



Operational Intelligence Report

Criminal usage of Bitcoin

Latest date of information: **XX Month YYYY**

Key judgements

1. The purpose of the key judgements is to draw the reader's attention to the main points/arguments of the brief. (Classification) (DLM)
2. The purpose of the key judgements is to draw the reader's attention to the main points/arguments of the brief. (Classification) (DLM)
3. The purpose of the key judgements is to draw the reader's attention to the main points/arguments of the brief. (Classification) (DLM)

Released under the FOIA Act
28 March 2017

AUSTRAC [Insert incident number without brackets]

Page 1 of 8

This information has been disseminated pursuant to Part 11 of the [Anti-Money Laundering and Counter-Terrorism Financing Act 2006](#) (AML/CTF Act). Information disseminated may only be used in accordance with the provisions of the Memorandum of Understanding between your agency and AUSTRAC. It should be noted that an officer who receives AUSTRAC information shall not divulge or communicate this information except as provided by Part 11 of the AML/CTF Act. In particular, the information detailed in a Suspicious Matter Report (SMR) or Suspect Transaction Report (SUSTR) is inadmissible as evidence in legal proceedings, except where permitted under section 124 of the AML/CTF Act and subsection 16(5D) of the [Financial Transaction Reports Act 1988](#) (FTR Act).

Background

What is Bitcoin and how does it work?

1. Bitcoin is a digital peer-to-peer currency traded online. Transactions are facilitated and verified by the network of users rather than a central user or operator. Bitcoins can be exchanged for mainstream fiat currency, other digital currency or goods and services. (U)
2. Bitcoin is backed by cryptographic algorithms rather than a physical substance like gold, other precious metal or mainstream currency. Purchased Bitcoins are stored in a virtual 'wallet' that can be web-based or stored locally. All transactions are publically broadcast to the network via the 'blockchain' or ledger but remain anonymous. Bitcoins are transferred between owners without the need for an intermediary to ensure any particular transaction is not duplicated. (U)¹
3. Attitudes to Bitcoin - a fork in the road – Bitcoin infighting between those who want to increase the block size and those that don't.

The regulatory landscape

4. At present, only virtual currency backed directly or indirectly by precious metal or bullion is covered by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). Bitcoin and other virtual currency exchangers operate openly in Australia, but are not regulated. They are not subject to Australia's AML/CTF regime because they do not provide a designated service under the AML/CTF Act.²

Historical success stories

5. Bitcoin has successfully been used as the platform for fundraising by high profile self-proclaimed whistle blower group Wikileaks and hacktivist group Anonymous. However, Bitcoin is perhaps most infamous for its role as the financial platform for Silk Road, the online market place for illegal goods such as drugs, fake identification, fireworks and hacking software. Media reporting suggests that at its peak, prior to the shutdown of its website by the FBI in October 2013, Silk Road had more than 900,000 registered users.
6. Yet Bitcoin is also vulnerable to money laundering as a result of the mechanisms through which it operates on such as:
 - The ability to open a bitcoin wallet (or account) and transfer value with no customer due diligence or identification.
 - The ability to disguise movement of value by changing it into different types of mainstream currency.
 - Poor visibility of transaction history
 - Movement of large amounts of funds between individuals and accounts offshore without limits on value

Criminals accepting payment for Bitcoins for illicit goods and services do not need to place physical cash within the financial system. This step is bypassed by accepting bitcoins directly instead of cash. subsection 37(2)(b)

¹ Bitcoin: overview, AML regulation and vulnerabilities May 2014 - Unclassified

² Bitcoin: overview, AML regulation and vulnerabilities May 2014 - Unclassified

subsection 37(2)(b)

What normal looks like when buying and selling bitcoin in Australia.

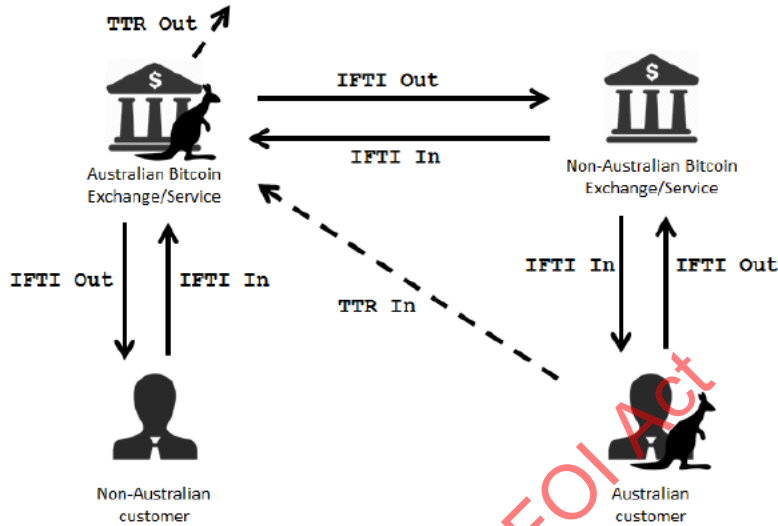


Figure 1: Bitcoin transactional model

Use of Bitcoin for legitimate business is limited in Australia. Bitcoins can be used either directly or indirectly to purchase or transfer value: Directly via direct transfer of Bitcoins to a merchant; indirectly by converting Bitcoins to mainstream currency through an intermediary.

subsection 37(2)(b)

Methodologies used for criminal and terrorist exploitation of Bitcoin

7. Criminals have been known to exploit bitcoin to extract ransom payments from victims of cyber-hacking.

What are we seeing in the data?

8. If the report contains tables or figures, then they should be referenced in the text (table 1). Or introduce the details as shown in figure 1. (Classification) (DLM)

Bitcoin and links to terrorism

9. Bitcoin is an ideal alternate payment method for terrorist organisations seeking to move funds covertly and independently of the formal financial sector.

10. para graph 33(a)(iii) and subsection 33(b)

³ subsection 37(2)(b)

⁴ subsection 37(2)(b)

⁵ para graph 33(a)(iii) and subsection 33(b)

**SECURITY CLASSIFICATION – Delete if not PROTECTED
Sensitive or [other DLM]**

11. Those aligned with Islamist extremist movements such as ISIL have acknowledged and spruiked the potential for Bitcoin to act as a platform for donations to ISIL. On 28 August 2015, Ali Shukri Amin was sentenced to 11 years in prison to be followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to the ISIL subsection 37(2)(b)

12. Amin admitted to using Twitter to provide advice and encouragement to ISIL and its supporters. He tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilise this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system to send money, using bitcoin, to the mujahedeen⁶.

13. The likelihood however that Bitcoin or other virtual currencies could become the preferred financial platform for terrorist organisations, as it was for Silk Road, remains unlikely for now. The complexities in the transactional model serve as a significant impediment to such a transition.

Implications and recommendations

14. Briefly conclude by outlining implications and recommendations that can be drawn from your judgements/assessments. Conclusions should be brief and clear. Each numbered paragraph should contain one statement. (Classification) (DLM)

15. Text (Classification) (DLM)

Intelligence gaps

16. Include key intelligence gaps. If none exist, delete this section. (Classification) (DLM)

Appendixes (Remove heading if none exist)

- A. Transactions in May 2015 [Example]
- B. Money flows to Country X in June 2015 [Example]

Attachments (Remove heading if none exist)

- 1. Disclosure from XXXX FIU – Party Y [Example]
- 2. SMRs relating to Party Z [Example]

Dissemination list

- Insert agency 1
- Insert agency 2
- Insert agency 3

⁶ <https://www.coe.int/t/dghl/monitoring/moneyval/Publications/Emerging-Terrorist-Financing-Risks.pdf>

**SECURITY CLASSIFICATION – Delete if not PROTECTED
Sensitive or [other DLM]**

Additional information

For additional information on any information contained within this report please contact the AUSTRAC Operational Intelligence Team via operational_intelligence@austrac.gov.au.

A glossary and list of commonly used abbreviations within AUSTRAC reports can be accessed at <http://www.austrac.gov.au/book/export/html/205>.

Feedback

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any positive outcomes associated with this report by contacting AUSTRAC via operational_intelligence@austrac.gov.au or through AUSTRAC *Intelligence*.

Released under the FOI Act
28 March 2017

**SECURITY CLASSIFICATION – Delete if not PROTECTED
Sensitive or [other DLM]**

Security procedures

This report has been protectively marked in accordance with the Australian Government security classification system, which supports the information security core policy and information security management protocol within the Protective Security Policy Framework (PSPF).

The information has been assessed as requiring increased security to protect its confidentiality. To reduce the risk of unauthorised disclosure, agencies should take all reasonable and appropriate precautions to ensure that only people with a proven need-to-know and the correct security clearance gain access to this information.

Protectively marked sensitive and security classified information requires special handling and should be stored in physical and electronic environments that provide a fitting level of protective security. This also applies to the removal, transfer, receipt, and disposal of the information.

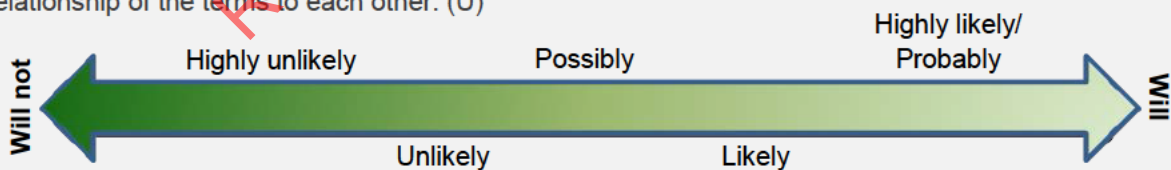
Agencies should refer to the Australian Government information security management guidelines, protectively marking and handling sensitive and security classified information.

Copying

This document remains the property of the Australian Transaction Reports and Analysis Centre (AUSTRAC) and may not be used or further copied, disseminated or otherwise made available outside of your agency except as agreed by AUSTRAC.

Estimative language

Certain words are used in this assessment to convey confidence and analytical judgement regarding the probability of a development or event occurring. Judgements are often based on incomplete or fragmentary information and are not fact, proof or knowledge. The figure below describes the relationship of the terms to each other. (U)



**SECURITY CLASSIFICATION – Delete if not PROTECTED
Sensitive or [other DLM]**

Appendix A - Transactions in May 2015 (EXAMPLE)

1. Paragraph numbers recommence with each new appendix. Include classification marker and/or DLM at end of each paragraph. (Classification) (DLM)

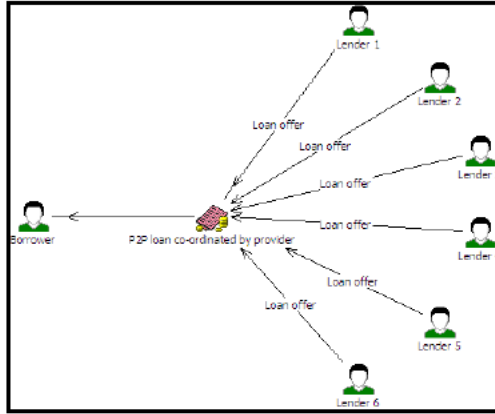


Figure A1: Captions - make them brief and descriptive (Classification) (DLM)

Text	Text	Text

Table A1: Captions - make them brief and descriptive (Classification) (DLM)

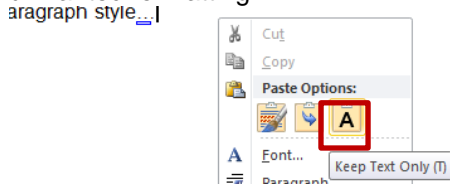
Released under the FOIA Act
28 March 2017

**SECURITY CLASSIFICATION – Delete if not PROTECTED
Sensitive or [other DLM]**

How to use this template

To use this template correctly please follow these simple steps:

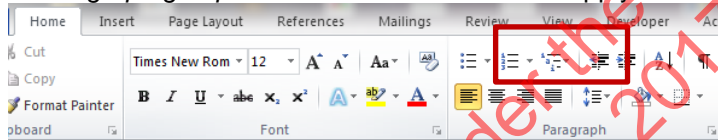
1. **Use 'Paste text only' method.** If you are copying and pasting content from another document into this clean template, use the *Copy > Right-click > select **Paste text only*** method to remove unwanted formatting:



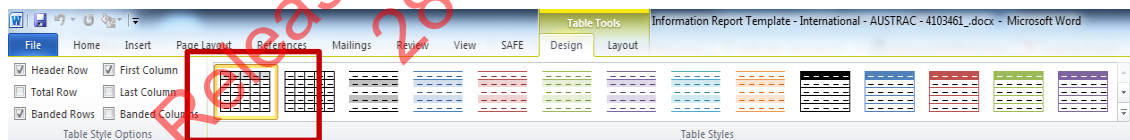
2. **Use built-in paragraph and heading styles to format your document.** To access the styles go to the *Home tab > Styles group* and select the appropriate style. Please note that the *Numbered paragraph style* should be used for the body text and the *Heading 1 style* should be used for the paragraph headings.



3. **Use built-in list function to create lists.** To create a bullet or numbered list, go the *Home tab > Paragraph group* and use the list functions to apply to text.



4. **Use built-in table styles.** Word 2010 has a large selection of built-in table styles that can be accessed by placing your cursor in the table > selecting the **Table Tools** tab > selecting a style from the **Table Styles** list. Please select the Intel table style to maintain consistency across documents.



5. **Use built-in break out boxes** for highlighting information and inserting case studies. To access the break out box go to the *Home tab > Styles group* and select *Styles window (or Alt-Ctrl-Shift-s.)* Highlight your text and select *Block Text* from the *Styles window*.