REGULATORY & COMPLIANCE BRIEF

OCTOBER 2020

THE FOLLOWING PRESENTATION IS FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS ADVICE, INVESTMENT, LEGAL, OR OTHERWISE.

Introduction

This brief is intended to provide an overview of PIVX for regulators, policy-makers, compliance professionals, and the general public. If an exchange can be compliant with FATF guidelines for the Bitcoin network, then by definition it can be compliant with the PIVX network as well. The reasons for this are outlined below.

PIVX is not a security and through its blockchain offers the public, and exchanges, greater transparency and less risk than Bitcoin with regards to privacy.

PIVX is fully compliant with the Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) requirements written by the Financial Action Task Force (FATF). The FATF recommendations can be found on their website: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

Furthermore, the optional privacy-preserving features of PIVX (est. Q4 2020/Q1 2021) place it into an even more favorable light when it comes to protecting digital identities online, which is of growing concern with FATF.[1] In fact, PIVX would be an optimal candidate to further help nations and governments with the following (from FATF guidelines):

> *Digital ID systems that meet high technology, organisational and governance standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying natural persons in a wide variety of settings, such as financial services, health, and e-government in the global economy of the digital age. These digital IDs are referred to as those with higher assurance levels.*

PIVX is an open-source, decentralized virtual currency, similar in nature to Bitcoin. As a fork from Bitcoin code, the PIVX network operates with nearly identical transaction rulesets as the Bitcoin network. Additionally, PIVX

[1] *http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf*

incorporates most Bitcoin backports to maintain a high degree of similarity with the current Bitcoin implementation.

As of right now, both PIVX and Bitcoin networks are public blockchains that are completely transparent. Every transaction on each network identifies the sending and receiving addresses as well as the amount of the transaction. There is no way to obscure any of those data points due to the transparent nature of the blockchain. Having that said, there is absolutely no distinguishing feature between Bitcoin and PIVX that would enable one to comply with regulatory guidelines while excluding the other.

PIVX is currently listed on many large cryptocurrency exchanges, such as Binance, Bittrex, Bithumb and Kucoin, under the ticker “PIVX”.

Privacy

Privacy-as-an-option coins are, by default, transacted in a manner that is visible on a public ledger (unlike Monero and Grin which are “privacy always on” coins). Yet they allow users the ability to conduct privacy-enhanced transactions by activating optional privacy-enhancing features. ***Bitcoin and PIVX are both examples of privacy-as-an-option coins.***

As written by Perkins Coie in their brief, certain privacy coins can and do satisfy AML/KYC and FATF regulations.

FATF released a separate “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” in 2019[2] (“FATF Virtual Asset Guidance”) to help member jurisdictions understand specifically how the FATF Recommendations apply to virtual asset activity. In June 2020, FATF completed a 12-month review of member countries’ and service providers’ compliance with

[2] *As a result of its recent June 2020 plenary, FATF agreed to a public consultation of modifications to Recommendation 1 and its corresponding Interpretive Note, which aim to strengthen the requirements for jurisdictions and private sector entities to identify, assess, and mitigate the risks of potential breaches, non-implementation, or evasion of the targeted financial sanctions related to financing of weapons of mass destruction. See FATF, Outcomes FATF Virtual Plenary, 24 June 2020 (2020), http://www.fatfgafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html.*

such recommendations on VASPs. In summarizing the key findings of its review,[3] FATF found that "overall, both the public and private sectors have made progress in implementing the revised FATF Standards" in addition to concluding that FATF need not amend its revised Standards on virtual assets and VASPs at this time. FATF also stated that it would continue its enhanced monitoring of virtual assets and VASPs by undertaking a second 12-month review by June 2021 and consider whether further updates to the FATF Standards are necessary.[4]

INITIAL RISK ASSESSMENT, CUSTOMER DUE DILIGENCE, AND PREVENTION AND MITIGATION MEASURES

The FATF Recommendations endorse essential measures that guide countries to effectively identify risks and develop policies, pursue money laundering and terrorist financing, apply preventive measures for the financial sector, establish governmental powers and enforcement authority, enhance transparency and availability of beneficial ownership information, and facilitate international cooperation.[5]

FATF further recommends that countries identify, assess, and understand the money laundering and terrorist financing risks from virtual asset activities and the operations of VASPs.[6] Based on that assessment, a risk-based approach should be applied to ensure that prevention and mitigation measures are commensurate with the risks identified.[7] FATF notes that countries should require these VASPs to "identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks."[8]

The FATF Virtual Asset Guidance mentions that "[virtual asset] products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher [money laundering or terrorist financing] risks, particularly if they

---

[3] FATF, 12 Month Review of Revised FATF Standards – Virtual Assets and VASPs (July 7, 2020), http://www.fatfgafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.
[4] However, FATF did note the eventual need for additional guidance on virtual assets and VASPs generally. See FATF, Outcomes FATF Virtual Plenary, 24 June 2020 (2020), https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html.
[5] See International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), p. 6.
[6] Id. at Interpretative Note to Recommendation No. 15.
[7] Id.
[8] Id.

inhibit a VASP's ability to identify the beneficiary. The latter is especially concerning in the context of [virtual assets], which are cross-border in nature. If customer identification and verification measures do not adequately address the risks associated with non-face-to-face or opaque transactions, the [money laundering or terrorist financing] risks increase, as does the difficulty in tracing the associated funds and identifying transaction counterparties."[9]

Consequently, FATF recommends that VASPs should consider, among others, the following elements when "identifying, assessing, and determining how best to mitigate the risks associated with covered [virtual asset] activities and the provision of VASP products and services . . . any unique features of each [virtual asset], such as [anonymity-enhanced cryptocurrencies ("AECs")], embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions."[10] FATF encourages regulators to determine whether a "VASP can manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to AECs," and if "the VASP cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities."[11]

In the context of virtual assets like privacy coins (or AECs as defined by FATF), FATF recommends that AML and CFT regulations apply to virtual assets and VASPs in addition to requiring those VASPs to be licensed and to comply with relevant financial regulations.[12] For situations involving a higher risk of money laundering or terrorist financing, FATF also recommends taking enhanced due diligence measures that are consistent with the risks identified.[13] In that regard, FATF emphasizes the need for enhanced due diligence of business relationships

---

[9] *FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 28*
[10] *Id. at paragraph 31.*
[11] *Id. at paragraph 110.*
[12] *See International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Recommendation No. 15; see also id. at Recommendation No. 26 (recommending that financial institutions be subject to adequate regulation and supervision in addition to effectively implementing the FATF Recommendations); see also id. at Interpretative Note to Recommendation No. 15 (recommending that countries should apply relevant measures to the virtual assets and the VASPs).*
[13] *Id. at Interpretative Note to Recommendation No. 10.*

and transactions with natural and legal persons from higher-risk countries in the case of virtual assets (given their cross-border nature).[14]

Additionally, FATF recommends that jurisdictions ensure that all VASPs be required to file SARs (which FATF refers to as "suspicious transaction reports") as appropriate.[15] FATF notes that "[SARs] that reference [virtual assets] have proven invaluable in furthering law enforcement investigative efforts as well as for improving the [financial intelligence unit's] ability to better understand and analyse both providers and activities in the [virtual asset] ecosystem," mentioning specifically that VASP SARs "enabled U.S. law enforcement to take action in 2017 against BTC-e" by "helping them to identify [virtual asset] wallet addresses used by BTC-e and detect different illicit streams of activity moving through the exchange."[16]

LICENSING AND REGULATORY OVERSIGHT

FATF recommends that VASPs be required to license or register and be subject to certain application requirements.[17] However, a separate licensing or registration system is not necessary for persons already licensed or registered as financial institutions within the country that subjects those financial institutions to the applicable obligations under the FATF Recommendations.[18]

In addition, FATF notes that countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML and CFT concerns and that the VASPs are effectively implementing the FATF Recommendations to mitigate money laundering and terrorist financing risks emerging from virtual assets.[19] These regulation and monitoring requirements are placed on the VASPs and not the individual virtual assets. As for supervision, FATF recommends that VASPs be supervised by a competent authority and not a self-regulating body.[20] These supervisory authorities should have "adequate powers to supervise or

[14] *FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 123.*
[15] *Id. at paragraph 124*
[16] Id. at paragraph 126.
[17] See International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Interpretative Note to Recommendation No. 15.
[18] *Id.*
[19] *Id.*
[20] *Id.*

monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing" and include the authority to conduct inspections, compel the production of information, and impose sanctions.[21]

THE FATF TRAVEL RULE

To prevent terrorists and other criminals from having unfettered access to wire transfers for moving funds, and for detecting certain misuses upon occurrence, the FATF Recommendations include a rule similar to the Funds Travel Rule, known as the FATF Travel Rule.[22] The FATF Travel Rule recommends that financial institutions be required to pass certain information to the next financial institution for qualifying funds transmittals that involve more than one financial institution.[23]

This information generally includes the name of the originator, the originator's account number or unique transaction reference number that permits traceability, the originator's information,[24] the beneficiary's name, and the beneficiary's account number.[25] Notably, however, if the information for domestic transmittals can be made available to the beneficiary financial institution and appropriate authorities by other means, then the ordering financial institution need include only the account number (or unique transaction reference number), so long as that number permits the transaction to be traceable to the originator or the beneficiary.[26]

In the context of virtual assets and privacy coins, the FATF Recommendations make clear that the FATF Travel Rule should apply to all VASPs for virtual asset transmittals as well.[27]

---

[21] *Id.*
[22] *Id. at Recommendation No. 16.*
[23] *Id. (requiring compliance in addition to recommending that records be retained for at least five years in accordance with Recommendation No. 11). The FATF Recommendations contemplate a de minimis threshold for cross-border wire transfers (no higher than $1,000), below which a financial institution would be required to pass a more limited set of transaction information to the next financial institution.*
[24] *The originator's information includes, for example, the originator's address, identification number, or date and place of birth.*
[25] *See International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Recommendation No. 16.*
[26] Id. at Interpretative Note to Recommendation No. 16 (requiring that this information should be able to be made available within three business days of receiving a request to do so)
[27] *Id. at Interpretative Note to Recommendation No. 15 (referring to the obligations in Recommendation No. 16)*

However, the FATF Recommendations expressly mention that this information, with respect to VASPs and virtual asset transmittals, "can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers."[28]

The FATF Virtual Asset Guidance elaborates on this requirement, noting that FATF "does not expect that VASPs and financial institutions, when originating a [virtual asset] transfer, would submit the required information to individual users who are not obliged entities." However, FATF stated that "VASPs receiving a [virtual asset] transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual [virtual asset] user using his/her own [distributed ledger technology] software, such as an unhosted wallet), should obtain the required originator information from their customer."[29]

COMPLIANT VASPs CAN ALREADY SATISFY REGULATOR MANDATES

In general, cryptocurrencies, including privacy coins, fit within and can comply with the current financial regulatory structure[30]. Like government-issued fiat currency, many cryptocurrencies serve as a medium of exchange existing entirely in intangible form[31]. However, cryptocurrencies are not recognized as legal tender but can substitute for such[32]. While cryptocurrencies allow for peer-to-peer transactions, they are essentially convertible to legal tender and other cryptocurrencies through the intermediaries that maintain, transfer, and exchange the cryptocurrencies.

The key difference between most cryptocurrencies and privacy coins is that most cryptocurrencies rely on a transparent public ledger, whereas privacy coins obfuscate certain transaction details and history from the public. These privacy features, however, do not prevent VASPs from complying with regulations in various jurisdictions.

---

[28] *Id. (referring to the submission of information obligations set forth in Recommendation No. 16)*
[29] *0 FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 117.*
[30] *See, e.g., FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001) (stating that FinCEN's May 9, 2019, guidance does not establish any new regulatory expectation or requirements for cryptocurrencies).*
[31] *See Sarah Jane Hughes & Stephen T. Middlebrook, Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries, Yale Journal on Regulation, Volume 32, Issue 2 (2015), http://www.cs.yale.edu/homes/jf/Hughes.pdf.*
[32] *Id.*

PRIVACY COINS CAN BE SUPPORTED WITHIN A RISK-BASED AML PROGRAM

As described above, VASPs[33] are required to implement a risk-based AML Program, which is typically based on a risk assessment. When conducting an AML risk assessment, a VASP is generally expected to analyze (a) the inherent AML risk of its customers, geographies, products, and operations, (b) the controls it applies to mitigate such inherent risks, including enhanced due diligence, and (c) the residual AML risk that the VASP faces[34]. As FATF has emphasized, its recommendations "do not predetermine any sector as higher risk," and different entities "within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, and the strength of the entity's compliance program[35]."

Inherent AML Risk of Privacy Coins, in a Comparative Context

An analysis of relevant FATF/FinCEN factors shows that privacy coins pose inherent AML product risks roughly comparable to (and in any event, not materially greater than) other cryptocurrencies or higher risk traditional payment types, such as cash, that are routinely supported by VASPs as part of a risk-based AML Program.

FATF and FinCEN have long identified, as factors tending to increase AML risk, products or services that inherently favor anonymity or products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders, and international money transfers by mobile phone. When assessing how the inherent AML risk of privacy coins under these factors compares to other cryptocurrencies and traditional currency and payment instruments, it is important to distinguish between the "anonymity" and "ease of crossing borders" factors.

---

[33] Examples of VASPs are cryptocurrency administrators, exchanges, and hosted wallet providers, including MSBs in the United States

[34] FATF, Guidance for a Risk-Based Approach for Money or Value Transfer Services, paragraph 40 (2016), http://www.fatfgafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf.

[35] FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 25.

Regarding the “anonymity” factors, privacy coins and other cryptocurrencies provide greater anonymity than account based currency equivalents (such as bank-issued payment instruments) since the transaction identifier is recorded using a cryptographically generated address, rather than personal information. But they still provide levels of anonymity nearing bearer instruments, like cash, card, or paper payment instruments, because the transactions are executed using networked distributed ledger technology and therefore are (to varying degrees) pseudonymous rather than truly anonymous. Depending on the privacy coin or cryptocurrency, addresses can be traced to natural persons using forensic technology, or permissions can be given to VASPs (e.g., view keys) enabling them to see transaction data and related addresses, as discussed below.

With regard to the “ease of crossing borders” factor, privacy coins and other cryptocurrencies present a higher inherent AML risk than cash, which is physically bulky and therefore more difficult to transport across borders, because large amounts of cash would require sufficient physical transportation and passing government border security. But privacy coins and other cryptocurrencies arguably pose a lower risk, in this respect, than cash, card, or paper payment instruments, which can cross borders with no transfer record at all (i.e., not even a publicly broadcast blockchain transaction).

FinCEN and FATF also highlight, as a related product risk factor, “the global reach of the product or service offered.” Here, too, privacy coins and other cryptocurrencies have attributes that are comparatively higher and lower risk when viewed against other payment types. Cryptocurrencies are technically capable of worldwide reach, given that any person with an internet connection and relevant software could obtain them. But they are generally not recognized as legal tender or accepted as a medium of exchange, unlike fiat currency and other traditional payment types. These limitations substantially mitigate their practical utility and reach on a global basis. For example, holders of cryptocurrencies cannot widely exchange them for goods or services. In other words, if a person were to obtain such assets when conducting illicit activity, such person could not readily convert them into cash without engaging a VASP and transacting through the VASP’s platform. Such VASP engagement

presumably would result in the holder being identified and the transaction being monitorable.

> ***If anything, privacy coins pose lower inherent AML risk than other cryptocurrencies when considering evidence of illicit use in practice.***

A recent study by the RAND Corporation found that, while most transactions made with cryptocurrencies are legitimate, Bitcoin is "widely documented to be the most dominant cryptocurrency on the dark web[36]." According to RAND, more than 90% of the cryptocurrency addresses mentioned on dark web markets or forums were Bitcoin addresses.

Other commonly cited AML product risk factors, such as whether products permit the exchange of cash for a negotiable instrument or whether products have a high or no transaction limit, do not (unlike the factors discussed above) turn on inherent characteristics of the product. These can generally be mitigated, or accentuated, for any product depending on how a VASP chooses to offer it. Thus, privacy coins and other cryptocurrencies do not present structurally higher (or lower) AML risks under these factors as compared to traditional payment types.

Viewing these product AML risk factors on balance, it appears that privacy coins pose inherent AML risks in the approximate range of high-risk traditional payment types, such as cash, other cryptocurrencies, or card or paper payment instruments. To be sure, we anticipate that VASPs supporting privacy coins would likewise classify them as inherently high-risk products (as they commonly classify other cryptocurrencies).

***But the critical takeaway here is that privacy coins do not pose an inherent AML risk that is uniquely or unmanageably high, since that risk does not appear materially greater than other high-risk traditional products that VASPs have long supported in a responsible and compliant manner*.** Just as with those traditional

---

[36] Silfversten, Erik, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, & Adrian Salas, Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. Santa Monica, CA: RAND Corporation (2020), https://www.rand.org/pubs/research_reports/RR4418.html.

products, appropriate controls can in fact yield a substantially lower and manageable AML risk for privacy coin.

Conclusion

Privacy coins reflect a nascent, but important, effort to safeguard our fundamental interest in personal and commercial financial privacy. The AML risks of privacy coins, while real, do not require specific, tailored regulations that may pose an unnecessary risk of stifling privacy coins' growth. Rather, VASPs can adequately address those AML risks by maintaining an effective, risk-based program. Allowing VASPs to support privacy tokens under current, tested AML regulations strikes the appropriate policy balance between preventing money laundering and allowing beneficial, privacy-preserving technology to develop.

For the full brief, please visit here.

In December 2020 or early in 2021, PIVX will offer users functionality that is similar to the Bitcoin network but that includes the added option of enhancing privacy through the use of zero-knowledge proofs[37] [38]. This protocol was developed by the Electric Coin Company[39], and currently used by Zcash[40].

The new protocol will differentiate the two types of addresses: transparent and shielded. Choosing between them will be completely **optional**.

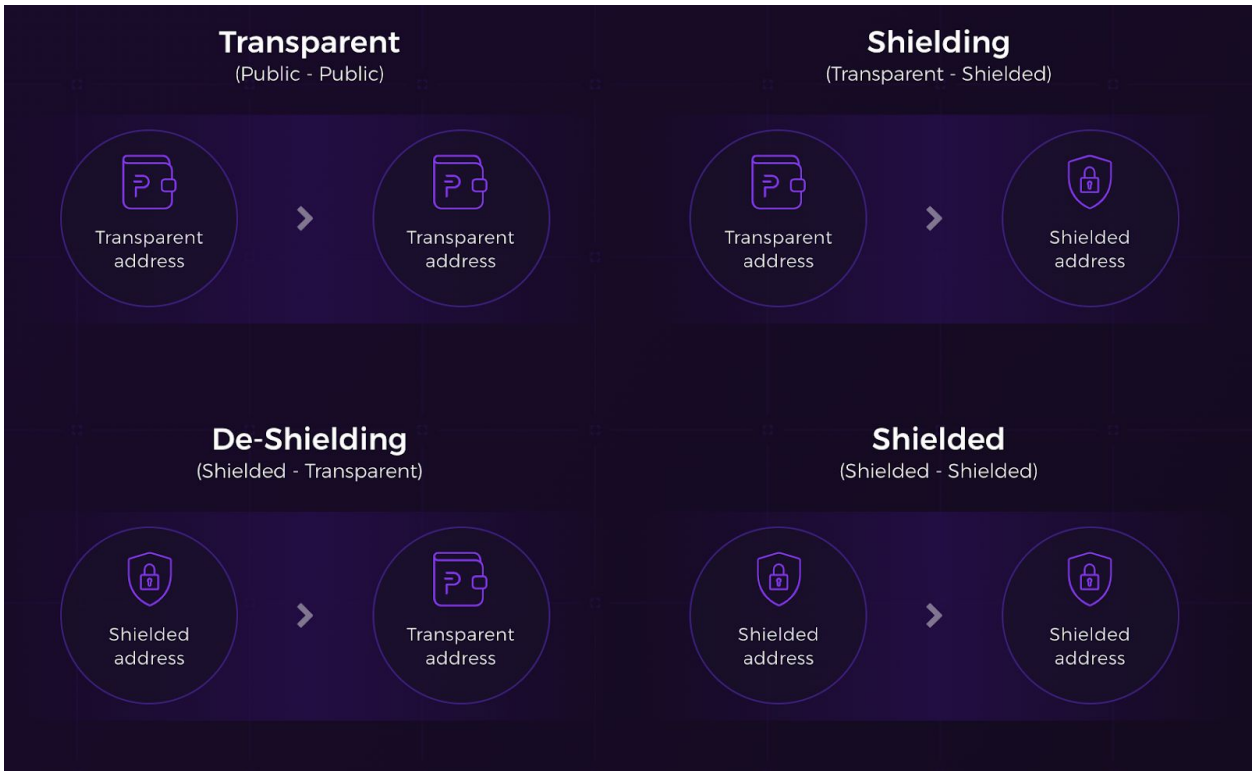
Transparent addresses are the very same as the regular addresses seen in Bitcoin and all other public blockchains. On the other hand, PIVX will allow the users to **shield** their funds by transferring the funds from the transparent address to the shielded address, making it virtually impossible to recognize for any outside observer. Funds can be **unshielded** at any time later by transferring them back to the transparent address, which makes them visible on the blockchain again.

[37] https://decrypt.co/resources/zero-knowledge-proofs-explained-learn-guide
[38] https://www.wired.com/story/zero-knowledge-proofs/
[39] https://electriccoin.co/
[40] https://z.cash/

The zero-knowledge proof privacy enhancement to certain PIVX transactions allows for verification of transactions without revealing certain information to the public. However, users that send or receive PIVX from or to their D- or S-address (shielded address) have the ability to reveal the details of the transaction that are specific to their account via a viewing key. This viewing key can be shared with any third party and enables full transparency with regard to the account associated with that viewing key. This enables users and VASPs to disclose certain transaction details associated with a given account to a third party, without publicly disclosing that user's transactional information.

To clarify, the use of the shielded addresses is completely optional. Exchanges can allow the deposits only using the transparent transactions, which keeps PIVX in the same position as Bitcoin or any other public blockchains.

This optionality will enable **four different types** of transactions on the PIVX network.



Transparent addresses are the very same as the regular addresses seen in Bitcoin and all other public blockchains. On the other hand, PIVX will allow the users to **shield** their funds by transferring the funds from the transparent address to the shielded address, making it virtually impossible to recognize for any outside observer. Funds can be **unshielded** at any time later by transferring them back to the transparent address, which makes them visible on the blockchain again.

To clarify, the use of the shielded addresses is completely optional. Exchanges can allow the deposits only using the transparent transactions, which keeps PIVX in the same position as Bitcoin or any other public blockchains.

Additionally, in the short future, a sending user can include a brief memo with each transaction that only the recipient can see. This enables users to share information that may be necessary in a given transaction. For example, when required, users may include certain information in the memo that is necessary for VASPs to comply with the Travel Rule (where implemented). Additionally, required originator and beneficiary information could be attached directly to shielded PIVX transactions, facilitating compliance with Travel Rule requirements[41]. Furthermore, users can elect to transact without using any of the above-mentioned privacy features, making certain transactional data visible to the public.[42] Lastly, VASPs can require up-front disclosures during the registration process and on an ongoing basis to satisfy KYC obligations.

[41] https://electriccoin.co/blog/how-zcash-is-compliant-with-the-fatf-recommendations/
[42] *Public PIVX transactions are viewable by the public, just like regular Bitcoin transactions.*

IN SUMMARY:

1. PIVX is not a security and through its blockchain offers the public, and exchanges, greater transparency and less risk than Bitcoin with regards to privacy.

2. If an exchange can be compliant with FATF guidelines for the Bitcoin network, then by definition it can be compliant with the PIVX network as well.

3. PIVX is an open-source, decentralized virtual currency, similar in nature to Bitcoin. As a fork from Bitcoin code, the PIVX network operates with nearly identical transaction rulesets as the Bitcoin network. Additionally, PIVX incorporates most Bitcoin backports to maintain a high degree of similarity with the current Bitcoin implementation.

4. PIVX and Bitcoin are both “privacy optional” - and inasmuch no different than Bitcoin, and in fact carries a lower risk of regulatory non-compliance than Bitcoin for both technical and non-technical reasons.

Summary of Guidelines for exchanges as it relates to VAs/AECs

Within the FATF guidelines, the VASP must ultimately be able to prove that the VASP can understand, manage, and mitigate the risks presented in all Virtual Assets offered by the VASP, including the features that may hide the identity of the sender, recipient, holder or beneficial owner of a Virtual Asset.

The Travel Rules stipulate that all VASPs require their users provide specific details about the originator or beneficiary of a VA transfer deposits into customer accounts or withdrawals from customer accounts.

For any withdrawals, the VASP must also indicate whether the originator or beneficiary addresses are custodied at another VASP.

The originating VASP must provide and verify accuracy of the required originating transaction information, while the beneficiary VASP must do the same for the beneficiary side of the transaction.

This helps ensure accurate information and an equal division of requirements between the two parties.

The goal of these Travel Rules is to most closely mimic the already in place regulatory requirements observed between traditional fiat wire transfers.

The Travel Rule that specifically addresses this point mandates that the VASP must be able to collect required information/details which includes a plethora of details. Exchanges are in a unique solution to adequately obtain this information in that, unlike many wallet providers, KYC/AML processes are already a familiar and standard part of the onboarding process for any user of a larger centralized exchange.

Outgoing transfers of PIV are covered: Withdrawals by an individual with an account on the exchange (from the VASP) - this data is able to be reported to regulators including originator's name, originator's account number, originator's physical (geographical) address, national identity number, and beneficiary's account number as an individual could be precluded from sending from a shielded address from centralized exchanges. This would be enforced by the exchange requiring that outgoing transfers could ONLY be made from and to an "unshielded" address.

PIVX's optional privacy solution (sending from a shielded address) can only be activated by the sender, so there is zero risk for an exchange for outgoing transfers because they maintain complete control of the processing of customer withdrawal requests.

Incoming transfers (deposits) of PIV are covered — A deposit to an exchange that has come from a shielded address is easily identifiable by a VASP due to a VASP's use of transparent deposit addresses and it's own KYC/AML service platforms. Due to the transparency of the Bitcoin network, there are many service platforms that can perform this function. PIVX, which also has a transparent blockchain, with identical rulesets to Bitcoin is also covered by many service platforms performing this function. Utilizing these services a VASP can detect

these transactions, filter them and report on them to regulators in an easy and efficient manner.

PIVX privacy technology is built upon the functionality that is similar to the Bitcoin network but that includes the added option of enhancing privacy through the use of zero-knowledge proof. This is accomplished through the use of two types of addresses: transparent and shielded, and the exchange would have the right and ability to limit and restrict the types of addresses used.

Also of note: Cross-border transfers below the USD/EUR 1,000 threshold must include the above information as well, however, it does not need to be verified for accuracy unless there is some suspicion of terrorist financing or money laundering.

How to remain compliant with the Travel Rule with PIVX

Bitcoin and PIVX are two cryptocurrencies that possess many similarities including its optional privacy aspect and are equivalent in respect to all legal standings.

With this being true, the solution to remaining compliant with the Travel Rule and PIVX is no different as well. The current mechanisms and protections that are utilized in and for the Bitcoin ecosystem for money laundering prevention are equally as applicable to PIVX.

Unshielded transactions can be readily distinguished as such on the blockchain and thus, all transactions through (to and out of) the exchange can be risk scored based on behavioral patterns, proximity to problematic addresses, country of origin or receipt of transaction, and any other value, or other criteria defined by the exchange that would place the transaction (and user) as risky.

The FATF Guidelines make it clear there onus and is on the exchange to remain compliant and provide the required documentation and details. Many of these tools are provided by KYC/AML providers, and these providers work extensively with law enforcement, traditional financial institutions, and VASPs. More and more companies are entering into this space, and these service partners continue to grow. These services are available to support Bitcoin, and PIVX.