



## Financial Intelligence Consultative Group

### The use of cryptocurrencies for terrorism financing in Southeast Asia

#### A) Caveat

*This document shall be distributed to Financial Intelligence Consultative Group (FICG) members only and is not intended to be released to the public without the consent of all contributing Southeast Asia Counter Terrorism Financing Working Group (SEACTFWG) member Financial Intelligence Units (FIUs).*

#### B) Background

This Southeast Asia Counter Terrorism Financing Working Group (SEACTFWG) project aims to increase the collective knowledge for Financial Intelligence Consultative Group (FICG) members relating to cryptocurrencies/virtual assets<sup>1</sup> in the Southeast Asia region, including Australia and New Zealand. This intelligence report captures the information provided by FICG member FIUs and has been collated to examine the threat of cryptocurrencies being used to finance terrorism activities, if any.

#### C) Executive summary / findings

1. Across Southeast Asia, Australia and New Zealand, there is limited information in suspicious activity reporting to FIUs to indicate terrorist groups are using cryptocurrencies as a primary method to finance their activities.
2. Cryptocurrencies are being used across a number of crime types, in particular money laundering and fraud/scam related activities.
3. As cryptocurrencies increase in use for legitimate activities, criminal exploitation of cryptocurrencies across 'traditional' crime types is likely to also increase.

---

<sup>1</sup> References to cryptocurrency in this report include the term 'virtual asset', 'digital asset', 'virtual currency', 'digital payment token' and 'digital currency'.

4. As the uptake and acceptance of cryptocurrencies continues, this is likely to make them more attractive for, and an increasingly viable alternative in, funding terrorism activities.
5. Bitcoin is the dominant cryptocurrency used for illicit activities likely due to broader acceptance and liquidity. Suspicious activity reporting indicates other cryptocurrencies such as Ethereum, Ripple, Tether and Litecoin are common for financing crime and anonymity enhanced coins are increasingly accepted by darknet marketplaces.
6. The evolving cryptocurrency sector and the broader cryptocurrency ecosystem (including the volatility observed during 2022) is likely to impact the take up and threat of cryptocurrencies being used in terrorism financing in the short term.
7. Where possible, sharing detailed financial indicators will educate financial institutions/reporting entities in identifying terrorism financing activities and improve the quality of suspicious matter reports submitted to FIUs.

## D) Overview

This information report has been developed as part of the Southeast Asia Counter Terrorism Financing Working Group (SEACTFWG) and contains consolidated responses to a survey from the Financial Intelligence Units (FIUs) of Australia, Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, New Zealand, Philippines, Singapore, Thailand and Vietnam.<sup>2</sup> FIUs examined suspicious activity reporting from 2020 to May 2022.

This paper offers a point-in-time overview of the current regulatory environment relating to cryptocurrencies across the region. It captures broad themes of the current likely misuse of cryptocurrencies by criminals, and those seeking to finance terrorism related activities.

---

<sup>2</sup> Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia; Financial Intelligence Unit, Autoriti Monetari Brunei Darussalam (FIU, AMBD), Brunei Darussalam; Cambodia Financial Intelligence Unit (CAFIU), Cambodia; Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), Indonesia; Anti-Money Laundering Intelligence Office (AMLIO), Lao PDR; Unit Perisikan Kewangan Bank Negara Malaysia (UPWBNM), Malaysia; Myanmar Financial Intelligence Unit (MFIU), Myanmar; New Zealand Financial Intelligence Unit (NZFIU), New Zealand; Anti Money Laundering Council (AMLC), Philippines; Suspicious Transaction Reporting Office (STRO) Singapore; Anti-Money Laundering Office (AMLO), Thailand, State Bank of Vietnam (SBV), Vietnam.

## E) Introduction

Cryptocurrency is becoming more widely available and easier to access across Southeast Asia, New Zealand and Australia. Pseudonymous in nature, cryptocurrencies are easily transferable – at speed across international borders and transportable. As such, cryptocurrencies may offer an alternative for terrorist groups to raise funds to finance their activities. In recent years, some terrorist groups have been known to fund terrorist activities using digital currency donations and crowdfunding, where small amounts are received from a large group of individuals.<sup>3</sup>

This paper will provide an overview of current information reported to FICG FIUs relating to:

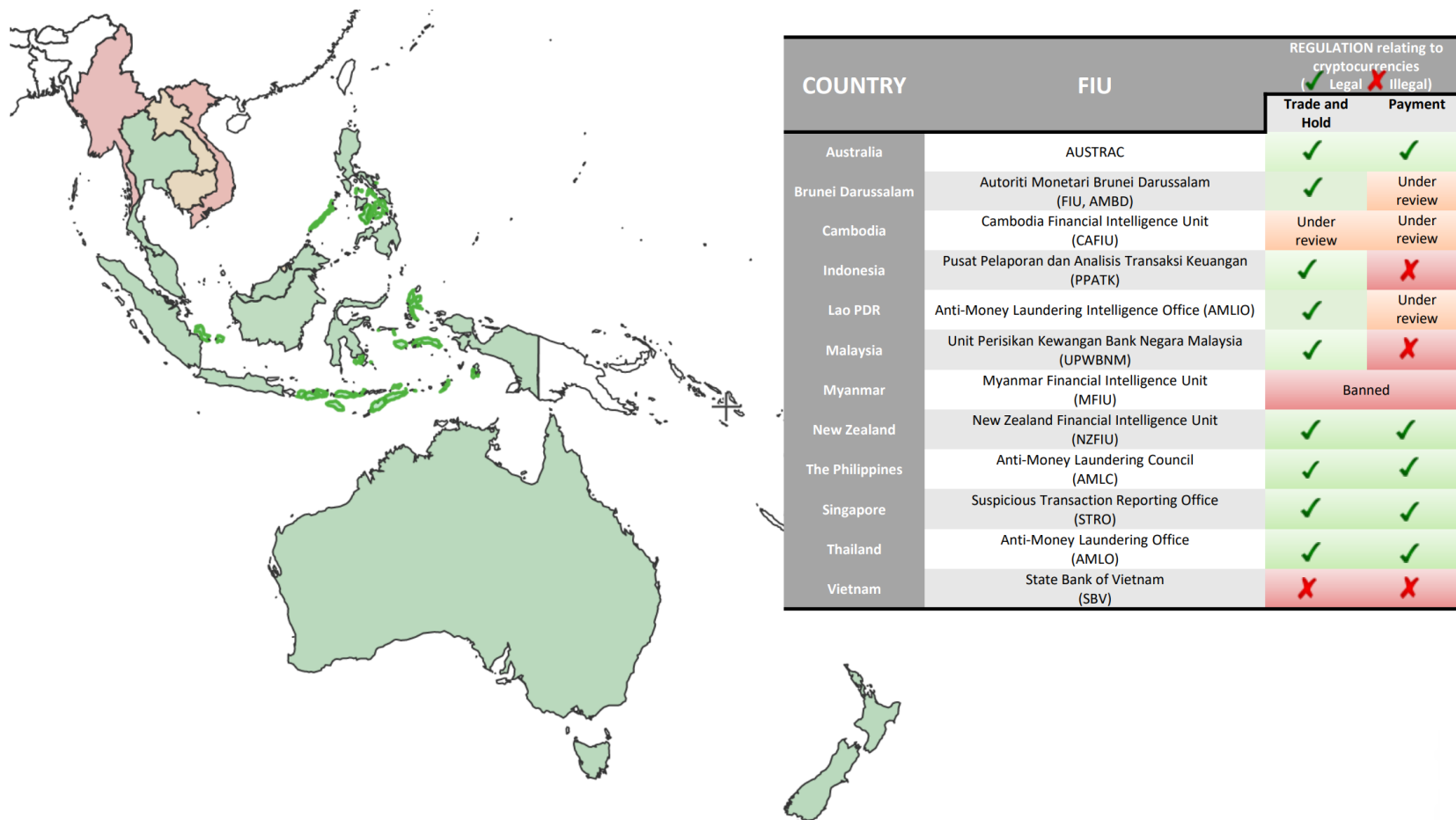
- a) regulatory approaches relating to cryptocurrencies
- b) criminal misuse of cryptocurrencies in suspicious activity reporting and
- c) cryptocurrencies relating to terrorism financing activities in suspicious activity reporting.

---

<sup>3</sup> <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

## Regulatory approaches relating to cryptocurrencies in the Southeast Asia region

Current regulatory approaches relating to cryptocurrencies differ across the Southeast Asia region. A brief snapshot of each country is depicted in Figure 1.



**Figure 1:** Current regulatory approaches relating to cryptocurrencies differ across the Southeast Asia region (as at October 2022).

*(Not for public release – limited distribution – FICG members only)  
October 2022*

## AUSTRALIA

Australia's current legislation<sup>4</sup> uses the term 'digital currency'<sup>5</sup> and digital currency exchange providers (DCEPs). In Australia, DCEPs relate to the businesses who exchange fiat currency for digital currency and vice versa and these have been regulated by AUSTRAC since April 2018. DCEPs must be registered with AUSTRAC before businesses can provide digital currency exchange services<sup>6</sup> and are enrolled with AUSTRAC as part of the registration process. DCEPs are also required to collect relevant Know Your Customer (KYC) information on their users, keep transaction records for seven years, and to report suspicious activity and all cash transactions of AU\$10,000 or more. Further legislative changes are under consideration as part of a future phase of broader AML/CTF reforms.

## BRUNEI DARUSSALAM

The FIU conducted a review of relevant legislations to identify and address gaps which included identifying specific activities that were not covered by existing regulatory framework. To address one of these gaps, Brunei has introduced interim measures to register VASPs that fall outside the scope of existing legislation through the Brunei Darussalam Central Bank (BDCB) FinTech Regulatory Sandbox and issuance of Notice under Section 54(1) of the Brunei Darussalam Central Bank Order 2011 that specifically covers persons operating payment systems.

In addition, Brunei has completed and endorsed a Money Laundering and Terrorism Financing Risk Assessment on Virtual Asset Service Providers in Brunei Darussalam 2021 to assess the overall risk VASPs currently pose to Brunei Darussalam by taking into consideration their inherent risks and vulnerabilities. Further actions are being considered to address and mitigate any risks identified.

## CAMBODIA

Cambodia does not currently provide regulation relating to cryptocurrencies. According to the National Risk Assessment of Cambodia in 2016, the Terrorism and Terrorist Financing risk was assessed as Medium Low. At the time, the national risk assessment did not specifically mention cryptocurrencies. CAFIU has made reporting entities aware of terrorism financing risks and updated them with indicators to report suspicious transactions relating to terrorism financing. CAFIU has not received reporting relating to cryptocurrencies and terrorism financing.

---

<sup>4</sup> <https://www.legislation.gov.au/Details/C2022C00179>

<sup>5</sup> [http://classic.austlii.edu.au/au/legis/cth/consol\\_act/alacfa2006522/s5.html](http://classic.austlii.edu.au/au/legis/cth/consol_act/alacfa2006522/s5.html)

<sup>6</sup> <https://www.austrac.gov.au/business/industry-specific-guidance/digital-currency-exchange-providers>

## INDONESIA

Cryptocurrencies (regulated as 'crypto assets') are treated as commodities and are regulated in Indonesia by the Commodity Futures Trading Regulatory Commission (COFTRA). Cryptocurrencies are not allowed as legal tender or as a payment instrument according to Currency Law in Indonesia.

## LAOS

The government of Laos has issued new regulations governing cryptocurrency mining operations and trading platforms.<sup>7</sup>

## MALAYSIA

The authoritative body that oversees Virtual Assets (VA) and VASPs in complying with the AML/CFT requirements in the onshore jurisdiction is the Securities Commission (SC). Meanwhile, Federal Territory of Labuan (Labuan) is one of Malaysia's federal government territories and for the purpose of this survey, where applicable, we refer to Labuan as 'offshore' while the remaining parts of Malaysia as 'onshore'. The Labuan Financial Services Authority (LFSA) regulates and supervises all reporting institutions subjected to the AML/CFT requirements including VASPs.

*For onshore:*

In January 2019, under the Securities Commission Malaysia (SC)'s regulatory framework, digital assets that fulfil certain conditions are prescribed as securities pursuant to the coming into force of the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019.

The operators of the following activities are required to be registered by the SC and are subjected to the SC's regulatory framework under the relevant guidelines including Guidelines on Recognized Market and the Guidelines on Digital Assets. Digital asset mining activities are not covered under the SC's regulations:

i) Digital Asset Exchange (DAX) - Trading of permitted digital assets such as Bitcoin (BTC), Ether (ETH), Ripple (XRP), Litecoin (LTH) and Bitcoin Cash (BCH) on registered DAXs.

ii) Digital Asset Custodian (DAC) - Safekeeping and/or administration of digital assets or instruments enabling control over digital assets and transfer of digital assets.

iii) Initial Exchange Offering (IEO) platform operators - Participation in and provision of financial services related to an issuer's offer and/or sale of a digital asset.

---

<sup>7</sup> <https://laotiantimes.com/2021/11/15/government-issues-regulations-for-cryptocurrency-miners-and-platforms-in-laos/>

To date, there are four registered DAXs, two IEO platform operators but no registered DACs.

*For offshore:*

LFSA commenced regulating VA and VASPs on 26 June 2018, since the issuance of the Circular on Innovative Financial Services (IFS) in the Labuan International Business and Financial Centre. VASPs are within the context of its current licencing scope. Labuan entities are required to obtain LFSA's prior approval to conduct innovative financial services (IFS) activities that fall within the ambit of Labuan Financial Services and Securities Act 2010 (LFSSA) and Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA). The IFS that can be offered include digital asset activities, robo-advisory services, blockchain or distributed ledger, InsurTech and any other IFS activities.

On 31 March 2022, LFSA published their guidelines on AML/CFT and TFS for Labuan Key Reporting Institutions, requiring Labuan Key Reporting Institutions undertaking digital financial business including dealing with digital assets as Labuan Digital Financial Services (LDFS) to adhere to the requirements under the Guidelines. This document complements the Guidelines on Digital Governance Framework that was issued in 2021.

## **MYANMAR**

Myanmar does not currently allow VASPs and cryptocurrencies.

## **NEW ZEALAND**

In New Zealand, VASPs are considered 'financial institutions' under the AML/CFT Act.<sup>8</sup> There are a number of 'capture points' under the act where VASPs offering specific services are likely to be captured under AML/CFT legislation. These include issuing or managing the means of payment, transferring money or value for, or on behalf of, a customer, accepting deposits from the public, and money or currency changing.

## **The PHILIPPINES**

The Bangko ng Sentral ng Pilipinas (BSP) issued BSP Circular No. 944, Series of 2017, which was later on, amended by Circular No. 1108, Series of 2021 or the Guidelines for Virtual Asset Service Providers (VASP). The regulation and scope of the guidelines apply only to VASPs defined as 'any entity that offers services or engages in activities that provide facility for the transfer or exchange of Virtual Asset (VA), which involve the conduct of one or more of the following activities:

1. Exchange between VAs and fiat currencies;
2. Exchange between on or more forms of VAs;

---

<sup>8</sup> <https://www.legislation.govt.nz/act/public/2009/0035/latest/DLM2140720.html>

3. Transfers of VAs; and
4. Safekeeping and/or administration of VAs or instruments enabling control over VAs.

*BSP's approach in regulating the VASPs involves the following:*

1. Registration – VASPs shall secure a Certificate of Authority to operate as an Money Service Business (MSB), and upon compliance with requirements as specified in the Manual of Regulations for Non-Bank Financial Institutions (MORNBF1).
2. Capitalization – VASP shall have a minimum required capital of Php 10M or minimum of Php 50M (roughly USD180,000 and USD900,000 respectively as of end-July 2022) depending on its provision of safekeeping and/or administration services for VAs.
3. Transactional – for VA transfers amount to Php 50,000 (roughly USD900 as of end-July 2022) or more, or its equivalent in foreign currency, the originating institution in a VA transfer must obtain and hold the required and accurate originator information as well as the required beneficiary information. A VASP shall only transact with duly licensed VASPs and financial institutions. VA transfers are considered as cross-border wire transfers and shall comply with the pertinent wire transfer rules set out by the BSP.
4. Controls – all VASPs shall maintain and have Internal Controls, Technology Risk Management, Consumer Protection measures, Wallet Security and Management, and sound AML practices.
5. Reportorial Requirements – Submission of Audited Financial Statements of the VASPs, Quarterly Report on Total Volume and Value of VCs transacted, and List of operating Offices and websites.
6. Sanctions – Supervisory actions (e.g., monetary penalties, other enforcement actions, etc.) and Revocation of License.

Guidelines in the said regulation are based on leading standards such as FATF recommendations on anti-money laundering and counter-terrorist financing standards, as well as other recognized risk management principles, and shall serve as baseline requirement for VASPs.

AMLC receives STRs from various VASPs<sup>9</sup> and from other financial institutions.

---

<sup>9</sup> <https://www.bsp.gov.ph/Lists/Directories/Attachments/19/VASP.pdf?msclkid=4f531efbd00111ec86e883ada0580486>

## SINGAPORE

The Monetary Authority of Singapore (MAS) introduced the Payment Services Act 2019<sup>10</sup> (PS Act) in January 2020 to regulate Digital Payment Token (DPT) Service Providers in Singapore. These entities provide any service of dealing in DPTs and any service of facilitating the exchange of DPTs<sup>11</sup> in Singapore.

Further amendments to the PS Act<sup>12</sup> were passed in Parliament in January 2021 to expand the scope of DPT service to include transfers of DPTs and provision of custodian wallet services for DPTs. In addition, amendments to the Financial Services and Markets Act<sup>13</sup> were passed in Parliament in April 2022 to regulate all persons in Singapore who conduct a business of providing virtual asset services purely outside Singapore, if they are created in or operate their business from Singapore, primarily to address ML/TF risks.

All DPT Service Providers are required to comply with anti-money laundering and countering the financing of terrorism measures as set out in Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service<sup>14</sup>. In particular, DPT Service Providers are required to comply with customer due diligence, ongoing monitoring, value transfer, record keeping requirements and suspicious transactions reporting under paragraphs 6, 13, 14 and 16 of PSN02 respectively.

## THAILAND

In Thailand, the Emergency Decree on Digital Asset Businesses B.E. 2561 (2018) regulates and oversees the business operations and activities related to digital assets. AMLO continuously coordinates with VASPs and examines transactions conducting report. At this time, AMLO has not received reporting from VASPs that cryptocurrencies/virtual assets have been used by terrorist groups or used for the purposes of financing terrorism in Thailand.

Assets detected by financial investigations or reporting from Reporting Entities are not qualified as virtual assets according to definition under the law (Emergency Decree in Digital Asset Businesses B.E. 2561 (2018)).

---

<sup>10</sup> <https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220>

<sup>11</sup> Please refer to the Paragraph 3 of the First Schedule to the PS Act for the definition of DPT service.

<sup>12</sup> <https://www.mas.gov.sg/news/speeches/2021/payment-services-amendment-bill>

<sup>13</sup> <https://www.mas.gov.sg/news/speeches/2022/financial-services-and-markets-bill-second-reading-speech-on-4-april-2022>

<sup>14</sup> <https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service>

## VIETNAM

VASPs are currently not regulated or supervised in Vietnam. In October 2017, the State Bank of Vietnam (SBV) banned the use of virtual currencies for payment, and the State Securities Commission (SSC) banned publicly-listed companies, and securities and fund management companies from issuing, transacting or brokering in cryptocurrencies. However, open source searches indicate significant cryptocurrency investment and mining in Vietnam, which do not necessarily breach either of these prohibitions. VA and VASPs are not regulated for AML/CFT purposes in Vietnam.<sup>15</sup>

---

<sup>15</sup> Para 21. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/APG-Mutual-Evaluation-Report-Vietnam-2022.pdf>

## Criminal misuse of cryptocurrencies in suspicious activity reporting

Suspicious activity reporting<sup>16</sup> notes cryptocurrencies are being used across the following crimes themes:

**Money laundering** - the abuse of cryptocurrencies in money laundering matters and movement of proceeds of crime (crypto laundering). Bitcoin is by far the most commonly use cryptocurrency, with some FIUs noting criminals also use other coins such as Ethereum and Tether.

**Fraud, theft and scam activity** - scams commonly involve people who have little knowledge of cryptocurrency are targeted. Reporting also reflects the recruitment of 'money mules' (knowingly or unknowingly) under guises of employment (job scams) or romantic interest (romance scams).

**Ransomware payments** - Bitcoin is the common payment method sought by criminal actors connected to ransomware activities.

**Darknet Markets** – payments (ranging in values) to notable Darknet marketplaces and fraud shops as well as larger Darknet vendors attempting to cash out funds.

---

<sup>16</sup> PPATK, NZFIU, STRO, BNM and AUSTRAC.

## Cryptocurrencies relating to terrorism financing activities in suspicious activity reporting

A small number of suspicious matter reports have been received by FIUs where cryptocurrencies are related to terrorism financing. Reporting has included both religiously motivated groups like Al Qaeda and ideologically motivated groups (such as extreme right-wing violent extremist groups). Where financial institutions report suspicions relating to cryptocurrencies and terrorism financing activities, FIUs share these reports with domestic law enforcement agencies and international partners. A snapshot of these matters are included below:

### *Snapshot 1:*

AMLC received a report from a VASP that disclosed that an account holder had cashed in funds through a Money Service Business (MSB) and converted them to BTC. These funds were then sent to an unlabelled wallet address. Further analysis on the blockchain platform reveals that the BTC from the said wallet address was eventually forwarded to another wallet address associated with BTC transfer/bitcoin transfers which has links/associated with terrorist organization. This matter has been referred to domestic law enforcement and international counterparts.

### *Snapshot 2:*

#### *Al-Qaeda/associated terrorist groups soliciting cryptocurrency donations*

Al-Qaeda and other associated terrorist groups have used social media including Telegram and Twitter to solicit bitcoin donations.

The Abu Ahmed Foundation and Al Sadaqah used Telegram, WhatsApp and Twitter to encourage supporters to donate to Bitcoin address 15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf (and other cryptocurrencies) to purchase uniforms for Mujahideen in Syria (reflected in Figure 2 below).

Between 1 November 2017 and 5 November 2020, bitcoin address 15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf transacted 23 times on the Bitcoin blockchain. It has received a total of 0.09036343 BTC (US\$1,942.69) and has sent a total of 0.08945595 BTC (US\$1,923.18). The current value of this address is 0.00090748 BTC (US\$19.51).<sup>17</sup>

<sup>17</sup> <https://www.blockchain.com/btc/address/15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf>



Figure 2: Social media screen captures - AAF and Al Sadaqah seeking donation via cryptocurrencies

### Snapshot 3:

#### IMVE entities - use of cryptocurrencies

The pseudo-anonymous nature of cryptocurrencies is likely to appeal to ideologically motivated violent extremism (IMVE) entities. Open source research reflects IMVE related content use across different funding platforms, including online monetisation tools and cryptocurrencies, to solicit, process and earn funds.<sup>18</sup>

AUSTRAC has analysed holdings relating to IMVE use of cryptocurrencies and shared information with various law enforcement and international partners.

<sup>18</sup> <https://www.aspi.org.au/report/buying-and-selling-extremism>