contents

3 ABOUT US
4 CHANGES ARE VISIBLE – MORE COMPLIANCE AND MORE SECURITY
5 KNOW YOUR EXCHANGE
7 EXECUTIVE SUMMARY
11 EXAMINATION METHODOLOGY
17 RISK ASSESSMENT RESULTS
27 APPENDIX: EXCHANGE SPECIFIC FINDINGS
34 APPENDIX: GLOSSARY
38 APPENDIX: CASE STUDIES
39 DISCLAIMER
about us

Coinfirm is a global leader in compliance technology for cryptocurrencies and the blockchain-based financial ecosystem. By providing solutions that fight fraud and allow traditional financial institutions to meet compliance requirements when interacting with online currencies, we bridge the gap between the crypto and fiat currency worlds, enabling new monetary technologies to reach their full potential and contributing to the creation of a seamless, democratic and transparent financial system.

Coinfirm is the world’s leading provider of anti-money laundering (AML) risk assessment products and services for cryptocurrencies and blockchain applications. The Coinfirm AML Platform sets the global standard in this area covering over 70% of the cryptocurrency market - our software is blockchain agnostic, and we analyze Bitcoin, Bitcoin Cash, Litecoin, ETH (incl. ERC tokens), NEO, Dash, Hyperledger and more. We analyze transaction patterns in real time, using more than 200 risk indicators, including behavioral analysis and data science techniques, delivering reports that let you make a simple yes or no decision. In short, we simplify the complicated.

Coinfirm’s AML Platform offers a variety of off-the-shelf and tailored AML products for companies and financial institutions operating in the cryptocurrency ecosystem. One such example is the real-time monitoring of AML risk of cryptocurrency exchanges, wallet providers, payment processors, token issuers and other types of entities. The user can run fully automated AML risk assessment and risk monitoring of thousands of wallets belonging to various users.

Coinfirm provides an end-to-end know your customer (KYC) solution covering entities’ activity in the crypto ecosystem. We deliver a clear risk assessment score, in a unified format and in line with the legal requirements of different jurisdictions, allowing our clients to make a more informed decision and whether to accept a client or a transaction risk. Coinfirm combines our extensive regulatory and operational experience in banking, AML/KYC with the very latest technological developments.

Coinfirm offers more than just a simple screening process; in addition to user identification (ID) and verification, we provide a full KYC risk assessment, backed by proprietary algorithms and technologies including live video ID, and risk evaluation of cryptocurrency wallets belonging to screened profiles.

Additionally, Coinfirm has developed dedicated blockchain solutions such as the data provenance platform Trudatum that was recently integrated by the largest bank in Central Europe. We offer services to major traditional and blockchain institutions in jurisdictions all over the world including the UK, US, EU, Switzerland, Japan and the Middle East.
Previously Coinfirm published a ‘Risk Based Guidance for Managing Cryptocurrencies’ (the ‘Guidance’) which was provided to guide users and interested parties on how to manage cryptocurrency risks, and in this report we provide guidance on the risks associated with the exchanges that handle these currencies, using a range of risk factors associated with financial crime, consumer protection and regulatory compliance.

Visit [www.coinfirm.com](http://www.coinfirm.com) to know more about our products and services.

**changes are visible - more compliance and security**

Since the first day that Coinfirm became operational in 2016 there has been a growing trend for the largest cryptocurrency exchanges in the market to move towards regulation and authorisation, and to seek approval and acceptance, whilst electing to do so in those jurisdictions that have a more sympathetic and supportive regulatory framework, and that also have a positive reputation for consumer protection.

Many of the entities that have been reviewed in this Report have sought authorisation by regulatory supervisors such as FinCEN, AUSTRAC or the Japanese Financial Services Authority, have done so to enhance their reputation and lower their perceived compliance risk.

We expect that more entities will follow this path, as new regulations are introduced around the world as part of a global standard of oversight, and firms seek to attract new investments and use by those who wish to have the comfort and assurance that regulation seeks to provide.

Looking forward beyond 2019, it is our firm belief that the use of cryptocurrencies will fall under two separate headings, regulated activity and unregulated activity. Those firms that choose not to seek authorisation and become ‘mainstream’, are likely to meet with close scrutiny from law enforcement agencies due to the fact that any value exchange that is performed and not licensed, is likely to be considered unlawful. Coinfirm aims to support those businesses who wish to operate to the most appropriate regulatory standards whilst managing the rights of individuals to have privacy and security in their activities.
know your exchange

Recent innovative technologies such as blockchain offers an exciting new foundation to develop RegTech solutions that can achieve significant improvements in productivity, efficiency and effectiveness in global compliance and payments solutions and services.

The cryptocurrency exchanges are the mainstay and guardians of the crypto ecosystem. They are primarily responsible for protecting their clients and promoting the good reputation of cryptocurrency markets. Negative news relating to exchanges adversely impacts upon the market and even impact the valuation of cryptocurrencies itself.

Exchanges are gatekeepers to the crypto markets – if this responsibility is exercised effectively and diligently then they can provide control, stability, security and comfort. Know Your Exchange is one of the most important challenges for market participants and financial institutions looking for exposure to this sector.1

Coinfirm AML Risk Report - the new Know Your Exchange solution

---

The aims and objectives of this analysis is to provide reliable, objective and authoritative data that can be used to guide and inform readers on good compliance and to identify potential risks that may indicate a greater risk of financial or reputational loss or disadvantage.

The analysis that has been performed is based upon a range of risk factors that are recognised in international laws, regulations and guidance, including factors such as: the application of customer due diligence procedures to identify and verify users of the exchange services; regulatory licensing and authorisation; jurisdiction risk; customer risk; and adverse media news that may indicate any association with crime and terrorism.

The details that are provided should not be deemed as providing advice or in any way appear to recommend that the reader should use or not use a service, but we do hope and anticipate that the results can be used as part of a wider and comprehensive process of risk assessment of each exchange.

The purpose of this report is primarily therefore to:

1. Help users to understand more about some of the key risks that can be identified and are associated with each cryptocurrency exchange, to support the user to make a more informed decision;

2. Guide supervisors who are charged with developing a framework of regulatory systems and controls to manage the activities of cryptocurrency exchanges and to benefit from having access to a comprehensive and consolidated set of financial crime compliance risk analysis.

This Report is the first in a series of updates that will be provided and published periodically to clients of Coinfirm products and services, and also on demand when requested by interested parties. Our sincere hope and expectation is that by providing this information and analysis on some of the inherent risks relating to cryptocurrency and blockchain use, we can make a sustainable and measurable contribution to the development and promotion of global standards in AML/KYC for blockchain applications.

The Report does not cover the risk associated with:

- Custodial Wallets (note, in some situations activity can be very similar in terms of operating model to exchanges)
- Payments Applications and Payments Gatekeepers
- Security Token Offering Market Operators (STO).
executive summary

This report and analysis represents the findings of a review of 216 cryptocurrency exchanges who collectively represent more than 90% of global exchange activity. They include a variety of crypto-exchange models, some trade both cryptocurrency and fiat currencies, whilst others trade only between cryptocurrencies and appear to have taken steps to remove any risks related to the exchange of fiat currency.

Overall, the levels of compliance across all 216 exchanges is generally below those that are expected to be seen in regulated businesses. However, the results also appear to suggest that those exchanges that have chosen to be licensed and meet the requirements of regulatory authorisation, similar to the path taken by similar ‘money value’ transfer operators such as Money Service Businesses, have the highest standards of technical compliance.

Each exchange has been assessed against seven categories of risk detailed in the Examination Methodology (see below). Each category has been assigned a risk assessment of either low, medium or high risk. The cryptocurrency market is by default considered to be high risk for financial crime, and so the use of terms that include ‘low’ refers to a category of lower risk, within a high-risk business. It should not be inferred that this means that the activity is considered to be low risk.

The findings presented in this independent report represent the outcomes from a data collection and examination period conducted from September 2018 to February 2019 and is provided in the utmost good faith. It does not therefore include any subsequent developments after the period of when the data was collected, however Coinfirm may undertake to update these findings going forward and will amend the report accordingly. Please contact for any details.

Assessment of selected three exchanges - table and description (presented on following page)

<table>
<thead>
<tr>
<th>Exchange Name</th>
<th>Licensed and Authorised</th>
<th>Customer Due Diligence/KYC</th>
<th>AML Policies and Procedures</th>
<th>Sanctions</th>
<th>Senior Public Figure/PEPs</th>
<th>Jurisdiction</th>
<th>Negative and Adverse Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShapeShift</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Binance</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Poloniex</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Exchange</td>
<td>Description</td>
<td>AML Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shapeshift</td>
<td>An Exchange that allows you to exchange cryptocurrencies and tokens without completing any registration process.</td>
<td>The exchange supports anonymous coins such as Monero, Zcash and Komodo. More recently ShapeShift has announced the gradual introduction of membership, which will support the verification of participants. There is no information about AML policies implemented.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binance</td>
<td>One of the biggest exchanges (according to trade volume). The platform is available only for cryptocurrencies, and fiat currencies are not supported. Deposits and withdrawals (below 2 BTC) are allowed with no requirement to completing KYC. For withdrawals above 2BTC a user needs to be identified and verified. The AML Policy of Binance includes reference to detecting unusual activity in the account and access controls to the account. The exchange supports anonymous coins Monero and Zcash.</td>
<td>Although recent changes appear to have been implemented to improve compliance systems and controls, the lengthy period of exposure to anonymous activity that pre-dates these new enhanced controls has resulted in the regulatory risk rated as ‘High’.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poloniex</td>
<td>A US-based cryptocurrency exchange platform launched in 2014 and it was the first exchange that offered cryptocurrency-to-cryptocurrency trading on a large scale. Fiat currencies are not supported. There was no KYC process required on the exchange up until 2018, but now all trading options are available only after completing KYC verification and transaction monitoring process has been implemented. Poloniex is registered with the Financial Crimes Enforcement Network (“FinCEN”) as a Money Services Business (“MSB”).</td>
<td>The risk is lower. One of the leaders of the changes. Both in terms of KYC / AML processes but also licensing and jurisdiction.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conclusion**
(overall risk assessment based upon findings of this review)
If it has been possible to confirm that an exchange has implemented comprehensive procedures to counter the threat of illicit activities, then a lower risk indicator has been assigned. If it has not been possible to confirm that an exchange has implemented policies and procedures in a risk area, or if the procedures introduced do not appear to be sufficiently robust to deter or detect illicit activities, then a higher level of risk has been assigned.

In this report, we have resisted the temptation to apply an overall risk assessment for each exchange.

Instead, an objective assessment has been performed and recorded for each risk factor for each exchange and a final assessment of lower, medium or higher risk provided of individual risks.

This is considered to be appropriate because it is recognized that each component part of the framework of systems and controls is equally and separately as important and inter-dependent on the other factors when conducting a financial crime risk assessment for each exchange.

**Number of exchanges classified as high/medium/low risk under each of the examined risk categories:**

<table>
<thead>
<tr>
<th>RISK</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>License and Authorisation</td>
<td>30</td>
<td>7</td>
<td>179</td>
</tr>
<tr>
<td>Customer Due Diligence/KYC</td>
<td>67</td>
<td>35</td>
<td>114</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>56</td>
<td>69</td>
<td>91</td>
</tr>
<tr>
<td>Sanctions</td>
<td>76</td>
<td>21</td>
<td>119</td>
</tr>
<tr>
<td>Senior Public Figure/ PEPs</td>
<td>63</td>
<td>7</td>
<td>146</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>47</td>
<td>109</td>
<td>60</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>114</td>
<td>85</td>
<td>17</td>
</tr>
</tbody>
</table>
Average monthly volume on exchanges classified as high/medium/low risk under each of the examined risk categories (in billion USD):

<table>
<thead>
<tr>
<th>RISK</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>License and Authorisation</td>
<td>$42.2 B</td>
<td>$12.2 B</td>
<td>$291.7 B</td>
</tr>
<tr>
<td>Customer Due Diligence/KYC</td>
<td>$62 B</td>
<td>$42 B</td>
<td>$242.1 B</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>$81.7 B</td>
<td>$195.9 B</td>
<td>$68.4 B</td>
</tr>
<tr>
<td>Sanctions</td>
<td>$200.9 B</td>
<td>$54.5 B</td>
<td>$90.7 B</td>
</tr>
<tr>
<td>Senior Public Figure/PEPs</td>
<td>$97.7 B</td>
<td>$1.8 B</td>
<td>$246.6 B</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>$32.4 B</td>
<td>$260 B</td>
<td>$53.8 B</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>$84.2 B</td>
<td>$229.8 B</td>
<td>$32.1 B</td>
</tr>
</tbody>
</table>

The most consistent areas of high risk due to low levels of compliance relate to screening for Politically Exposed Persons and the KYC process. These are important controls due to the risks of laundering the proceeds of crimes including: sales of illicit drugs, bribery and corruption, illegal arms dealing, the financing of terrorism and nuclear proliferation and humanitarian abuses such as human trafficking.

Coinfirm will continue to engage and monitor exchange activities, adding new exchanges and new areas of risks and controls to provide the fullest possible assessment of risk in cryptocurrencies exchange activity.
examination methodology
examination methodology

According to the risk assessment models and guidance that have been published by leading bodies such as the Basel Committee (‘Sound management of risks related to money laundering and financing of terrorism’\(^2\)) and the Financial Action Task Force (‘40 Recommendations’ published in February 2012)\(^3\) regulated entities are required to adopt a risk-based approach to manage and assess financial crime risks.

These risk indicators and considerations include assessing whether the entity has:

1. Obtained a regulatory license and authorisation to operate
2. Anti-Money Laundering Policies and Procedures
3. Customer Due Diligence/ Know Your Customer Procedures
4. Transactions Monitoring Procedures (Sanctions Screening and Proof of Source of Funds)
5. Senior Public Figures/ Politically Exposed Persons Risk Screening
6. Been incorporated in a higher risk jurisdiction
7. Negative News or Adverse Media

A framework of systems and controls to manage financial crime risks includes many more policies and procedures in a mature regulated business, including: appointing a senior manager with responsibility for financial compliance control; internal audit testing according to the three-line defence model; suspicious activity reporting; and record keeping.

The absence of any reference to these controls does not suggest that these are not important. However, these entity-specific controls cannot be verified without authorised disclosure of this information. This information has not been available at the time of this report but will be included going forward when an entity chooses to freely disclose this information so that this may be included in the assessment of their risk profile.

Described below are the seven categories of compliance risk and control that are considered essential to support compliance standards and the effective management of regulatory and operational risks.

---

\(^2\) [https://www.bis.org/bcbs/publ/d405.pdf](https://www.bis.org/bcbs/publ/d405.pdf)

\(^3\) [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf)
1. Licensed and Authorised Activity

It is increasingly recognised that exchange activities should meet minimum standards of financial crime regulatory compliance as part of a global response to managing and mitigating the use and abuse of cryptocurrency-related services by illicit actors.

One measure that infers a higher level of compliance performance, and therefore risk mitigation, is that the exchange entity has sought approval and authorisation of a regulatory supervisor or central banking authority. This infers that the entity has made a commitment to meet regulatory standards that will enhance the effectiveness of financial crime management controls.

Whilst being authorized should not by itself be relied upon to neither confirm that an exchange is compliant, nor default to a lower risk status overall, the process for seeking authorization from a supervisory body typically requires that the entity is able to demonstrate that:

1. The senior management team are ‘fit and proper’ persons and have the commensurate level of skills, knowledge and ethics to manage the entity in an appropriate manner

2. The entity has in place an appropriate framework of systems and controls to manage and mitigate the threat of the entity being used by criminals

3. The clients of the entity will be required to meet minimum standards of customer due diligence checks and verification before they enter into a relationship with the entity, and thereafter as part of a continuous programme of crime risk management

4. The entity will not support financial crimes or the financing of terrorism

5. The entity has in place appropriate controls to ensure that client assets and investments are held securely, and that the threats from for example computer-based ‘cyber’ activity are mitigated

It is recognized that exchange activity is not yet required to be ‘regulated’ in every jurisdiction, but where this is required, and an exchange has been authorised in any jurisdiction then this is noted as lower risk.

Where the entity has been licensed in a jurisdiction that is assessed as ‘higher’, the medium risk may have been recognized. However, presence in any sanctioned country always resulted in high risk evaluation.

Where an entity is not licensed, or it has not been possible to confirm any licensing, then this has been noted as representing a higher risk.
2. Anti-Money Laundering Policies and Procedures

A fundamental requirement for any financial services provider, wherever they are incorporated, is to have in place documented policies and procedures that confirm the systems and controls that the firm has in place to manage financial crime risks.

In this review, an exchange that has publicly available documents, and that can therefore be scrutinised to confirm the technical merits of these policies, have been assessed more favorably than an exchange where this has not been possible. Those that have policies and procedures that are available have been assessed as low risk if these meet regulatory expectations and medium risk where they meet some, but not all, regulatory requirements. The absence of records, or the inability to identify these records, has been marked as higher risk.

3. Customer Due Diligence/Know Your Customer Procedures

The cornerstone and foundation of an effective framework of financial crime compliance systems and controls is for an exchange to have in place robust and effective processes to identify and verify the identity and risk of each customer, whether that customer is a natural person or legally formed entity or legal arrangement, using independent sources of data and documentation.

Natural customer identifying details include: name; residential address; date of birth; and nationality.

Legally formed entities are required to be identified from documents that confirm the date and place of incorporation, the beneficial owners and controlling persons, and usual business trading address and type of activity.

For each customer it is expected that the source of funds will be identified, typically using technology that can scrutinize the public ledger, and so it is expected that an exchange will have in place transaction monitoring technology to confirm the provenance of funds, and to identify any links to illicit sources of funds on the public ledger.

4. Sanctions Compliance

Non-compliance with sanctions is a criminal offence in most jurisdictions of the world, and all exchanges are required to have in place policies and procedures to manage and mitigate the threat that sanctions evaders use their services to move value in contravention of these national and international sanctions laws. These laws include designations that have been made by the United Nations Security Council according to the mandate and authority under Chapter 7 of the UN Charter.
Additionally, where exchanges use fiat currencies such as the US dollar, then these exchanges are required to observe and comply with prohibitions and licensing laws that apply, such as imposed by the United States of America (Office of Foreign Asset Control)\(^4\), and other supranational bodies, such as the European Union. The absence of any statements of compliance in exchange policies and procedures has been assessed as higher risk, whilst any statement of compliance has been assessed as lower risk.

5. Senior Public Figures/Politically Exposed Persons

Senior public figures who abuse their positions of office are the subject of increasing international scrutiny and monitoring for risks relating to bribery and corruption and criminal tax evasion.

The fight against crime, and the steps that must be taken to mitigate and identify this abuse, require that exchanges must identify public officials and manage these relationships according to enhanced due diligence requirements. This includes obtaining greater comfort and confidence concerning the source of funds and wealth by verifying the details that are provided by the customer.

In addition to taking steps to identify the source of the customers wealth, an exchange is also expected to have in place policies and procedures that support the continuous monitoring of customer’s related news and social media updates for information that may indicate a risk of association with criminal conduct.

6. Jurisdiction Risk (Place of Registration or Incorporation)

Factors that contribute to financial crime compliance risks in a country or jurisdiction include sanctions restrictions, terrorist activity, criminal conduct, bribery and corruption, political instability, poor regulation and weak judiciary.

The overall and final assessment of jurisdiction risk was determined by a reasonable assessment of these risk factors and having regard for reports provided by national crime bodies and groups such as FATF, Transparency International and START\(^5\), for each country relevant for this Report.

The pictorial representation of countries risk assessment conducted for the purpose of this Report was presented on diagram on following page.

---

\(^4\) The Office of Foreign Assets Control (OFAC) is a financial intelligence and enforcement agency of the U.S. Treasury Department. It administers and enforces economic and trade sanctions in support of U.S. national security and foreign policy objectives. Under Presidential national emergency powers, OFAC carries out its activities against foreign states as well as a variety of other organizations and individuals, like terrorist groups, deemed to be a threat to U.S. national security.

\(^5\) https://www.start.umd.edu/gtd/
7. Negative and Adverse Media (About the Exchange)

In an increasingly globalized and technologically advanced world it is possible to monitor and obtain news alerts and warnings of suspected or actual criminal conduct that can be used to refine and adjust risk assessments.

It is recognized that in most jurisdictions it is not appropriate to rely upon statements of suspected illicit conduct unless there is an actual successful criminal prosecution, and therefore in this assessment all reports are appropriately assessed on a case-by-case basis before a final risk assessment is confirmed.

Assessments of higher risk will be attributed to exchanges that have multiple or confirmed reports of association with criminal conduct, whilst those who have no identifiable reports will be lower. Exchanges with multiple reports of suspected adverse social media have been assessed as medium risk.
assessment results
risk assessment results

As part of our analysis we have analysed 216 cryptocurrency exchanges. This sample has been selected to provide a random sample of exchanges according to different trading volumes, different jurisdictions and a wide cross-section of available crypto currencies and tokens. Included in the sample are some better known exchanges who have been operating on the market for several years and others who started their operations in 2018.

1. License and Authorisation Risk

30 (14%) of exchanges were confirmed as being licensed by regulators and these are responsible for average monthly turnover of USD $42.2 billion.

Most exchanges that are registered have chosen to do so as a Money Service Business (MSB) with Financial Crimes Enforcement Network (FinCEN) in the United States, Hong Kong (HKMA) and Japan (FSA).

2. Anti-Money Laundering Policies and Procedures

125 (58%) of exchanges were confirmed as having in place statements of AML Policies and Procedures. In terms of transactions volume, more than 75% of exchanges were evaluated as lower or medium in this category as this infers better compliance.
Almost 56 (26%) of the exchanges were assessed as having introduced AML procedures that include procedures such as ongoing monitoring of transactions, recruiting a Money Laundering Reporting Officer or Compliance Officer and training employees in anti-money laundering.

3. Customer Due Diligence/ Know Your Customer Procedures

149 (69%) of exchanges did not have complete and transparent CDD/KYC procedures.

Almost 40% of exchanges do not support FIAT currencies and conduct exchange only between cryptocurrencies. Of those exchanges that do exchange FIAT currencies, 49 (23%) had full KYC processes that supported both deposits and withdrawals for crypto and fiat currency transactions.

45 (21%) are the exchanges that allow for the deposit of crypto funds without KYC, while all operations in FIAT on these exchanges require from user to finish full KYC process.

13 exchanges, including Yobit, Cryptonex, Livecoin support FIAT currency exchange but do not require any KYC to be performed for either FIAT or crypto transactions. In six out of said 13 exchanges the jurisdiction (place of registration or incorporation) of the entity was not identifiable and these exchanges were assessed as the highest risk.

<table>
<thead>
<tr>
<th>Average Monthly Volume (in billion USD)</th>
<th>KYC required</th>
<th>KYC not required</th>
<th>KYC required only above certain deposit/withdrawal threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptocurrency Deposits</td>
<td>$27 B</td>
<td>$311.8 B</td>
<td>$0.5 B</td>
</tr>
<tr>
<td>Cryptocurrency Withdrawals</td>
<td>$64.5 B</td>
<td>$99.5 B</td>
<td>$175.4 B</td>
</tr>
<tr>
<td>Fiat Deposits</td>
<td>$127.9 B</td>
<td>$8.8 B</td>
<td>$4.1 B</td>
</tr>
<tr>
<td>Fiat Withdrawals</td>
<td>$61.7 B</td>
<td>$8.2 B</td>
<td>$70.9 B</td>
</tr>
</tbody>
</table>
Out of 60 (28%) exchanges for which the KYC Process Risk was evaluated as high, 40 (19%) exchanges were also noted as being located within a high risk jurisdiction.

Below are some notable findings:

WEX requires full KYC for FIAT withdrawals, but not for other types of transactions. 17 (8%) of exchanges do not require any KYC for a deposit in crypto but do require it for withdrawal transactions. These exchanges include CoinBene, IDAX, DOBI, BitBay and ZB.com.

In the case of exchanges that do not support FIAT, there are only 3 exchanges that require users to go through the KYC process for both deposits and withdrawals, and that is Poloniex, BtcTrade.im and Stronghold.

Multiple exchanges have a limited KYC procedures. 31 have introduced a KYC process for crypto withdrawals below 10k USD (e.g. Huobi, DigiFinex, CoinsBank and RightBTC) and 29 have a limit above 10k USD (e.g. Binance, Bithumb, OKEx and Bibox). 13 have introduced a KYC process for FIAT withdrawals below 10k USD (e.g. OKEx Kraken, CEX and Indodax). Bithumb and BTC-Alpha exchanges require limited KYC which allows you to withdraw more than $10k of FIAT per day without KYC.
Most exchanges that do require KYC to be performed, obtain personal data and verify these details using documents such as a scanned copy of an identity card or passport and a selfie (mostly with a document). An increasing number of exchanges now require a second form of additional identity verification using a proof of address document.

Some exchanges observe higher standards of KYC compliance and require proof of a bank account (e.g. Kraken, Gemini, Stronghold, ISX), the source of funds (e.g. Poloniex, Gatecoin) and, in some cases, a video interview (e.g. Gatecoin, OKCoin.cn).

<table>
<thead>
<tr>
<th>Documents required in CDD/KYC process</th>
<th>Number of exchanges</th>
<th>% of number of exchanges</th>
<th>Average monthly volume (in billion USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal info</td>
<td>166</td>
<td>77%</td>
<td>$266 B</td>
</tr>
<tr>
<td>National ID number</td>
<td>124</td>
<td>57%</td>
<td>$136 B</td>
</tr>
<tr>
<td>ID scan or photo</td>
<td>154</td>
<td>71%</td>
<td>$198 B</td>
</tr>
<tr>
<td>Selfie</td>
<td>16</td>
<td>7%</td>
<td>$7 B</td>
</tr>
<tr>
<td>Selfie with a document</td>
<td>93</td>
<td>43%</td>
<td>$220 B</td>
</tr>
<tr>
<td>Proof of address</td>
<td>86</td>
<td>40%</td>
<td>$114 B</td>
</tr>
<tr>
<td>Proof of bank account</td>
<td>28</td>
<td>13%</td>
<td>$24 B</td>
</tr>
<tr>
<td>Source of funds</td>
<td>14</td>
<td>6%</td>
<td>$5 B</td>
</tr>
<tr>
<td>Video</td>
<td>10</td>
<td>5%</td>
<td>$24 B</td>
</tr>
<tr>
<td>Multiple tiers KYC</td>
<td>37</td>
<td>17%</td>
<td>$75 B</td>
</tr>
</tbody>
</table>
4. Sanctions Compliance

119 (55%) of exchanges do not have clear statements of policies and procedures that confirm that they comply with UN and other local sanctions laws such as those from the USA.

This implies that a significant number of transactions are not being screened to sanctions laws based on average monthly transaction volume.

5. Senior Public Figures/Politically Exposed Persons

146 (68%) of exchanges do not appear to have procedures in place to identify PEPs.

Less than one third of the exchanges appear to verify users registering on the exchange against the watch lists that are widely provided by KYC utility vendors to identify senior public officials and PEPs. Some exchanges have statements that state that they reserve the right to suspend the account or completely reject the application because of this risk.

6. Jurisdiction

156 (72%) of exchanges are located outside high-risk jurisdictions.

In terms of jurisdiction, more than 50% of all examined exchanges are incorporated in medium risk countries, with the United Kingdom, Hong Kong, United States of America, Republic of
Korea and Brazil accounting for the highest numbers of exchanges incorporated.

High-risk incorporations appeared to be concentrated in Turkey, Vanuatu and Thailand. The incorporation details for 36 other exchanges could not be determined from publicly available sources such as Terms of Service. These jurisdictions were noted as high-risk.

In the group of exchanges with unidentified jurisdiction, we have found 7 decentralized exchanges, e.g.: Bisq, Bitshares, DDex, the operation of which was evaluated as high risk in respect to all examined risk categories (except Negative and Adverse Media risk). None of these exchanges appear to have implemented KYC processes.

In the group of low-risk jurisdictions, Singapore was noted as the most popular location with 20 (9%) of the exchanges registering here.

13 exchanges were identified as having registered operations in multiple jurisdictions.

7. Negative and Adverse Media (About the Exchange)

17 (8%) of exchanges were identified as being related to adverse media news.

The following are the examples of exchanges that have adverse media listings:

- FCoin – which is accused of being a financial pyramid
8. Jurisdiction Specific Findings

This section presents a summary of the risk assessment for exchanges registered in selected jurisdictions.

The map below presents in pictorial way the average composite risk performance of exchanges registered in specific jurisdictions.
The tables below show the number of exchanges classified as high/medium/low risk:

### UNITED KINGDOM

<table>
<thead>
<tr>
<th>RISK</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed and Authorised</td>
<td>3</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>Customer Due Dilligence/KYC</td>
<td>7</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>6</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Sanctions</td>
<td>7</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>Senior Public Figures/PEPs</td>
<td>5</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>0</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>9</td>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

### SINGAPORE

<table>
<thead>
<tr>
<th>RISK</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed and Authorised</td>
<td>3</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>Customer Due Dilligence/KYC</td>
<td>4</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>6</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Sanctions</td>
<td>10</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Senior Public Figures/PEPs</td>
<td>7</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>18</td>
<td>2*</td>
<td>0</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>12</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

* Two of the exchanges registered in Singapore (low risk jurisdiction), were identified to be registered also in other -medium risk jurisdictions. Therefore, the Jurisdiction Risk evaluation of these two exchanges is considered medium.
<table>
<thead>
<tr>
<th>RISK</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HONG KONG</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensed and Authorised</td>
<td>1</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>Customer Due Diligence/KYC</td>
<td>2</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Sanctions</td>
<td>6</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Senior Public Figures/PEPs</td>
<td>7</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>0</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>6</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td><strong>UNITED STATES OF AMERICA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensed and Authorised</td>
<td>7</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Customer Due Diligence/KYC</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Sanctions</td>
<td>11</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Senior Public Figures/PEPs</td>
<td>7</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>0</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>JAPAN</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensed and Authorised</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Customer Due Diligence/KYC</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AML Policies and Procedures</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Sanctions</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Senior Public Figures/PEPs</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Negative and Adverse Media</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
glossary

A **Address** – an address is like a bank account and for example a Bitcoin address starts with either a ‘1’ or a ’3’ or a ‘bc1’ and is 26-35 alphanumeric characters in length. The address is generated from the private key, which is required to move assets assigned to this address to another address(es).

**Anti-Money Laundering (AML)** – the process of systems and controls that are applied to deter, disrupt and detect the flow of illicit value between collusive criminals that represents the proceeds of crimes and predicate offences such as tax evasion, sanctions evasion, theft, counterfeiting and fraud.

B **Blockchain** – is a public ledger that records transactions that are performed. This is achieved without any trusted central authority as the maintenance of the blockchain is performed by a network of communicating nodes running the software. Network nodes validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes.

C **Combating the Financing of Terrorism (CFT)** – the process of deterring and disrupting the financing of terrorism and proliferation. It is increasingly difficult to distinguish from money laundering activity due to the collusive conduct of terrorist financiers and transnational organized criminals, but it is typically distinguished from money laundering on the grounds that the sources of money laundering must be criminal, whereas the sources of finance for terrorism include donations from lawfully earning income. The goal of money laundering is typically a financial gain, while the goal of terrorism financing is typically ideological activity.

**Customer Due Diligence (CDD)** – a process to assess all of the risks associated with a client or relationship, including KYC, and that requires that the overall client conduct and transactions are assessed to determine if this is unusual and reportable. CDD requires that obliged entities assess the risks before entering in to a relationship, and continuously thereafter in response to trigger events or suspicious activity for example. It is a continual process that is designed to assess and monitor changes in customer risks.

D **Decentralized Virtual Currencies** - (cryptocurrencies) are distributed, open-source, mathematically-based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include: Bitcoin, Ethereum, Litecoin and Namecoin.

**Distributed Ledger (Shared Ledger)** - ‘Ledgers’, or put simply, records of activity, were historically maintained on paper, more recently these were transferred to bytes on computers, and are now supported by algorithms in blockchains. They are essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically using ‘keys’ and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network.

(Taken from UK Government: ‘Distributed Ledger Technology: beyond block chain’).
Electronic money (e-money) - is an electronic store of monetary value, based on technological mechanism for holding and accessing fiat currency.

Enhanced Customer Due Diligence (EDD) – a higher standard of due diligence, including identity verification and investigation that is required to be performed for those clients and relationships that have been identified as presenting the greatest risk of financial crimes. These risks include among other PEPs, Correspondent Banking, non-face-to-face activities such as virtual currency and private banking.

Exchanger / virtual currency exchange – is a website service, or an entity, engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wire payments, credit cards, and other virtual currencies. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts. Examples include: Bitstamp, GDAX, Kraken, OKCoin and ItBit.

Fiat Currency – is legal tender that is backed by the central government who issued it. Examples are the US Dollar, Japanese Yen and UK Sterling.

‘Fifth’ EU Money Laundering Directive (5MLD) – an amendment to the 4MLD that was agreed in response to the terrorist attacks across Europe in 2015 and 2016. The new law must be transposed by member states by 10th January 2020, and new measures include the requirement for virtual currency exchange services and virtual currency custodian wallet providers to be treated as ‘obliged entities’.

FinTech – refers to new applications, processes, products or business models that are being applied to improve the efficiency and security of financial services.

Fourth EU Money Laundering Directive (4MLD) – European response to the FATF 40 Recommendations from February 2012 and was required to be transposed by EU member states by 26th June 2017.

Hash – A hash value (or simply hash), also called a message digest, is a string of characters generated from a string of digital data, e.g. a pdf file. The hash is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value and it is extremely difficult to reverse to identify the source message.

Know Your Customer (KYC) – the identification and verification of the natural person, legal entity or legal arrangement through identifying information, such as name and address, and the verification of these details to identify fraud, misrepresentation etc.

Money Laundering – a process to disguise the illicit source of value, either by self-laundering or through the placement, layering or integration process, conducted by criminals who ultimately wish to use this value for self-gratification, or to continue to finance their illicit activities.

Money Laundering Reporting Officer (MLRO) – the chief compliance officer responsible for all AML/CFT
activities and responsible for ensuring that an obliged entity is not used by criminal or the financiers of terrorism.

**Nodes** – are computers in the blockchain network which receive new transactions and blocks, validate these transactions and blocks and spread valid transactions and blocks to connected nodes and ignore invalid transactions and blocks. It is generally considered that the more nodes exist in the network, the more secure the is the system.

**Non-Cooperative Countries and Territories (NCCT)** – jurisdictions that are identified as being high risk for money laundering and terrorist financing by FATF.

**Politically Exposed Person (PEP)** – a person of high public office who may be able to influence the misappropriation of public funds whilst in office, or the awarding of public contracts. Include members of government, ruling classes such as Presidents, Royalty, Ministers of the Government and military and judiciary. The families of PEPs, and their close business associates, are also included due to the close affinity and trust that they may enjoy in their relationship, and which may lead to the PEP using these relationships as ‘front’ or ‘informal’ nominees.

**Private Key** – a private key is a cryptographic code that functions as a secret password that allows the user to sign a cryptocurrency transaction and transfer funds to another cryptocurrency address. Using the private key proves ownership of cryptocurrency.

**RegTech** – is the recent innovation provided by companies that use technology to help businesses comply with regulations more efficiently and inexpensively.

**Sanctions** – when applied to financial services, represent a prohibition on providing regulated services to the subject of the sanction, and the requirement to freeze and report any assets that are held to the local jurisdiction sanctions administrator, such as OFAC or HMT.

**Simplified Due Diligence (SDD)** – a lower level of customer due diligence verification that can be performed where there is no, or a lesser, risk of money laundering.

**Trading platforms** – function as marketplaces, bringing together buyers and sellers of virtual currencies by providing them with a platform on which they can offer and bid among themselves. In contrast to exchanges, the trading platforms do not engage in the buying and selling themselves. Some trading platforms give their customers the option of locating potential customers nearby. Examples include LocalBitcoins.com and Mycelium Local Trader.

**Transaction Fee** – is earned by miners when a transaction is completed. The minimum transaction fee required is determined by the “size” (kilobytes) of the transaction data. Most small transactions require a fee of about 0.0001 BTC and transactions with larger fees are given priority to be added to the block, so they are usually confirmed faster than transactions with low fees.
case studies

Throughout the period of significant growth and development in cryptocurrencies, the number of exchanges operating on the market has correspondingly increased. However, some crypto exchanges have been closed their operations due to a number of differing factors and we have noted some of the most notable examples as these offer further insights as to the types of risks that must be managed.

1. **BTC-e** was a Russian based exchange that was established in July 2011. BTC-e was supporting FIAT currencies (USD, EUR and RUB) when it was closed in July 2017 due to the allegations relating to international money laundering, including holding funds originating from the hack of Mt.Gox exchange.

2. **Tokyo GateWay** was established in 2017 in Japan. The exchange allowed BTC, ETH, XRP, ZEC against JPY. GateWay decided to withdraw their application to operate as a recognized exchange under FSA rules and shut down all operations and on March 2018.

3. **EasyCoin** was based in Poland and commenced operations in 2015. EasyCoin allowed trading BTC against PLN. The exchange suspended its operations in April 2018 in connection to the termination of the agreement with the bank that maintained their bank accounts.

4. **CryptoHub** was founded by a Russian developer, specializing in small market cap coins. It was shut down in September 2018 after an alleged hack.

5. **Zebpay**, one of the largest cryptocurrency exchanges in India was closed in September 2018 due to a crypto banking ban imposed by the country’s central bank.

6. On September 2018, the FBI seized the domain of 1Broker, shutting down the platform for allegedly violating money laundering regulations and distributing securities as an unregistered dealer. The SEC alleged that an FBI special agent, acting in an undercover capacity, successfully purchased several security-based swaps on 1Broker’s platform from the U.S., despite not meeting the discretionary investment thresholds required by the federal securities laws.

The cases noted above represent just a small sample of exchanges who ceased trading earlier than was expected, but these demonstrate a range of risks that must also be considered when managing cryptocurrency activities.
These risks can be grouped under headings such as: regulatory risks; risks associated with the conduct of the exchange owners; or to the exchange itself being the victim of a criminal attack such as cybercrime on the assets held on behalf of users; as well to regulatory action.

**disclaimer**

The findings presented in this independent report represent the outcomes from a data collection and examination period conducted from September 2018 to February 2019 and is provided in the utmost good faith. It does not therefore include any subsequent developments after the period of when the data was collected, however Coinfirm may undertake to update these findings going forward and will amend the report accordingly. Please contact for any details.

Coinfirm is not liable for any changes in assumptions and updates to this document in the case of new facts or circumstances occurring after the date of the report.

Any decision taken by the recipient of this report is made solely on their own risk. The liability of Coinfirm is hereby excluded to the fullest extent permitted by the applicable law.

In no event will Coinfirm be liable to the recipients for:

(i) any act or alleged act, or any omission or alleged omission, that does not constitute willful misconduct by Coinfirm, as determined in a final, non-appealable judgment by a court of competent jurisdiction,

(ii) any indirect, special, punitive, incidental, exemplary, expectancy or consequential damages, including lost profits, lost revenues, loss of opportunity or business interruption, whether or not such damages are foreseeable, or

(iii) any third-party claims (whether based in statute, contract, tort or otherwise).

This report should be read in full because any separate analysis of each of its parts can lead to erroneous conclusions.

Employees of Coinfirm involved in preparation of this report are available to clarify any aspects contained therein. Please contact us at report@coinfirm.com
Coinfirm is the global leader in regtech for digital currencies and the blockchain-based financial ecosystem. By providing solutions that fight fraud and allow traditional financial institutions to meet compliance requirements when interacting with online currencies, we bridge the gap between the crypto and fiat currency worlds, enabling new monetary technologies to reach their full potential and contributing to the creation of a seamless, democratic and transparent financial system. We provide anti-money laundering (AML) and know your customer (KYC) services for virtual currencies and blockchain actors - both new ventures financed by ICOs and some of the largest banks in the world. Our proprietary solutions streamline compliance to near-automation. By creating our own token, the AMLT, we’re supporting the creation of a global community of like-minded organizations and individuals who want to protect the ecosystem. Our Trudatum product gives users the ability to register and authenticate any type of data, providing instant, secure online confirmation of the authenticity of documents and other files. Explore more about Coinfirm product and services at www.coinfirm.com