Risk-Based Approach for AML/CFT Audits of Fiat-Backed Stablecoins

Harry Zhou

February 22, 2019

Table of Contents

I. Executive Summary 1

II. Fiat-Backed Stablecoin (FBSC) Programs 1

A. Introduction 1

B. Emergence and Current State of FBSC 2

C. U.S. Regulatory Frameworks of FBSC Programs 3

D. FBSC Risk Categories 3

III. Risk-Based Approach for Auditing AML/CFT Measures of FBSC Programs 6

A. Step One: Risk Assessment 6

1. Program Size and Activity Level 6

2. Segmentation Risks 8

3. Geographic Risks 9

4. Acquisition Channels (Funding Methods) 10

5. Access to Cash 11

B. Step Two: Review Policies, Procedures, Processes, and Controls 12

1. Program Participant Due Diligence 12

2. Customer Due Diligence 13

3. Transaction Monitoring 14

4. Record Keeping 14

5. Blocking and Reporting 15

6. Training 16

C. Step Three: Forming Audit Conclusions 16

IV. Conclusions 17

V. References 19

Appendix A Overview on FBSC Blockchain Analytics for AML/CFT Purposes 20

Appendix B Glossary 23

I. Executive Summary

More and more U.S. financial institutions are considering whether to bank or issue virtual currencies that are price-stable as measured in a sovereign currency. Known as stablecoins, these novel blockchain-based monetary instruments present a challenge for anti-money laundering/combating the financing of terrorism (AML/CFT) compliance staff and auditors because their nascent nature and unique risk profiles often render AML/CFT frameworks, particularly ones that are meant for traditional monetary instruments and non-stablecoin virtual currencies, ineffective.

This white paper intends to aid AML/CFT professionals in assessing and auditing the money-laundering/financing terrorism (ML/FT) risks of fiat-backed stablecoins. It does so by providing background information on fiat-backed stablecoins, discussing how their risks compare to those of physical cash, noncash monetary instruments, and non-stablecoin virtual currencies like Bitcoin, and proposing a risk-based framework for their risk assessments and audits. Appendices to this white paper provide further resources, including a glossary and a discussion on how emerging measures like blockchain analytics can help mitigate ML/FT risks of fiat-backed stablecoins.

II. Fiat-Backed Stablecoin (FBSC) Programs

A. Introduction

The prices of most virtual currencies are volatile, as they are set solely by market supply and demand. Stablecoins are different: While they rely the same distributed ledger technologies used by many virtual currencies, their prices as measured in a sovereign currency are stable.

Stablecoins achieve price stability through many different arrangements (e.g., algorithmic, autonomous trading bots). The most common method of doing so, however, is through fiat collateralization, where a trusted program provider promises to exchange one unit of a stablecoin for one unit of a fiat currency. The provider will also promise to hold 100% of the received fiat in reserve to ensure market confidence in the stablecoin's redeemability. Stablecoins that are price stable as a result of fiat collateralization are generally referred to as fiat-backed stablecoins, or FBSCs.

FBSCs have been rapidly expanding in number and size because of their decisive advantages over bank wires and price-unstable virtual currencies when used for virtual currency trading. Their providers now range from offshore companies to U.S.-regulated financial institutions, such as state-chartered trust companies in New York and Nevada. Notably, on February 14, 2019, JPMorgan Chase N.A. announced its prototype of "JPM Coin," potentially becoming the first U.S. national bank to offer a stablecoin program.[1]

FBSCs present unique AML/CFT risks because 1) their cash-like characters make identifying ultimate holders and surveilling and blocking their transfers challenging, 2) their use of distributed ledgers allow

[1] "J.P. Morgan Creates Digital Coin for Payments," J.P. Morgan Chase & Co., February 14, 2019, https://www.jpmorgan.com/global/news/digital-coin-payments.

them to be transferred in a bilateral, near–instant, and borderless manner, and 3) these features combined with guaranteed price stability and fiat redeemability could make them highly susceptible to ML/FT activities. These risks are heightened by the fact that most FBSCs have highly liquid Internet-based secondary markets with varying AML/CFT standards.

B. Emergence and Current State of FBSC

FBSC emerged in 2017 when a U.S. commercial bank terminated a correspondent banking relationship with a Taiwanese commercial bank that provided USD clearance and settlement services for an Internet-based virtual currency exchange. To resume U.S. dollars settlement, the affected exchange listed FBSC One,[2] an FBSC program provided by a then Asia-based company with unclear beneficiary structure and place of organization. Circulating units of FBSC One were purportedly backed by an equal number of U.S. dollars. Namely, its provider claims that it will issue, or "mint," one unit of FBSC One for each U.S. dollar received, and will revoke, or "burn," one unit of FBSC One for each U.S. dollar redeemed. Received U.S. dollars are purportedly held in reserve awaiting redemption.

In September 2017, the Chinese government announced a ban on centralized virtual currency trading.[3] This development forced Chinese virtual currency exchanges to seek alternative funding channels as their preexisting banking arrangements shuttered. FBSC One experienced explosive growth by enabling these Chinese exchanges to continue operating outside of the regulation and supervision of the major economies, and removing their need for accessing the formal financial system.

FBSC One led to the emergence of other FBSC programs, all with varying degrees of commercial success and regulatory soundness. These FBSC programs include the following typical participants and responsibilities:

- **Program provider –** An entity that designs and maintains the features and characteristics of the FBSC program, and runs the program's day-to-day operations.
- **Bank[4] –** At least one "bank" responsible for holding the fiat deposits in full reserve to ensure price stability. The bank and the program provider may or may not be the same entity. In programs where the program provider and the bank are separate, depending on the specifics of contractual arrangement, either the provider or the bank will clear and settle the FBSC purchase and redemption requests.
- **Nonbank exchanger –** In rare cases, an FBSC program may have one or more designated nonbank exchangers that will clear and settle the FBSC's purchase and redemption requests.
- **Blockchain –** A distributed ledger that replaces the role of payment processors.
- **Trading venues–** Secondary trading venues, such as virtual currency exchanges, that list FBSC for trading.

[2] Although fictitious names are used, all FBSC programs referenced in this white paper are real and circulating.
[3] PBOC, CAC, MIIT, SAIC, CBRC, CSRC, and CIRC, "Announcement … on the Prevention of the Risk of Subsidy Issuance," The People's Bank of China, September 4, 2017, http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html (in Chinese).
[4] "Bank" as defined in FFIEC.31 C.F.R. 1010.100(d) includes "a … trust company organized under the laws of any State or of the United States."

In a typical FBSC program, a prospective customer must first create an account and undergo remote identity verification with an FBSC program provider. The customer can then purchase a certain number of FBSCs by funding the account with an equivalent number of U.S. dollars (or virtual currencies to be converted into U.S. dollars). In return, the provider will issue, or "mint," the purchased FBSCs to a designated blockchain address owned by the customer.

At this point, the FBSC's transfer characteristics become almost indistinguishable from those of virtual currencies: They can be settled on its blockchain in a bilateral, near–instant, and borderless manner, and can be transferred to anonymous third parties with little restriction.

To redeem FBSCs for fiat, a customer must typically deposit FBSCs into a designated redemption address for the provider to revoke or "burn." Upon confirmation that the burning has succeeded, the provider will transfer to the customer fiat (e.g., U.S. dollars) in a number equal to that of the units of FBSC burned.

As of January 23, 2019, the aggregate amount of the five largest FBSC programs in circulation is about USD 2.8 billion. Of that, about USD 768 million, or 27%, are from U.S.-based FBSC programs.[5]

C. U.S. Regulatory Frameworks of FBSC Programs

FBSCs are fundamentally a digital representation of fiat currency; they electronically transfer value that has legal tender status. FBSCs therefore constitute "e-money" instead of "virtual currencies," according to the FATF 2015 *Guidance for a Risk-Based Approach to Virtual Currencies*.[6]

U.S. federal regulators will likely consider FBSC as a form of "prepaid access" because FBSC could be seen as representing "access to funds … that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle."[7] Therefore, any nonbank provider that has principal oversight and control over an FBSC program will be deemed a money services business and be required to comply with all applicable legal requirements.[8]

U.S. state regulators will likely consider FBSC as "money or monetary value" for purposes of state money transmission law.[9] State money transmitter licenses will thus be required for nonbank FBSC providers, unless contractual arrangements stipulate that a program bank assumes principal oversight and control.

D. FBSC Risk Categories

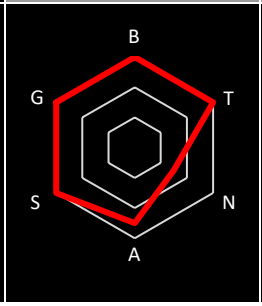
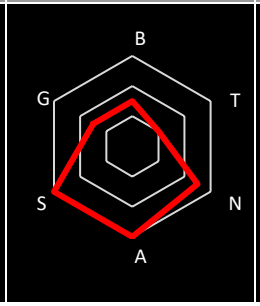
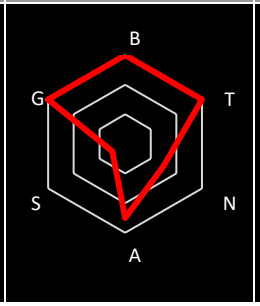
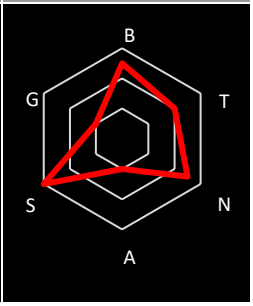
The FBSC risk categories below summarize FBSC-specific risk factors discussed. These categories are based on the FATF 2013 *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services.* Columns for Physical Cash, Virtual Currencies, and New Payment Products and

[5] Supporting data are retrieved from the Bitcoin OMNI layer and the Ethereum blockchain, https://www.omnilayer.org/ and https://www.ethereum.org/.
[6] See page 26 of the FATF 2015 *Guidance for a Risk-Based Approach to Virtual Currencies*.
[7] FFIEC.31 C.F.R. 1010.100(ww).
[8] See FinCEN FAQs on "Final Rule—Definitions and Other Regulations Relating to Prepaid Access," November 2, 2011, https://www.fincen.gov/sites/default/files/shared/20111102.pdf.
[9] See, e.g., "Supervisory Memorandum—1037," by C.G. Cooper, January 2, 2019, Texas Department of Banking, ("stablecoins that are pegged to sovereign currency may be considered a claim that can be converted into currency and thus fall within the definition of money or monetary value under Finance Code § 151.301(b)(3)."), available at https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.

Services (NPPS) serve to compare risk factors across various instruments and to demonstrate the distinctiveness of FBSC programs' AML/CFT risk profile.

These categories should be considered along with risk factors common to all NPPS in determining the overall level of risk of an FBSC program as part of an audit risk assessment. The outcome of the risk assessment should in turn guide the depth and granularity of audit efforts in accordance with the risk-based approach. Finally, because the size and nature of FBSC programs vary, auditors should also adapt these risk categories to reflect each FBSC program's unique features, including its total amount in circulation and arrangement complexity.

Attributes of Various Payment Instruments:

	FBSC	Physical Cash	Virtual Currencies	NPPS
Acquisition Channels	+ Not face-to-face	- Face-to-face	+ Not face-to-face	+ Not face-to-face
Access to Fiat	+ Guaranteed	+ Guaranteed	- Not guaranteed	+ Guaranteed
Transfer Mechanism	+ Electronic transfer + Bilateral settlement + Borderless	+ Bilateral settlement - Physical transfer only	+ Electronic transfer + Bilateral settlement + Borderless	+ Electronic transfer - Some bilateral settlement
Price Stability	+ High	+ High	- Low	+ High
Negotiability	- Hardly accepted[10]	+ Generally accepted - No online negotiability	▪ Depends	+ Generally accepted
Record Keeping	+ Anonymous on-chain + Untraceable if mixed - Extensive off-chain	+ Anonymous + Untraceable	+ Anonymous on-chain + Untraceable if mixed - Extensive off-chain	- Extensive
Geographical Reach	+ Broad	▪ Depends on the issuer	+ Broad	- Limited
Segmentation	+ Can be segmented	▪ Not applicable	▪ Not applicable	+ Can be segmented
CDD – Identification	+ Anonymous on-chain[11] ▪ Some on-chain identities - Possible at conversion	+ Anonymous	+ Anonymous on-chain ▪ Some on-chain identities - Possible when traded	- Customers identifiable
CDD – Verification	+ Anonymous on-chain - Possible at conversion	+ Anonymous	+ Anonymous on-chain	- Identities verifiable
CDD – Monitoring	- Ongoing monitoring	+ None	- Ongoing monitoring	- Ongoing monitoring
Control – Amt. Cap / Acct.	+ None on-chain - Possible at conversion	+ None	+ None	- Possible
Control – Amt. Cap / Tx.	+ None on-chain - Possible at conversion	+ None	+ None	- Possible
Control – Frequency Cap	+ None on-chain - Possible at conversion	+ None	+ None	- Possible
Control – Expiration Date	+ None	+ None	+ None	- Possible
Composite Risk Graphs B – Acquisition Ease T – Transfer Ease N – Negotiability A – Anonymity S – Price Stability G – Geographical Reach				

[10] FBSC's negotiability is low outside of virtual currency exchanges. That might change as FBSC awareness among payment processors, merchants, and consumers improve. See, e.g., "Why Is BitPay Settling to Merchants with Stablecoins?" by C. Pustejovsky, November 12, 2018, https://blog.bitpay.com/why-bitpay-is-using-stablecoins.

III. Risk-Based Approach for Auditing AML/CFT Measures of FBSC Programs

A risk-based approach for auditing AML/CFT measures of FBSC Programs is proposed below as a baseline for auditors to conduct initial or subsequent audits. To ensure relevance, this proposal focuses on FBSC-specific risk factors and mitigants; auditors should consider this proposal in combination with generally applicable AML/CFT guidance on NPPS and virtual currencies when designing their audit frameworks to reflect each program's unique size and nature. Nor does this proposal address non-AML/CFT compliance of FBSC programs, such as consumer protection, cybersecurity, and tax matters.[12]

Under this proposal, a risk-based audit of an FBSC program should generally involve four steps. First, review the FBSC program's latest risk assessment (or perform one if none exists) to determine the audit depth and granularity for each risk category. Second, review the policies, procedures, processes, and controls of the FBSC program to evaluate their adequacy given the risks presented. Third, perform transaction testing to validate the completeness, correctness, and effectiveness of the implementation of policies, procedures, processes, and controls. Fourth, form conclusions about the adequacy of the program's AML/CFT measures based on evaluation and testing outcomes for the audit report.

A. Step One: Risk Assessment

An effective risk-based audit begins with an accurate risk assessment. Auditors should examine applicable risk factors in the FBSC risk categories discussed above (after adapting the list to reflect an FBSC program's overall size and features) to reach a conclusion about the program's risk level in each category and overall risk level. Auditors may select the specific quantitative or qualitative assessment methodologies in accordance with industry and regulatory guidance.[13]

Risk assessment conclusions should be substantiated with data. When auditing NPPS, auditors usually must assume that the data provided by business, compliance, and IT functions are accurate because these parties are often the sole custodians of business information. FBSC programs, however, use blockchains, and blockchain activities are almost always public. Auditors should therefore consider gathering on-chain information to augment and verify data from audit targets.

1. Program Size and Activity Level

FBSC programs' sizes and activity levels can differ by orders of magnitude, and those with larger sizes and higher activity levels tend to emanate higher risks. As with NPPS, FBSC with better liquidity tend to be more susceptible to ML/FT misuses as they offer financial criminals a higher chance of blending illicit transactions with legitimate ones.

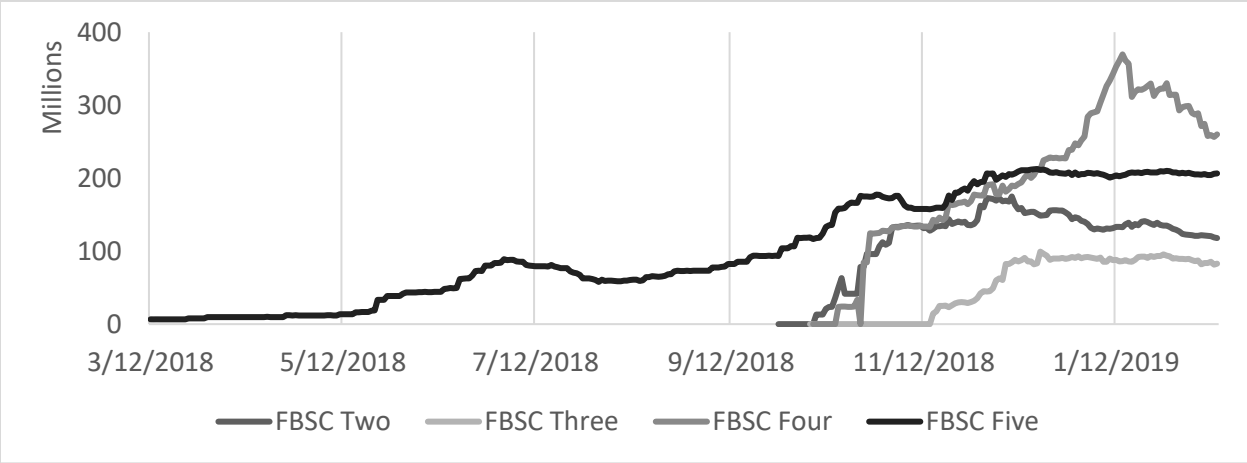
---

[12] See, generally, *FFIEC BSA/AML Examination Manual, "*Procedures for Prepaid Access," available at https://bsaaml.ffiec.gov/manual/ProductsAndServices/10_ep.

[13] See, e.g., *The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption*, 2015, available at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf.

An FBSC program's size can usually be measured by its total reserve held at the program's bank. This information should be readily available whether the program is bank-centered or not as the bank maintains the reserve accounts in both cases. Alternatively, the FBSC's total circulation as evidenced by the relevant blockchain can also be an accurate indicator of the program's size, given the 1:1 fiat to virtual currency pegging.

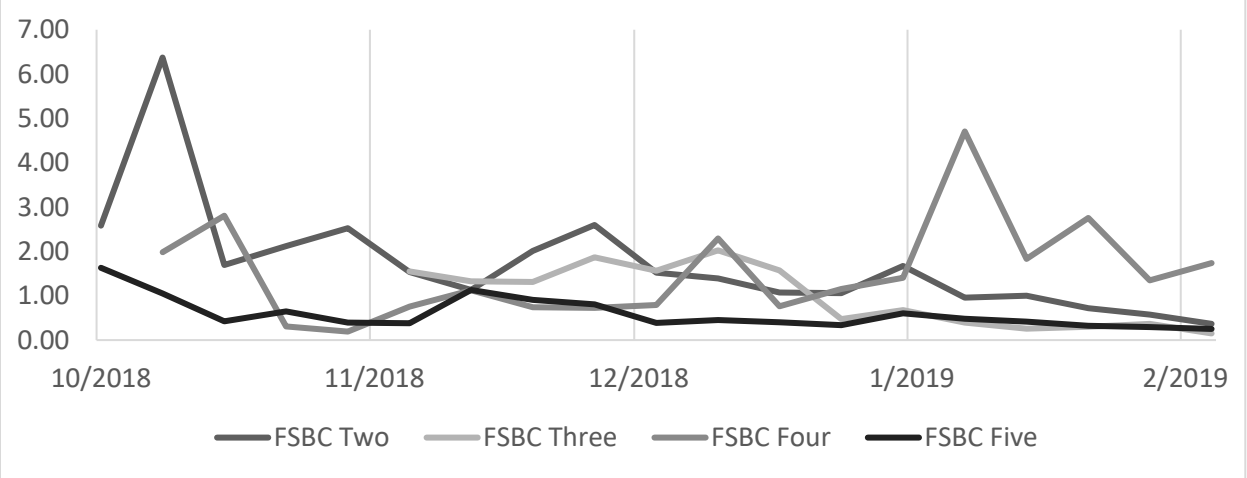
Growth in Sizes of Four US-based FBSC Programs



Data and chart produced by Merkle Data for this white paper

The figure above shows the growth in sizes of four U.S.-based FBSC programs from March 12, 2018, to February 13, 2019, as retrieved from the Ethereum blockchain.

An FBSC program's activity level can usually be measured by its aggregate on-chain transaction volume as normalized by its total amount in circulation. This information can be directly retrieved from the FBSC's blockchain.



Data and chart produced by Merkle Data for this white paper

The figure above shows the aggregate on-chain transaction volumes per week as normalized by total amounts in circulation, respectively, for four U.S.-based FBSC from October 2018 to February 2019 as retrieved from the Ethereum blockchain.

2. Segmentation Risks

Structures of FBSC programs can vary greatly from one program to another because of a lack of prior examples in organizing these new forms of NPPS. Indeed, prior to September 2018,[14] there was no consensus on whether FBSCs could ever receive affirmative regulatory approval in any jurisdiction regardless of its structure. Patchwork money-transmission licensing regimes in the United States further complicate the structuring decision. Providers with U.S. state trust charters, full coverage in state money-transmitter licenses, and/or E.U. e-money license often opt for a bank-centered structure where a single entity handles all aspects of program management, while providers with lesser or no licenses often enlist the help of one or more financial institutions to operate their FBSC program. Auditors should evaluate segmentation risks of FBSC programs with these contexts in mind.

Higher segmentation risks in FBSC programs include these factors:

- **Nonbank-centered structure –** Nonbank-centered FBSC programs can have several parties, each performing one or several aspects of program management. The setup introduces higher MF/FT risks because, among other things, the chain of transaction information stretches across the applicable blockchain and multiple parties, and program participants could have a different understanding of which participant is responsible for what aspects of AML/CFT compliance.
- **Inexperienced provider –** Nonbank providers of FBSC programs are often newly formed virtual currency businesses. These providers may be unfamiliar with AML/CFT obligations and may not have the relevant experience to design, implement, and operate effective controls.
- **International provider –** Nonbank FBSC providers operating outside of the United States increase segmentation risks because the providers may be in jurisdictions with inadequate AML/CFT measures**.** Additionally, the jurisdictional difference reduces the progr**a**m bank's visibility of the provider's activities and makes it harder for the U.S. regulators and the AML/CFT authorities in the provider's jurisdiction to detect and trace suspicious activities.
- **Nonbank exchangers –** FBSC programs with exchangers (in addition to the bank) that promise to exchange the FBSCs to and from fiat show higher segmentation risks because the AML/CFT measures of the exchangers may be inadequate.

Lower segmentation risks in FBSC programs include these factors:

- **Bank-centered structure –** Segmentation risks are lower in a bank-centered structure where a bank h**a**ndles all aspects of program operations, including customer onboarding, fiat transactions, blockchain transactions, ongoing monitoring, record keeping, and regulatory correspondence.
- **U.S.-based regulated provider –** If a FBSC program is nonbank-centered, the program's segmentation risks are lower if its provider is otherwise U.S.-based and subject to substantive AML/CFT supervision and examination by one or more functional regulators.

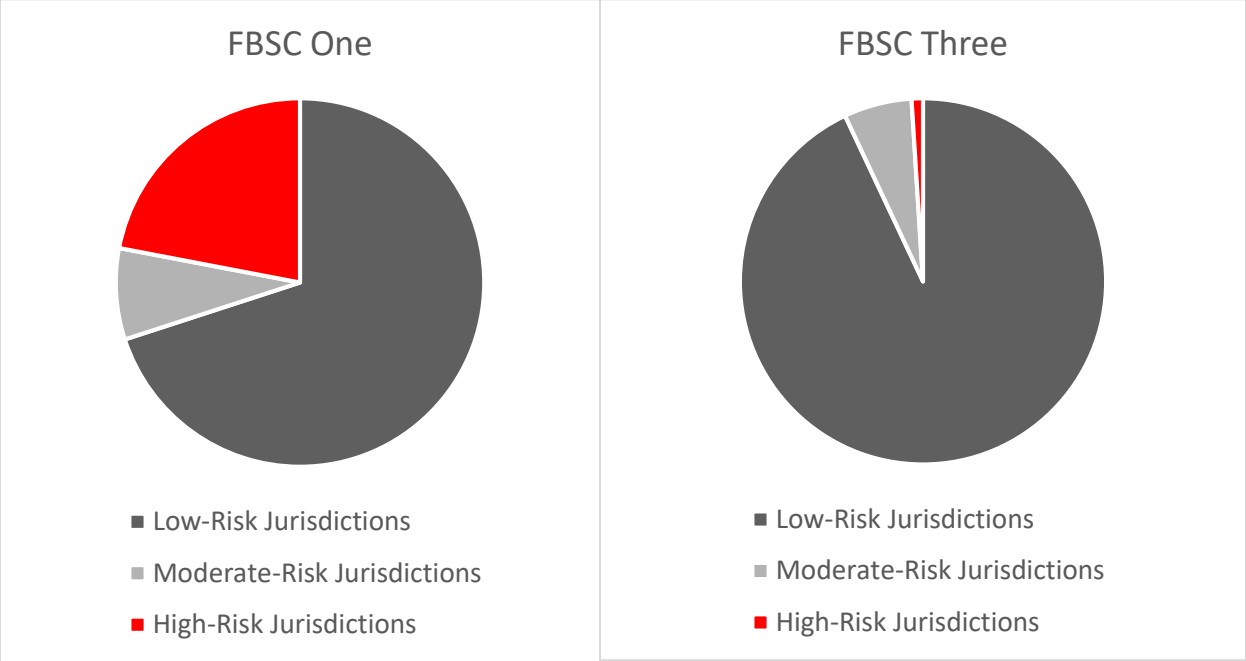
[14] See, e.g., "DFS Continues to Foster Responsible Growth in New York's FinTech Industry With New Virtual Currency Product Approvals," by Richard Loconte, Sept. 10, 2018, available at https://www.dfs.ny.gov/about/press/pr1809101.htm.

3. Geographic Risks

While FBSC's bank and nonbank exchangers may have limited geographic presence, FBSC's use of blockchains often leaves program providers with no practical means to prevent anonymous intermediaries from electronically receiving, holding, and transferring FBSCs in a borderless manner.

But blockchains may offer ways to assess geographic risks that are unattainable for cash and NPPS. Determining the precise level of cash or NPPS transfers relating to high-risk jurisdiction is hard because these transfers are physical transports with unreliable controls like border intercepts.[15] Blockchain analytics can, however, reveal with a reasonable degree of certainty the geographic location of the control person of an FBSC blockchain address even if the control person is anonymous to the program provider. Appendix A to this white paper provides an overview of using blockchain analytics for FBSC AML/CFT.

Geographic Risk Categories for FBSC One and FBSC Three



Data and charts produced by Koi Compliance for this white paper

The two figures above illustrate the breakdowns of geographic risk categories of on-chain transactions for FBSC One and FBSC Three on January 17, 2019. FBSC One is a non-U.S., nonbank-centered, unregulated program primarily traded on unregulated trading venues. FBSC Three is a U.S.-based, bank-centered, regulated program primarily traded on regulated trading venues.

FBSC program's geographic risks generally become higher as the percentage of transfers to, from, or in any FATF high-risk and other monitored jurisdictions rises. It is therefore likely that FBSC One exhibits a higher level of geographic risks than FBSC Three.

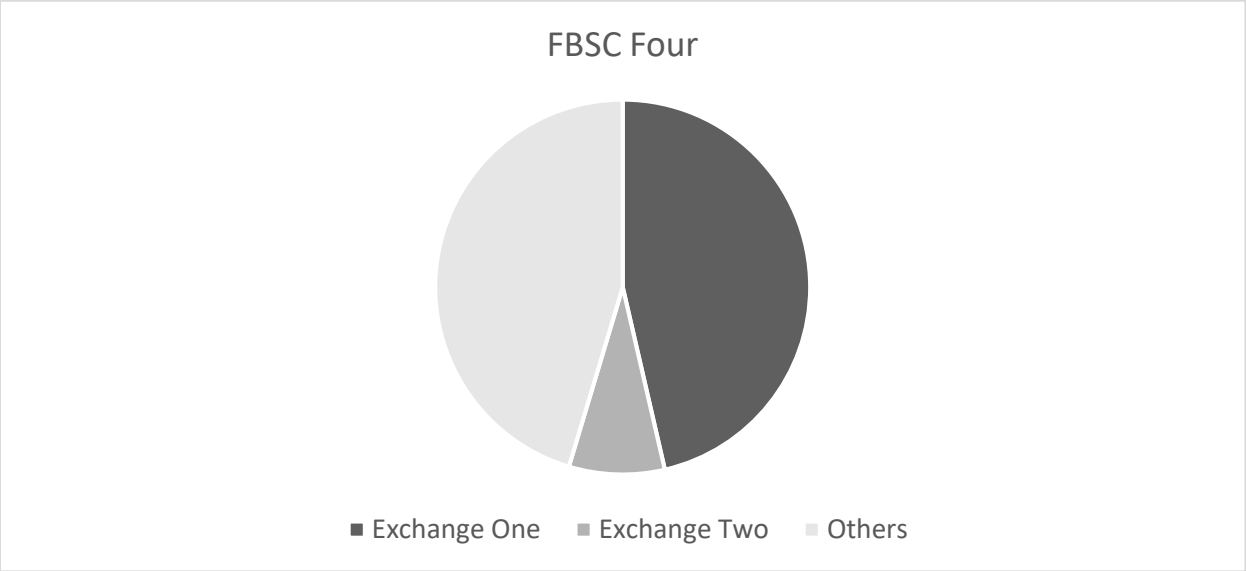
[15] See, generally, FATF Report *Money Laundering Through the Physical Transportation of Cash*, October 2015, available at https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf. See also, FATF Recommendation 32.

4. Acquisition Channels (Funding Methods)

At present, almost all FBSC programs are entirely Internet-based. Customers typically undergo remote identity verification before they can access their FBSC accounts (a.k.a., FBSC purchases). No cash, third-party, or anonymous funding is permitted. For these reasons, funding risks associated with certain NPPS (e.g., prepaid access cards) may not be present or pronounced in FBSC programs.

Yet large-scale secondary trading of FBSC introduces new funding-method risks because most owners of FBSC are likely not direct customers of the FBSC programs. Instead, they acquire FBSC from virtual currency exchanges and over-the-counter dealers or brokers by paying virtual currencies, other FBSC, e-money, and/or cash. These exchanges and dealers may not collect or verify user identities at all.

The figure below shows that as of January 20, 2019, about 45% (USD 88 million) of all FBSC Four, a U.S.-based nonbank-centered program, are held by users of Exchange One, an Internet-based virtual currency exchange. Most of the exchange's users are ineligible for FBSC Four accounts as the program accepts only institutional traders.



Data and chart produced by Koi Compliance for this white paper

FBSC like FBSC Four are typically moved between program-managed accounts and virtual currency exchanges by institutional traders engaging in arbitrage, quantitative, and/or proprietary trading. These institutional traders are *de facto* bureaux de change that enable a substantial number of persons unknown to program providers to come into possession of FBSC.

Many of these institutional traders are the FBSC programs' own trading teams. Because listing an FBSC as a quote currency on leading virtual currency exchanges is perceived as vital to the FBSC's commercial success, FBSC program providers often contractually agree to undertake market-making obligations for its trading pairs during a specified period after listing. To do so, an FBSC program provider will often open an account for itself, purchase a large amount of its own FBSC with proprietary funds, and instruct

its internal trading teams to trade with these FBSC in fulfillment of market-making obligations on various exchanges. An FBSC program provider engaging in this practice is effectively issuing a large amount FBSCs to a known virtual bureau de change, itself, with the full knowledge and express intent that these FBSCs are to be swiftly resold to non-customer persons whose identities are unknown to the provider. The net effect is that the FBSC provider is circumventing its own customer due diligence (CDD) safeguards.

Therefore, auditors should consider at least the following as higher funding-method risk factors:

- **Virtual currency exchanges with deficient AML/CFT measures –** If blockchain data demonstrate that a substantial sum of FBSCs are deposited with unregulated virtual currency exchanges that have deficient AML/CFT measures, the FBSC's ML/FT risks are elevated because there is a higher likelihood that neither the FBSC program provider nor the exchange operators know or have the means to know the identities and sources of income of exchange users who hold the FBSCs.
- **Virtual bureaux de change prevalence –** An FBSC's ML/FT risks become higher if a large percentage of the program's customers are known to act as virtual bureaux de change, or the program provider uses an internal trading arm as a virtual bureau de change for a substantial sum of the FBSCs.

Conversely, lower funding-method risk factors include these factors:

- **Virtual currency exchanges with satisfactory AML/CFT measures –** An FBSC program shows lower ML/FT risks if blockchain data show that the FBSCs are primarily deposited with regulated virtual currency exchanges located in low-risk jurisdictions that have satisfactory AML/CFT standards.
- **Limited presence of virtual bureaux de change –** An FBSC's ML/FT risks are lower if the program performs sufficient CDD to prevent unauthorized virtual bureaux de change, and/or if it limits the market-making activities of its internal trading arm to virtual currency exchanges with satisfactory AML/CFT standards.

5. Access to Cash

Unlike prepaid access products that can access ATM networks, FBSCs today do not provide direct cash access. FBSC holders can redeem FBSCs into e-money only with the program provider and gain indirect access to cash through common banking networks. Alternatively, FBSC holders may sell FBSCs on various virtual currency trading venues and rely on the increasing interconnectedness of virtual currencies with other NPPS for indirect access to cash.

Higher risk factors relating to FBSC's cash access include these factors:

- **Interconnected NPPS with cash access –** An FBSC's ML/FT risks are higher if its program provider interconnects FBSC accounts with affiliated NPPS that have domestic or international cash withdrawal capacity. This is more likely in bank-centered FBSC programs because the bank provider usually has the necessary license to provide cash-capable NPPS.
- **Offline trading venues –** An FBSC's ML/FT risks are higher if offline trading venues that support cash transactions for the FBSC exist.

Lower risk factors relating to FBSC's cash access include this factor:

- **Lack of interconnected NPPS with cash access –** An FBSC has lower ML/FT risks if neither its provider nor any of its official or unofficial exchangers provide direct or indirect cash access through NPPS.

B. Step Two: Review Policies, Procedures, Processes, and Controls

Based on the risk-assessment outcome, auditors should evaluate the FBSC program's policies, procedures, processes, and controls to determine their adequacy and whether the controls are effective in reasonably protecting the bank from ML/FT activities given the risks. The following list of audit areas is intended to be illustrative; auditors should adapt the list as needed to reflect the specific risk profile of the FBSC program under audit.

1. Program Participant Due Diligence

For a lower-risk, bank-centered FBSC program wherein the bank performs principal oversight and control over all aspects of the program, auditors should determine at least whether:

- the bank's risk assessment of the program is accurate and reliable;
- the bank's management and trading teams understand the unique risk profile of FBSC and follow a culture of compliance; and
- the bank has a BSA/AML program tailored for and consummate with the type and level of ML/FT risks presented by the FBSC program and virtual currencies in general.

For a higher-risk, nonbank-centered FBSC program wherein a nonbank third-party performs principal oversight and control over the FBSC program, auditors should determine at least whether:

- a clear description of the bank and the nonbank-provider's program responsibilities exists (at a minimum, the description should include details on each party's AML/CFT and sanctions-related obligations, program responsibilities, and information sharing);
- the nonbank provider's risk assessment of the program is accurate and reliable;
- the nonbank provider's management is generally familiar with AML/CFT concepts and follows a culture of compliance;
- the nonbank provider has an AML/CFT compliance program tailored for, and consummate with, the type and level of ML/FT risks presented by the FBSC program and virtual currencies in general; and

- the bank's onboarding and ongoing oversight programs on the FBSC program providers are reasonably satisfactory to protect the bank.

For each listing arrangement established by the FBSC program provider with a virtual currency exchange, auditors should determine at least whether:

- the virtual currency exchange has AML/CFT measures, in particular CDD measures, that are consistent with the size and nature of FBSC and virtual currencies trading activities on the exchange;
- the exchange agrees to provide information that the FBSC program provider reasonably believes to be necessary to meet its compliance obligations, in particular the obligation to have transactional records needed to "reconstruct" FBSC transfers from, to, or between exchange users that are not FBSC customers;[16] and
- the virtual currency exchange's management understands the unique risk profile of FBSC and has a general culture of compliance.

In addition, for each listing arrangement reached with a higher-risk exchange that is either located in a high-risk jurisdiction or has inadequate AML/CFT measures, auditors should determine at least whether:

- the program provider has the right to perform onsite AML/CFT audits of the exchange;
- the virtual currency exchange has sufficient controls, including daily withdrawal limits and blockchain analytics tools, that mitigate the risk of anonymous exchange users holding the FBSC; and
- documented procedures exist for the delisting of the FBSC if the exchange's AML/CFT deficiencies remain unresolved beyond a reasonable period of time.

Participant due diligence audit conclusions should be substantiated with third-party due diligence records produced by the provider and the bank.

2. Customer Due Diligence

For a lower-risk, bank-centered FBSC program wherein the bank undertakes the CDD obligations, auditors should determine at least whether:

- the CDD policies, procedures, and processes are adequate to allow the bank provider to form a reasonably reliable understanding of the nature of the FBSC customers' businesses and their sources of funds (both fiat and virtual currencies); and
- risk-based controls are in place to 1) limit customer base to certain low-risk sectors (e.g., requiring membership in an intrabank wholesale settlement network open to institutions that have undergone enhanced due diligence[17]), 2) detect and refuse to establish relationships with prospective customers from high-risk jurisdictions using identity documents and blockchain analytics, and 3) identify customers acting as exchangers or virtual bureaux de change that have the effect of circumventing the program's CDD safeguards.

[16] See FinCEN's BSA Requirements for MSBs: 31 C.F.R. 1022.420.

[17] See, e.g., "FAQs" from the Silvergate Exchange Network, available at https://www.silvergatebank.com/digital-currency/exchanges.html.

For a higher-risk, nonbank-centered program, auditors should determine at least whether:

- the nonbank-provider's CDD policies, procedures, and processes are adequate to support a reasonable understanding of the nature of the FBSC customers' businesses and their sources of funds (both fiat and virtual currencies);
- the nonbank-provider has implemented risk-based controls to 1) limit customer base to certain low-risk sectors and/or geographic areas, and 2) identify customers acting as exchangers or virtual bureaux de change that have the effect of circumventing the program's CDD safeguards; and
- the bank's onboarding and ongoing oversight programs over the FBSC program provider are adequate to allow the bank to form a reasonable understanding of the program's customer base.

If a program provider self-funds its FBSC to market-make, auditors should also determine whether:

- adequate policies, procedures, processes, and controls are in place to mitigate the risk of the provider's internal trading team acting as a virtual bureau de change that has the effect of circumventing the program's CDD safeguards.

CDD audit conclusions should be substantiated with transaction testing records on customer identification program (CIP), ongoing CDD, enhanced due diligence (EDD), and both on-chain and off-chain transaction histories.

3. Transaction Monitoring

Auditors should determine, at a minimum, whether effective measures are in place to:

- monitor and detect program-wide changes based on blockchain analytics to conduct ongoing risk assessment in response to substantial shifts in FBSC program size, activity level, customer-base composition, and geographical reach; and
- monitor, identify, and investigate both on-chain and off-chain suspicious activities of the FBSC program, including the abilities to 1) monitor and track funding, redemption, and velocity; 2) identify international activities, especially those relating to high-risk jurisdictions, with blockchain analytics; and 3) aggregate multiple transactions made by related parties.

Conclusions on the adequacy of transaction monitoring measures should be substantiated with records on the monitoring tools' configurations and features as well as due-diligence records on how transaction monitoring alerts are investigated and resolved.

4. Record Keeping

Auditors should determine, at a minimum, whether effective record-keeping measures are in place to:

- retain FBSC transaction-specific records generated in the ordinary course of business for at least a period required by applicable legal requirements. The types of records required to be maintained are those that would be needed to reconstruct FBSC purchases, purchases, withdrawals, transfers, redemptions, and other FBSC-related transactions (e.g., information regarding the type of transaction, amount, and location of transaction, date and time of transaction, and any other unique identifiers related to the transaction); and

- to require third-party participants to share with the FBSC program provider transaction information reasonably needed by the provider to fulfill its AML/CFT compliance obligations.

If the blockchain used by an FBSC has anonymizing features, auditors should further determine, at a minimum, whether:

- adequate controls are in place to mitigate the risk that the blockchain-wide anonymizing features might prevent the program provider from meeting its record-keeping obligations and deny the provider the ability to perform meaningful blockchain analytics for CDD and transaction monitoring purposes.[18]

Conclusions on record-keeping adequacy should be substantiated with sample testing on records for on-chain and off-chain FBSC transactions.

5. Blocking and Reporting

Auditors should determine, at a minimum, whether effective measures are in place to:

- report suspicious transactions in accordance with the relevant thresholds (which may differ depending on whether the program provider is a bank or not);
- block transactions and assets (both fiat and FBSC) suspected to be related to sanctioned persons, and report the blocking to the relevant sanctions authority; and
- comply with OFAC's November 2018 update on digital currencies in all respects.[19]

In particular, auditors should determine whether the blockchain, a second-layer protocol of the blockchain, or a smart contract running on the blockchain that serves as an FBSC's distributed ledger gives its provider the ability to block FBSCs held by intermediate persons who are not direct customers of the FBSC program. If the FBSC program provider has no such ability, auditors should further determine, at a minimum, whether:

- the program provider has plans to implement such blocking ability; and
- adequate controls are in place to mitigate the risk that the provider and regulators could lose track of suspicious assets if such assets underwent further layering in the form of obfuscation, anonymization, or mixing.

Audit conclusions on the adequacy of blocking and reporting measures should be substantiated by sampling of blocking and reporting records for both on-chain and off-chain FBSC assets.

---

[18] See, e.g., FinCEN's "Assessment of Civil Money Penalty" in the matter of BTC-E, July 26, 2017 ("BTC-e and Alexander Vinnik failed to conduct appropriate risk-based due diligence to address the challenges anonymizing features would have on compliance with BSA reporting and recordkeeping requirements"), at https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf. See also definitions of "anonymiser" and "mixer" in FATF 2015 *Guidance for a Risked-Based Approach: Virtual Currencies*, p. 28.

[19] See OFAC FAQs: Sanctions Compliance re: Questions on Virtual Currency, available at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#646

6. Training

FBSC programs are a new form of e-money that continue to evolve. The rapidly changing nature of FBSC and the new technologies and risks they introduce give AML/CFT training in this area particular importance. When evaluating the AML/CFT training adequacy of an FBSC program, therefore, auditors should at least determine whether the program's training component:

- includes a general overview of 1) the transfer mechanism of convertible decentralized virtual currencies and the ML/FT risks and mitigation opportunities blockchain introduces, 2) the structure of FBSC programs and the responsibilities of program participants, 3) the risks and mitigants unique to FBSC, 4) typologies of FBSC ML/FT activities, and 5) prior enforcement actions against virtual currency businesses for AML/CFT failures;
- regularly incorporates technological, regulatory, and enforcement updates on virtual currencies, FBSC, and NPPS; and
- contains information tailored for different parties within the program, including the onboarding team, financial crimes investigators, internal traders, business development executives (e.g., staff responsible for negotiating exchange listing), senior management, and third-party program participants and their staff and agents.

Audit conclusions on training adequacy should be substantiated with training records and documented training materials.

C. Step Three: Forming Audit Conclusions

Based on outcomes of the risk assessment and the evaluation of an FBSC program's AML/CFT measures as discussed above, auditors should form and document overall conclusions about the adequacy of the program's policies, procedures, processes, and controls.

The auditors should also recommend remediation actions for any identified deficiency along with a reasonable timeline. Below is a non-exhaustive list of common deficiencies among current U.S.-based FBSC programs and suggested improvements for them:

- **Failure to conduct blockchain-wide risk assessment –** FBSC program providers often fail to conduct blockchain-wide risk assessment, a valuable process that can precisely identify insights unavailable to providers of conventional cash-like NPPS. These insights may include 1) the geographic locations of the FBSC program's user cohorts, 2) the transfer patterns, and 3) the level of activities at various trading venues. For this deficiency, auditors should consider mandating the FBSC program provider to truly "know its blockchain" by conducting thorough and ongoing blockchain-wide risk assessments and use the results to inform its AML/CFT program design.
- **Self-defeating virtual bureaux de change –** FBSC program providers often fail to sufficiently consider the fact that their AML/CFT measures are defeated by their in-house traders tasked with dealing large amounts of FBSC with unknown third parties on exchanges with weak AML/CFT standards. For this deficiency, auditors should consider requiring an FBSC program provider to adopt more robust policies to ensure that the program's internal market-making team will only

provide liquidity on exchanges with satisfactory AML/CFT standards.[20] Due diligence efforts for selecting such exchanges should be comparable to those involved in establishing correspondent banking relationships.

- **No technical ability to block suspicious on-chain FBSC –** FBSC program providers often have no ability to block on-chain FBSCs. Instead, they may have only the ability to refuse to redeem when suspicious on-chain FBSCs are traceable and are deposited for redemption. For this deficiency, auditors should consider recommending an FBSC program provider to both apply enhanced blockchain analytics that can detect and trace suspicious on-chain FBSC, and, if feasible, to formulate a plan to develop and deploy the blocking feature in a timely manner.

IV. Conclusions

FBSC program risk assessments and audits are difficult. Blockchains give FBSC programs risk factors not previously seen in NPPS, and evaluating the effectiveness of mitigants often require the understanding of new processes and evolving technologies. It is especially hard to conclude whether an FBSC program's policies, procedures, and processes are adequate if the program is new and its business data, compliance records, and prior examinations are scarce.

The risk-based approach proposed in this white paper will aid AML/CFT professionals in their audit efforts, and so will regulatory clarification to come. The FATF has added "virtual assets" and "virtual asset service providers" to the Glossary of the FATF Recommendations[21] to urgently call for a "global, risk-based response to the AML/CFT risks associated with virtual asset financial activities." The FATF will "further elaborate on how these requirements should be applied" in relation to specific types of virtual assets, which would presumably include FBSC.[22] In the United States, FinCEN has long been promulgating regulations in response to the emergence of products and services with high vulnerability to ML/FT.[23] The virtual currency industry is anticipating FinCEN to soon issue guidance on applying prepaid access and virtual currency rules to FBSC. Finally, state regulators in New York[24] and Texas[25] have taken FBSC-specific actions. Auditors of FBSC programs should consider tracking these regulatory updates to keep their audit methodologies consistent with latest regulatory expectations.

---

[20] Selecting the exchanges on which to list an FBSC program usually won't work as a control for this deficiency because program providers rarely have such an ability. Given the distributed and permission-less nature of most blockchains on which FBSC programs run, exchanges can usually list an FBSC without the FBSC program provider's knowledge.

[21] "Outcomes FATF Plenary, 17-19, October 2018," FATF, October 19, 2018, available at http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html.

[22] "Regulation of Virtual Assets," FATF, October 19, 2018, available at http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html.

[23] See, e.g., "FinCEN Issues Prepaid Access Final Rule Balancing the Needs of Law Enforcement and Industry," FinCEN, July 26, 2011, available at https://www.fincen.gov/sites/default/files/shared/20110726b.pdf. See also "Guidance on Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FinCEN, March 18, 2013, available at https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[24] See note 14.

[25] "Supervisory Memorandum—1037," by C.G. Cooper, January 2, 2019, Texas Department of Banking, available at https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.

Technologies for mitigating FBSC ML/FT risks are also developing. For example, new on-chain due-diligence systems can identify common ownership of blockchain addresses, trace through weak mixers, and provide out-of-the-box rules for identifying suspicious on-chain transaction patterns. Aggregated and anonymized information sharing platforms supported by virtual currency businesses have also shown effectiveness in unveiling real-world identities of virtual currency owners across blockchains. Auditors of FBSC programs should consider keeping abreast of these technological advances by communicating with their blockchain engineering colleagues and attending virtual currency industry events on blockchain analytics.

FBSC auditors should also consider sharing indicators, typologies, and effective controls with the rest of compliance and regulatory communities. As with other emerging payment products, it will take joint contributions from direct industry participants to help their peers and regulators create effective yet balanced AML/CFT measures. Only then can FBSC continue to grow as a responsible payment innovation that may improve financial efficiency and inclusiveness beyond the virtual currency economy.

* * *

V. References

Announcement of the China Insurance Regulatory Commission of the China Banking Regulatory Commission of the Ministry of Industry and Information Technology of the Central Committee of the People's Bank of China on the prevention of the risk of subsidy issuance. (2017, September 4). The People's Bank of China. Retrieved from http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html (in Chinese)

Cooper, C. G. (2019, April 1). Supervisory memorandum–1037: Regulatory treatment of virtual currencies under the Texas Money Services Act. Texas Department of Banking. Retrieved from https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf

FFIEC.31 C.F.R. 1010.100(ww). (n.d.). Federal Financial Institutions Examination Council (FFIEC). Retrieved from https://www.ffiec.gov/default.htm

FFIEC. (n.d.). Procedures for prepaid access. *BSA/AML Examination Manual*. FFIEC BSA/AML Infobase. Retrieved from https://bsaaml.ffiec.gov/manual/ProductsAndServices/10_ep

Fruth, J. (2018, February 13). 'Crypto-cleansing:' Strategies to fight digital currency money laundering and sanctions evasion. Reuters. Retrieved from https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I

FATF. (2013, June). *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services.* Financial Action Task Force (FATF). Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

FATF. (2015, June). Definitions of "anonymiser" and "mixer." *Guidance for a Risked-Based Approach: Virtual Currencies*. Financial Action Task Force (FATF), 28. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

FATF. (2015, June). *Guidance for a Risk-Based Approach: Virtual Currencies*. Financial Action Task Force (FATF), 14. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

FATF. (2015, October). *Money laundering through the physical transportation of cash*. Financial Action Task Force (FATF). Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf

FATF. (2018, October 19). Outcomes FATF plenary, 17-19 October. Financial Action Task Force (FATF), 17-19. Retrieved from http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html

FATF. (2018, October 19). Regulation of virtual assets. Financial Action Task Force (FATF). Retrieved from http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

FAQs. (2019). Silvergate Bank. Retrieved from https://www.silvergatebank.com/digital-currency/exchanges.html

FinCEN. (n.d.) BSA requirements for MSBs: 31 C.F.R. 1022.420. U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/bsa-requirements-msbs. See also https://www.ecfr.gov/cgi-bin/text-idx?SID=2df5ac33e4575e7be6e95689037843e1&mc=true&node=se31.3.1022_1420&rgn=div8

FinCEN. (2011, July 26). FinCEN issues prepaid access final rule balancing the needs of law enforcement and industry. U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/sites/default/files/shared/20110726b.pdf

FinCEN. (2011, November 2). Frequently asked questions: Final rule–definitions and other regulations relating to prepaid access. U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/sites/default/files/shared/20111102.pdf

FinCEN. (2013, March 18). Guidance on application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies. U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

FinCEN. (2017, July 26). Assessment of civil money penalty. U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf ;

J. P. Morgan creates digital coin for payments. (2019, February 14). J.P. Morgan Chase & Co. Retrieved from https://www.jpmorgan.com/global/news/digital-coin-payments

Kaminsky, D. (2011, August 4). Black ops of TCP/IP 2011 (Blackhat USA 2011). In SlideShare. Retrieved from https://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011

Loconte, R. (2018, September 10). DFS continues to foster responsible growth in NY's fintech industry with new virtual currency product approvals. NYS Department of Financial Services. Retrieved from https://www.dfs.ny.gov/about/press/pr1809101.htm

Madore, P.H. (2018, November 29). U.S. blacklists Bitcoin addresses of Iranians behind Samsam ransomware. CCN Markets. Retrieved from https://www.ccn.com/us-blacklists-bitcoin-addresses-of-iranians-behind-samsam-ransomware

OFAC FAQs: Sanctions compliance: Questions on virtual currency. (n.d.). U.S. Department of the Treasury. Retrieved from https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

Pustejovsky, C. (2018, November 12). Why is bitpay settling to merchants with stablecoins? Bitpay. Retrieved from https://blog.bitpay.com/why-bitpay-is-using-stablecoins

The Wolfsberg frequently asked questions on risk assessments for money laundering, sanctions and bribery & corruption. (2015). The Wolfsberg Group. Retrieved from https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf

Appendix A

Overview on FBSC Blockchain Analytics for AML/CFT Purposes

Most FBSC and virtual currencies are only "pseudo-anonymous" because, while there is no systematic mapping between blockchain addresses and real-world identities, occasional linkage between the two is possible through blockchain analytics using identity records maintained by certain custodians (e.g., virtual currency exchanges with an effective CIP).[26]

This Appendix A provides an overview on how the FBSC program providers and auditors may consider using blockchain analytics for AML/CFT purposes. While relevant technical concepts will be briefly discussed for context, an in-depth explanation of blockchain technologies is outside of the scope of this Appendix A. Please refer to Appendix B of the FATF *Guidance for a Risk-Based Approach: Virtual Currencies* for further information on how blockchains function as a settlement mechanism.

At present, attribution analytics and geolocation analytics are the two main types of blockchain investigation techniques used for AML/CFT purposes.

1. Attribution Analytics

Attribution analytics of blockchain function in much the same way as how "dye packs" may help thwart bank robbers. Specifically, a variety of public sources (e.g., theft reports, darknet merchant advertisement, ransomware demands, illicit ICOs, and other high-field investment frauds websites) and private sources (e.g., regulators, financial intelligence units, and law enforcement agencies) can provide reliable information on the attributions of certain blockchain addresses (e.g., criminal, risky, or safe). Through a labor-intensive process, blockchain analytics providers can gather this information and manually tag blockchain addresses that are otherwise quasi-anonymous. Also, because transactions on popular blockchains are public and form a continuous chain, risk-tagged virtual currencies will be permanently traced as such.

OFAC's recent inclusion of two Bitcoin addresses in its SDN list is a special case of such risk tagging.[27] As a result of this development, attribution analytics providers will now tag all blockchain addresses that directly or indirectly interacted with the two OFAC sanctioned addresses as "risky" or "criminal" by association. The providers will also alert an FBSC program provider or virtual currency business if one of its customers has sent value to, or received value from, such addresses.

2. Geolocation Analytics

One reason why blockchains are only pseudo-anonymous is that the geolocation of the control person of a blockchain address can usually be approximated with reasonable certainty. To do so, the investigator need only operate or control a large number of nodes, known as "scouts," in the blockchain network.

[26] See page 28 of the FATF 2015 *Guidance for a Risk-Based Approach: Virtual Currencies*.
[27] "U.S. Blacklists Bitcoin Addresses of Iranians Behind SamSam Ransomware," by P.H. Madore, November 29, 2018, available at https://www.ccn.com/us-blacklists-bitcoin-addresses-of-iranians-behind-samsam-ransomware.

These nodes are to be strategically placed around the world to maximize geolocating coverage and accuracy.[28]

The geolocation of the sender of a blockchain transaction (e.g., the control person of the origin address) can be approximated from the order in which the scouts first heard the transaction: The scout that receives a transaction first is likely the closest to the sender geographically. Alternatively, the sender geolocation can also be multi-angulated using the geolocations of the first *n* scouts that receive the transaction.

Geolocation analytics can be helpful for AML/CFT processionals because they can identify FBSC or other virtual currency transactions occurring in or interacting with high-risk jurisdictions. An analysis of the geolocations of all blockchain transactions occurring in one day for an FBSC program can also serve as a reliable indicator of the program's overall level of geographic risks.

Geolocation analytics can be performed by in-house technical teams if they have adequate resources to operate and maintain approximately 200 nodes (the exact number needed depends on the node distribution of the blockchain at issue). More FBSC program providers and virtual currency businesses are choosing to outsource geolocation analytics of blockchain transactions to third-party providers as their products improve and costs reduce.

3. Limitations on Blockchain Analytics

Despite FATF's suggestion that "third-party digital identity custodians [that mitigate virtual currency risks] would themselves need to be regulated to ensure identification/verification integrity,"[29] most blockchain analytics providers currently operate as technology companies that are not subject to functional regulations. There is no guarantee that their proprietary attribution and geolocation analytics are either accurate or comprehensive.

In addition, attribution analytics tools may be defeated when suspicious assets are channeled through mixers, tumblers, virtual currency exchanges, or wallets with perfunctory AML/CFT measures, or the blockchain's built-in anonymizing features.[30] Also, Tor, VPN, and other proxy technologies can be used to evade geolocation analytics.

AML/CFT professionals should therefore avoid relying on blockchain analytics alone in controlling the MF/FT risks. Blockchain analytics should instead be an important part of a holistic risk-mitigation strategy that incorporates various risk mitigants to address each FBSC program's unique set of risks.

---

[28] See, e.g., Dan Kaminsky's speech at Blackhat USA, August 4, 2011, available at https://www.slideshare.net /dakami/black-ops-of-tcpip-2011-black-hat-usa-2011.

[29] See page 14 of the FATF 2015 *Guidance for a Risk-Based Approach: Virtual Currencies*.

[30] See, e.g., "'Crypto-cleansing:' Strategies to Fight Digital Currency Money Laundering and Sanctions Evasion," by J. Fruth, February 13, 2018, available at https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I ("privacy coins" that are intentionally designed to prevent the traceability of transactions).

4. Factors to Consider When Selecting Blockchain Analytics Solutions

Compliance professionals should consider the following factors when selecting blockchain analytics solutions that may serve as an important part of an FBSC program's risk-based controls:

- **Experience and expertise –** A solution provider should have past experience in assisting law enforcement agencies on blockchain forensics. The provider should also have in-house blockchain and AML/CFT expertise so that the solution can remain effective as the ML/FT risks of FBSC and virtual currencies continue to evolve.
- **Risk-scoring methodologies –** The risk-scoring and/or categorization methods of a solution should be demonstrably based on an informed framework designed by competent technical and compliance specialists to ensure a reasonable degree of certainty in their relevance, effectiveness, and accuracy.
- **Staffing adequacy –** A solution provider should be adequately staffed to 1) monitor various sources of information, 2) gather newly discovered blockchain intelligence, and 3) update its solution database timely and accurately.
- **Blockchain coverage –** A solution should have adequate coverage of the particular blockchain and blockchain-specific tokenization standard (e.g., BTC-OMNI, ETH-ERC20, EOS, BCH-WHC) used by an FBSC program.
- **Entity coverage –** A solution should have adequate coverage of high-risk entity types (e.g., darknet merchants, stolen virtual currencies, mixers, fraudsters, organizers of illicit ICOs, and sanctioned entities with identifying blockchain addresses published in any sanctions list).
- **Geolocation detection –** A solution should have the ability to detect and report with a reasonable degree of certainty the approximate geolocation associated with an on-chain transaction or a blockchain address.

Appendix B

Glossary

Unless otherwise specified, terms relating to virtual currencies used in this white paper have the meanings assigned to them in 1) Appendix A "Virtual Currencies—Key Definitions and Potential AML/CFT Risks" to the FATF 2015 *Guidance for a Risk-Based Approach: Virtual Currencies* and in 2) the FATF 2013 *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services*. Certain key phrases are reproduced below for referential convenience.

Anonymization, as it relates to blockchain transactions, refers to the process through which the linkage between the source(s) of a transaction and its destination(s) is obscured to facilitate anonymity. Anonymization can be achieved through third-party service providers like mixers (i.e., service-level anonymization) or through features built into blockchains (i.e., protocol-level anonymization). Anonymization can also be optional (e.g., Dash, GRIN) or mandatory (e.g., Monero).

A **blockchain** or a **distributed ledger** is a virtual currency transaction register in the form of a publicly available, shared database with a sequential record of all transactions.

Burning or **revocation**, as either relates to FBSC, refers to the process where an FBSC program provider effects a special on-chain transaction to destroy a certain number of units of existing FBSCs.

Conversion, as it relates to FBSC, refers to the process where a customer pays an FBSC program provider certain units of the program's FBSC in exchange for the same number of units of certain sovereign currency. Redeemability or fiat redeemability has a corollary meaning.

A **mixer** or **tumbler** is a service-level anonymizer that obscures the chain of transactions on the blockchain by linking all transactions in the same Bitcoin address and sending them together in a way that makes them look as if they were sent from another address.

Off-chain, as it relates to assets or transactions, refers to assets or transactions recorded in a non-blockchain book-entry database or medium.

On-chain, as it relates to assets or transactions, refers to assets or transactions recorded on a blockchain.

Minting or **issuance**, as either relates to FBSC, refers to the process where an FBSC program provider effects a special on-chain transaction to create a certain number of units of FBSC.

NPPS refers to new payment products and services that include prepaid cards, mobile payment products, and Internet-based payment services, and exclude virtual currencies and FBSC.

Purchase, as it relates to FBSC, refers to the process where a customer pays an FBSC program provider certain units of fiat in exchange for the same number of units of the program's FBSC.

Redemption, as it relates to FBSC, refers to the process where a customer pays an FBSC program provider certain units of the program's FBSC in exchange for the same number of units of certain fiat. Redeemability or fiat redeemability has a corollary meaning.

A **scout** or **scouting node** is a node in a blockchain network whose primary objective is to gather, for analytical purposes, transient transactional data transmitted through but not preserved in the blockchain.

Virtual currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. Virtual currency can be either convertible or inconvertible, and can be either centralized or decentralized.[31]

[31] See note 23.