking services. While maximizing shareholder value is the primary goal, it must be executed in a safe and sound manner that requires a considerable investment in compliance.

Review the board approved budget and be alarmed if overhead is flat. The budget needs to reflect anticipated increases related to compliance expenses.

Compliance Costs and Budget Considerations
- Human Capital/Consulting/Training Costs (initial and ongoing)
- Monitoring Software/Implementation Costs
- Independent Model Validation/Testing
- Internal/External Audits/Regulatory Examinations

---


**Crypto Compliance Policy**
The policy needs to be robust, well defined, and separate from the existing BSA/AML policy. Governance has to be clearly prescribed and responsibilities appropriately delegated. A committee must be formed to oversee the implementation of the new line of business and be held accountable for program oversight. Policy limits need to be established as a quantifiable metric (i.e., % of Core Deposits, % of Capital, etc.). Monthly tracking and reporting of policy metrics should be presented to the Committee and the Board regularly.

**MSB Risk Assessment**
A departmental as well as an enterprise-wide risk assessment must be performed to identify existing and emerging issues. The auditor needs to gauge the risk profile based on the documentation provided during the scoping process listed above under “Audit Considerations.” This process will help determine the sample sizes needed for the review.

Provide an overall assessment that evaluates all the risk factors involved and determine the score and/or rating for each component. Even when only conducting an AML audit, make sure to look at the entity as a whole and determine if the FI is in a position to service a high-risk line of business that demands a strong compliance program.

According to the FFIEC Manual, make sure the FI is taking the following factors into consideration when risk-weighting its MSB customers. Resources should be allocated in proportion to the level of risk associated with an account.

- Purpose of the account (i.e., payroll, operating account, etc.)
- Anticipated account activity (i.e., type and volume)
- Types of products and services offered by the MSB
- Locations and markets served by the MSB

**Designated BSA Officer**
The designated BSA officer is listed in the BSA/AML policy. As the auditor, you must assess whether or not the BSA officer has the skills and resources necessary to run an effective compliance program. If the existing BSA officer is not capable of managing the additional responsibilities associated with the new line of business, a separate individual should be appointed as the crypto compliance officer.

A token compliance officer will not suffice. High-risk lines of business require skilled and seasoned AML professionals capable of implementing and executing an exceptional AML compliance program. The BSA officer needs to have a seat at the table (the one in the board room and not the kiddie table at Thanksgiving).

- The BSA officer must possess requisite knowledge of the cryptocurrency industry
- The BSA officer and staff should have training and experience managing high-risk lines of business
- From front-line staff to the chairman of the board, enterprise-wide training must be sufficient
- The board must be held accountable and provide adequate resources for the BSA officer
- Regulation demands that the BSA officer report directly to the board (should be reflected in the minutes)

**Digital Due Diligence**
Creating banking procedures for an emerging trend is a difficult task. With regulators nearly a decade behind the technology, it complicates the matter even further. The best place to start is to build procedures based on existing requirements and best practices used for accounts with a higher risk of money laundering.

Although FinCEN’s Final Rule Customer Due Diligence Requirements for Financial Institutions⁴⁰ requires beneficial ownership (BO) to be determined at a minimum of 25 percent, the industry standard will most likely end up somewhere in the 10 percent range for higher risk relationships.

- Make sure the Customer Information Program (CIP)/know your customer (KYC) program is adequate
- Review the adequacy of the know your customer’s customer (KYCC)/customer due diligence (CDD) program(s)
- Ensure the FI is properly risk rating clients and performing enhanced due diligence (EDD) in a timely manner

**Note:** Detailed MSB Risk Mitigation and Due Diligence Expectations can be found in Exhibit C.

---

Unity in the Financial Intelligence Community

On May 26, 2016, Jamal El-Hindi, deputy director of FinCEN, addressed attendees of the Conference of State Bank Supervisors (CSBS) Federal Supervisory Forum. El-Hindi stated, "MSBs play an important role in a transparent financial system, particularly because they often provide financial services to people less likely to use traditional banking services and because of their prominent role in providing remittance services, both domestically and abroad."

When it comes to MSBs, the El-Hindi mentioned that FinCEN is focused on four key areas:

1. Transparency of the MSB industry
2. Transparency of the supervision of the MSB industry
3. Communicating consistent, reasonable expectations for providing banking services to MSBs
4. Facilitating industry best practices for MSBs to implement effective AML programs

In conclusion, the boxing match between the OCC and the NYDFS has not yet reached its final round. Regardless of the outcome, both agencies, along with their regulatory counterparts, must work together. Financial institutions and virtual currency exchanges need continued guidance and solutions that require advanced detection capabilities to prevent and deter criminal activity. For now, the best methodology leans toward the utilization of exiting MSB regulations and guidance as a foundation for which we can build on.

Information sharing amongst regulators, law enforcement and financial intelligence units is imperative in this highly anonymous yet extremely lucrative business. As AML professionals we have the power to shape and mold the regulation of this divergent industry. Together we honor the victims of terrorism by fighting back with financial intelligence. The key is to lead with integrity.

---

Exhibit A: The Association of Accounting Technicians (AAT) Reference Document

**HOW DO BITCOINS WORK?**

'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions.

Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app.

Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily.

Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out.

**WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK**

**HOW TO USE BITCOINS**

Download software to your computer or phone to set up a Bitcoin wallet. This gives you the basic facilities to send, receive and store Bitcoins.

Buy Bitcoins with a standard offline currency either from another user or through a dedicated Bitcoin exchange. Your new digital funds are added to your wallet.

The Bitcoin network authenticates transactions by recording them in the blockchain - the underlying code that preserves the integrity of the currency.

Use your software to send payments to other addresses. Divisions as small as 100000000th of a Bitcoin are possible - a unit called a 'Satoshi', after the currency's enigmatic inventor.

Source Website <<http://www.aatcomment.org.uk/bitcoin-what-is-it-how-it-works/>>
## Virtual Currency Timetable of Notable Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 2008</td>
<td>Satoshi Nakamoto White Paper</td>
</tr>
<tr>
<td>Jan 2009</td>
<td>First 50 bitcoins mined by Nakamoto: Genesis Block</td>
</tr>
<tr>
<td>May 2010</td>
<td>1st bitcoin transaction: 10,000 BTC for a pizza now worth $12,500,000 USD</td>
</tr>
<tr>
<td>Jul 2010</td>
<td>Mt. Gox Tokyo Virtual Currency Exchange launched</td>
</tr>
<tr>
<td>Aug 2010</td>
<td>Bitcoin Protocol bug fixed</td>
</tr>
<tr>
<td>Feb 2011</td>
<td>Silk Road - Black Market website launched</td>
</tr>
<tr>
<td>Mar 2011</td>
<td>First UK Virtual Currency Exchange began converting BTC to pounds sterling</td>
</tr>
<tr>
<td>Jun 2011</td>
<td>WikiLeaks begins accepting bitcoin donations after being blocked by big banks</td>
</tr>
<tr>
<td>Mar 2013</td>
<td>FIN-2013-G001: FinCEN Guidance on virtual currency</td>
</tr>
<tr>
<td>Aug 2013</td>
<td>NYDFS Virtual Currency Inquiry</td>
</tr>
<tr>
<td>Oct 2013</td>
<td>FBI shuts down Silk Road Black Market website</td>
</tr>
<tr>
<td>Jan 2014</td>
<td>NYDFS Virtual Currency Hearings</td>
</tr>
<tr>
<td>Feb 2014</td>
<td>Mt. Gox suspended trading after 850,000 BTC stolen</td>
</tr>
<tr>
<td>Mar 2014</td>
<td>IRS 2014-21: IRS Notice regarding tax treatment of digital money i.e. bitcoin</td>
</tr>
<tr>
<td>Apr 2014</td>
<td>FIN-2014-R007: FinCEN Ruling regarding individuals mining virtual currency</td>
</tr>
<tr>
<td>Jun 2014</td>
<td>FATF Virtual Currency CFT Risks</td>
</tr>
<tr>
<td>Jul 2014</td>
<td>NYDFS Proposes BitLicense Regulations</td>
</tr>
<tr>
<td>Dec 2014</td>
<td>NYDFS Updated BitLicense Regulations</td>
</tr>
<tr>
<td>May 2015</td>
<td>Ripple Inc. - $700,000 CMP</td>
</tr>
<tr>
<td>Jun 2015</td>
<td>FATF Guidance-RBA-Virtual-Currencies</td>
</tr>
<tr>
<td>Jun 2015</td>
<td>NYDFS Finalizes BitLicense rules and begins accepting applications</td>
</tr>
<tr>
<td>Sep 2015</td>
<td>NYDFS Awards 1st BitLicense (Circle Internet Financial)</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>FIN-2016-G001: FinCEN Guidance on MSB agent monitoring</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>OCC Responsible Innovation publication</td>
</tr>
<tr>
<td>July 2016</td>
<td>NYDFS Awards 2nd BitLicense (Ripple - Post CMP)</td>
</tr>
<tr>
<td>Oct 2016</td>
<td>FIN-2016-A005: FinCEN Advisory on cyber-crime</td>
</tr>
<tr>
<td>Dec 2016</td>
<td>OCC SPNB Charter Proposal</td>
</tr>
<tr>
<td>Jan 2017</td>
<td>NYDFS Comments on OCC SPNB (1st Opposition to SPNB)</td>
</tr>
<tr>
<td>Jan 2017</td>
<td>NYDFS Awards 3rd BitLicense (Coinbase)</td>
</tr>
<tr>
<td>Mar 2017</td>
<td>Comptroller Speaks @ LendIt Conference</td>
</tr>
<tr>
<td>Mar 2017</td>
<td>OCC Draft Licensing Manual Supplement for SPNBs</td>
</tr>
<tr>
<td>Apr 2017</td>
<td>NYDFS sends letter to OCC (2nd Opposition to SPNBs)</td>
</tr>
</tbody>
</table>


The cryptocurrency, bitcoin, is typically denoted with a lower case “b." There remain two schools of thought on the singular vs. plural form of the term. Some believe the word should remain singular for multiple units (i.e. gold); however, the more common practice is to add an “s” at the end the word bitcoin.

### Bitcoin Denominations (Multiples and Subdivisions)
- 10 BTC = decabitcoin (daBTC)
- 1,000 BTC = kilobitcoin (kBTC)
- 1,000,000 = megabitcoin (MBTC)
- 1 BTC = bitcoin
- .1 BTC = decicoin
- .01 BTC = centicoin (bitcent)
- .001 BTC = millibitcoin (mBTC/millicoin/millibit)
- .000001 BTC = microbitcoin (µBTC/bit)
- .00000001 BTC = satoshi
Exhibit C: Money Service Business (MSB) Compliance Checklist

**MSB Risk Assessment**

- Purpose of the account
- Anticipated account activity (type and volume)
- Types of products and services offered by the MSB
- Locations and markets served by the MSB

**MSB Risk Mitigation & Customer Due Diligence (CDD) Expectations**

- Confirm MSB is registered with FinCEN [FinCEN Money Service Business Registry Search](https://www. fincen. gov/)
  
  (Note: registration must be renewed every two years)
- If required, confirm MSB is licensed with appropriate state(s)
- Confirm agent status, if applicable
- Conduct a basic BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary
- If applicable, MSB confirms it is subject to examination for AML compliance by the IRS and/or the State(s)
- MSB affirms the existence of a written BSA/AML program
- MSB provides the BSA officer’s name and contact information
- MSB has an established banking relationship and/or account activity consistent with expectations
- MSB is an established business with an operating history
- MSB is a principal with one or a few agents, or is acting as an agent for one principal
- MSB provides services only to local residents
- Most of the MSB’s customers conduct routine transactions in low dollar amounts
- The expected (lower-risk) transaction activity for the MSB’s business operations is consistent with information obtained by the FI at account opening
  
  Examples include the following:
  
  - Check cashing activity is limited to payroll or government checks (any dollar amount)
  - Check cashing service is not offered for third-party or out-of-state checks
  - Money-transmitting activities are limited to domestic entities (e.g., domestic bill payments) or limited to lower dollar amounts (domestic or international)
- Completed FinCEN Beneficial Ownership Form (or similar form containing the information outlined below)

**FinCEN Rule Customer Due Diligence Requirements for Financial Institutions** Pages 59-61

**Certification of Beneficial Owner(s) (BO)**

- Item (BO)(a): Name and Title of Natural Person Opening Account
- Item (BO)(b): Name and Address of Legal Entity for Which the Account is Being Opened
- Item (BO)(c): The following information for each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of the legal entity listed above:
  
  - (BO)(c)(1) Name
  - (BO)(c)(2) Date of Birth (DOB)
  - (BO)(c)(3) Address (Residential or Business Street Address)
  - (BO)(c)(4) For U.S. Persons: Social Security Number (SSN)
  - (BO)(c)(5) For Foreign Persons:
    
    - Item (BO)(c)(5)(a): Passport Number
    - Item (BO)(c)(5)(a)(1): Country of Issuance
    - Item (BO)(c)(5)(b): Alien Identification Card Number
    - Item (BO)(c)(5)(b)(1): Country of Issuance
    - Item (BO)(c)(5)(c): Other Government-Issued Document Number
    - Item (BO)(c)(5)(c)(1): Evidence of Nationality/Residence
    - Item (BO)(c)(5)(c)(2): Photograph/Similar Safeguard
    - Item (BO)(c)(5)(c)(3): Country of Issuance
    - Item (BO)(c)(5)(c)(4): Legal Entity Identifier (Optional)
- Item (BO)(d): The following information for one individual with significant responsibility for managing the legal entity listed above, such as:
  
  - (BO)(d)(1): An executive officer or senior manager

  Note: If appropriate, an individual from section c (above) may be listed in this section as well
  
  - (BO)(d)(1)(a): Chief Executive Officer (CEO)
  - (BO)(d)(1)(b): Chief Financial Officer (CFO)
  - (BO)(d)(1)(c): Chief Operating Officer (COO)
  - (BO)(d)(1)(d): Managing Member
Enhanced Due Diligence (EDD)

Review the MSB’s BSA/AML program

Compliant with FIN-2016-G001 FinCEN Guidance on Existing AML Program Rule Compliance

Obligations for MSB Principles with Respect to Agent Monitoring (March 2016)

Under 31 CFR § 1022.210, an MSB’s AML program must, at a minimum:

- Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with the BSA and its implementing regulations
- Designate a person to assure day to day compliance with the program and the BSA and its implementing regulations
- Provide education and training of appropriate personnel concerning their responsibilities under the program, including training in the detection of suspicious transactions to the extent that the money services business is required to report such transactions under the BSA
- Provide for independent review to monitor and maintain an adequate program

Review results of the MSB’s independent testing of its AML program

Review written procedures for the operation of the MSB

Conduct on-site visits

Review list of agents, including locations, within or outside the United States, which will be receiving services directly or indirectly through the MSB account

Determine whether the MSB has performed due diligence on any third-party servicers or paying agents

When conducting monitoring of their agents, principals must, at a minimum:

- Identify the owners of the MSB’s agents
- Evaluate on an ongoing basis the operations of agents, and monitor for variations in those operations

Risk factors that principals should consider when conducting agent monitoring include, but are not limited to:

- Whether the owners are known or suspected to be associated with criminal conduct or terrorism
- Whether the agent has an established and adhered to AML program
- The nature of the markets the agent serves and the extent to which the market presents an increased risk for money laundering or terrorist financing (This does not mean that principals with agents providing services involving regions affected by conflict or terrorism cannot manage such risks, but rather that principals must take steps to account for and mitigate such risks)
- The services an agent is expected to provide and the agent’s anticipated level of activity
- The nature and duration of the relationship
- Evaluate agents’ implementation of policies, procedures, and controls

Review written agent management and termination practices for the MSB

Review written employee screening practices for the MSB
Title 18 USC §1956 and 18 USC §1957, were brought into existence by the Money Laundering Control Act of 1986, which has since been expanded. In general, these statutes prohibit knowingly engaging in financial transactions using funds derived from a Specified Unlawful Activity (SUA). Title 18 USC §1956 investigations have no dollar amount limit, other than that found in the LEM, and no requirement that a financial institution be involved; 18 USC §1957 prohibits monetary transactions over $10,000 or an aggregate of money transactions over $10,000 of criminally derived funds obtained from a SUA while utilizing a financial institution.

Money Laundering—Title 18 Violations
Title 18 USC §1956 and 18 USC §1957, were brought into existence by the Money Laundering Control Act of 1986, which has since been expanded. In general, these statutes prohibit knowingly engaging in financial transactions using funds derived from a SUA. Title 18 USC §1956 investigations have no dollar amount limit, other than that found in the LEM, and no requirement that a financial institution be involved; 18 USC §1957 prohibits monetary transactions over $10,000 or an aggregate of money transactions over $10,000 of criminally derived funds obtained from a SUA while utilizing a financial institution.

Lesser-included offenses in money laundering investigations include:
- 18 USC §2 (aiding and abetting)
- 18 USC §371 or 18 USC §1956(h) (conspiracy)
- 18 USC §1001 (false statements)
- 18 USC §1510(b)(3)(B)(i) (obstruction of 18 USC §1956 or 18 USC §1957 or Title 31 investigations)
- 18 USC §1621 (perjury)
- 18 USC §1960 (illegal money transmitting business)
- 31 USC §5322 (Title 31 criminal penalties)
- 31 USC §5324 (structuring)
- 31 USC §5332 (bulk cash smuggling)
- 18 USC §1028 and 18 USC §1028A (identity theft)

Title 18 USC §1956
Title 18 USC §1956 is the basic Title 18 money laundering offense. It has three specific parts. They are:
- 18 USC §1956(a)(1), Domestic Financial Transactions
- 18 USC §1956(a)(2), International Transportation of Monetary Instruments or Funds
- 18 USC §1956(a)(3), Sting Operations

Title 18 USC §1957 Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity
Title 18 USC §1957 prohibits an actual or an attempted monetary transaction of over $10,000 in SUA proceeds. To prove a violation of 18 USC §1957, the government must prove:
1. the defendant knowingly
2. engaged in, or attempted to engage in
3. a monetary transaction (i.e., a transaction by, through or to a financial institution)
4. in criminally derived property of a value in excess of $10,000 and the property is derived from SUA

Title 18 USC §1960 Prohibition of Unlicensed Money Transmitting Businesses
(a) Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

Title 31 Violations
Title 31, as the Bank Secrecy Act (BSA), requires filing reports with the government and recordkeeping by financial institutions or individuals for domestic and foreign transactions involving currency, monetary instruments, and foreign accounts. It also sets forth punishments for the failure to make or falsify reports or records. Offenses investigated by CI are summarized in the following sections. Title 31, Federal Criminal Code, Chapter 53, Money and Finance, contains information regarding the purposes, specific offenses, definitions and penalties for use with this Title.

Exhibit E: Examination Procedures
Nonbank Financial Institutions

Objective. Assess the adequacy of the bank’s systems to manage the risks associated with accounts of nonbank financial institutions (NBFI), and management’s ability to implement effective monitoring and reporting systems.

1. Determine the extent of the bank’s relationships with NBFIIs and, for banks with significant relationships with NBFIIs, review the bank’s risk assessment of this activity.

2. Review the policies, procedures, and processes related to NBFI accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank’s NBFI activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

3. From review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors NBFI accounts.

4. Determine whether the bank’s system for monitoring NBFI accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the nature of the bank’s customer relationships.

Money Services Businesses

5. Consistent with the interagency guidance released on April 26, 2005, determine whether the bank has policies, procedures, and processes in place for accounts opened or maintained for money services businesses (MSB) to:
   - Apply the bank’s CIP.\(^{42}\)
   - Confirm FinCEN registration, if required. (Note: registration must be renewed every two years.)
   - Confirm state licensing, if applicable.
   - Confirm agent status, if applicable.
   - Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required.

6. Determine whether the bank’s policies, procedures, and processes to assess risks posed by MSB customers effectively identify higher-risk accounts and the amount of further due diligence necessary.

Transaction Testing

7. On a basis of the bank’s risk assessment of its NBFI accounts, as well as prior examination and audit reports, select a sample of higher-risk NBFI accounts. From the sample selected, perform the following examination procedures:
   - Review account opening documentation and ongoing due diligence information.
   - Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity.
   - Determine whether actual activity is consistent with the nature of the customer’s business and identify any unusual or suspicious activity.

8. On a basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NBFI relationships.

---

\(^{42}\) Refer to 31 CFR 1020.100 (FinCEN); 12 CFR 21.21(Office of the Comptroller of the Currency); 12 CFR 208.63(b), 211.5(m), 211.24(j) (Board of Governors of the Federal Reserve System); 12 CFR 326.8(b)(2) (Federal Deposit Insurance Corporation); 12 CFR 748.2(b) (National Credit Union Administration).