Australian Government
AUSTRAC

Fintel Alliance

PREVENTING THE

CRIMINAL ABUSE OF DIGITAL CURRENCIES

FINANCIAL CRIME GUIDE APRIL 2022

COPYRIGHT

ATTRIBUTION

ACKNOWLEDGMENTS

This financial crime guide was developed by the Fintel Alliance, a public-private partnership led by AUSTRAC.

Thank you to all of our partners who contributed to this financial crime guide.

CONTENTS

HOW TO USE THIS FINANCIAL CRIME GUIDE

This financial crime guide has been developed to assist financial service providers, including **digital currency exchange (DCE) providers**, to understand and identify criminal activity facilitated through digital currencies and to report suspicious financial activity. The indicators and behaviours in this financial crime guide can be used by financial service providers to review their profiling and transaction monitoring programs. This will assist to identify, target and disrupt transactions associated with financial crime and money laundering using digital currencies.

Financial service providers should use the indicators in this guide and their own business knowledge to conduct further monitoring and identify if a suspicious matter report (SMR) needs to be submitted to AUSTRAC.

Intelligence and information shared by financial service providers is critical in helping AUSTRAC and our government partners identify and dismantle criminal networks moving the proceeds of crime through digital currencies.

SUSPICIOUS MATTER REPORTING

If you identify possible criminal abuse of digital currencies through financial transactions and determine you need to submit an SMR; include clear behavioural and financial indicators in your report. This will help AUSTRAC and our law enforcement partners respond and take action.

DE-BANKING

AUSTRAC discourages financial institutions from indiscriminate and widespread closure of accounts across entire sectors.

De-banking legitimate and lawful businesses can negatively impact individuals and businesses. It can also increase the risks of money laundering and terrorism financing and negatively impacts Australia's economy.

ABOUT FINANCIAL CRIME GUIDES

Financial crime guides provide information about the financial aspects of different crime types. They include case studies and indicators that can be used to identify if offending could be occurring. They are developed in partnership with AUSTRAC's Fintel Alliance members, relevant government agencies, and industry partners.

The Fintel Alliance also consulted with DCE providers to develop this financial crime guide.

ABOUT THE FINTEL ALLIANCE

The Fintel Alliance is a public-private partnership led by AUSTRAC that brings together government, law enforcement, private sector and academic organisations who work together to:

- support law enforcement investigations into serious crime and national security matters
- increase the resilience of the financial sector to prevent criminal exploitation
- protect the community from criminal exploitation.

The Fintel Alliance partners include businesses from the financial services, remittance and gaming industries as well as law enforcement and security agencies in Australia and overseas.

IMPORTANCE OF PARTNERSHIPS

Public-private partnerships are an effective way to identify, target and disrupt criminal activities using digital currencies.

The Fintel Alliance partners recognise the risk of uptake of digital currency for activities such as money laundering and terrorism financing and use the public-private partnership to identify, target and disrupt this offending to protect businesses and the Australian community.

INTRODUCTION

Digital currencies and **distributed ledger technology** (such as blockchain) enable digital transactions and the delivery of financial products and services in new online networks, environments and marketplaces. Digital currencies have seen a significant increase in value and acceptance over the last five years, with Australians rapidly taking up this new technology. As confidence in the security, traceability and speed of distributed ledger technology increases, it has the potential to create efficiencies across various sectors including payments, logistics and healthcare.

Unfortunately, organised criminal groups and individual offenders may also take advantage of these efficiencies to conduct criminal activities and attempt to evade law enforcement detection. The pseudo-anonymous and borderless nature of digital currencies presents a risk for the facilitation of serious crimes, including:

- money laundering
- the purchase and sale of illicit products via darknet market places
- terrorism financing
- scams
- tax evasion
- ransomware.

The increased use of digital currencies for various financial activities has created opportunities for criminals to operate outside of the traditional financial sector. However, the public nature of most digital currency transaction data creates opportunities to identify, target and disrupt criminal activities using digital currencies.

WHAT IS DIGITAL CURRENCY?

Digital currency is a digital representation of value that functions as a medium of exchange and a store of economic value.

Digital currencies can be traded or transferred with other digital or government issued currencies, and can be used for the payment of goods and services or for investment purposes.

References to digital currency in this financial crime guide includes 'crypto', 'cryptocurrency' and 'virtual assets'.

FINANCIAL CRIME THROUGH DIGITAL CURRENCIES

MONEY LAUNDERING

Money laundering through digital currencies is the process of concealing the origins of illegally obtained digital currency or government issued currency, also referred to as fiat. Criminals obscure the owner and source of the funds by passing them through a sequence of digital currency transactions and services. This process involves three stages including placement, layering and integration.

THE METHOD

STAGE 1: PLACEMENT

Placement occurs when the illicit proceeds in government issued currency (e.g. Australian dollars) are converted into digital currency or vice versa. Conversion between government issued currency and digital currency can be done in several ways, each of which will require differing amounts of identity information.

Customers may purchase digital currency through established DCE providers. In Australia, if the DCE providers exchange government issued currency for digital currency or vice versa, they are required to register with AUSTRAC and meet their anti-money laundering and counter-terrorism financing (AML/CTF) obligations, including identifying and verifying their customers.

The conversion to and from government issued currency is the point where a criminal is most exposed and identifiable.

STAGE 2: LAYERING

Layering involves the movement or conversion of illicit funds, either digital or government issued, across different digital currencies, accounts or institutions to distance the funds from their source. Once digital currency is held, it can be layered through various exchanges including digital currency-only and decentralised exchanges.

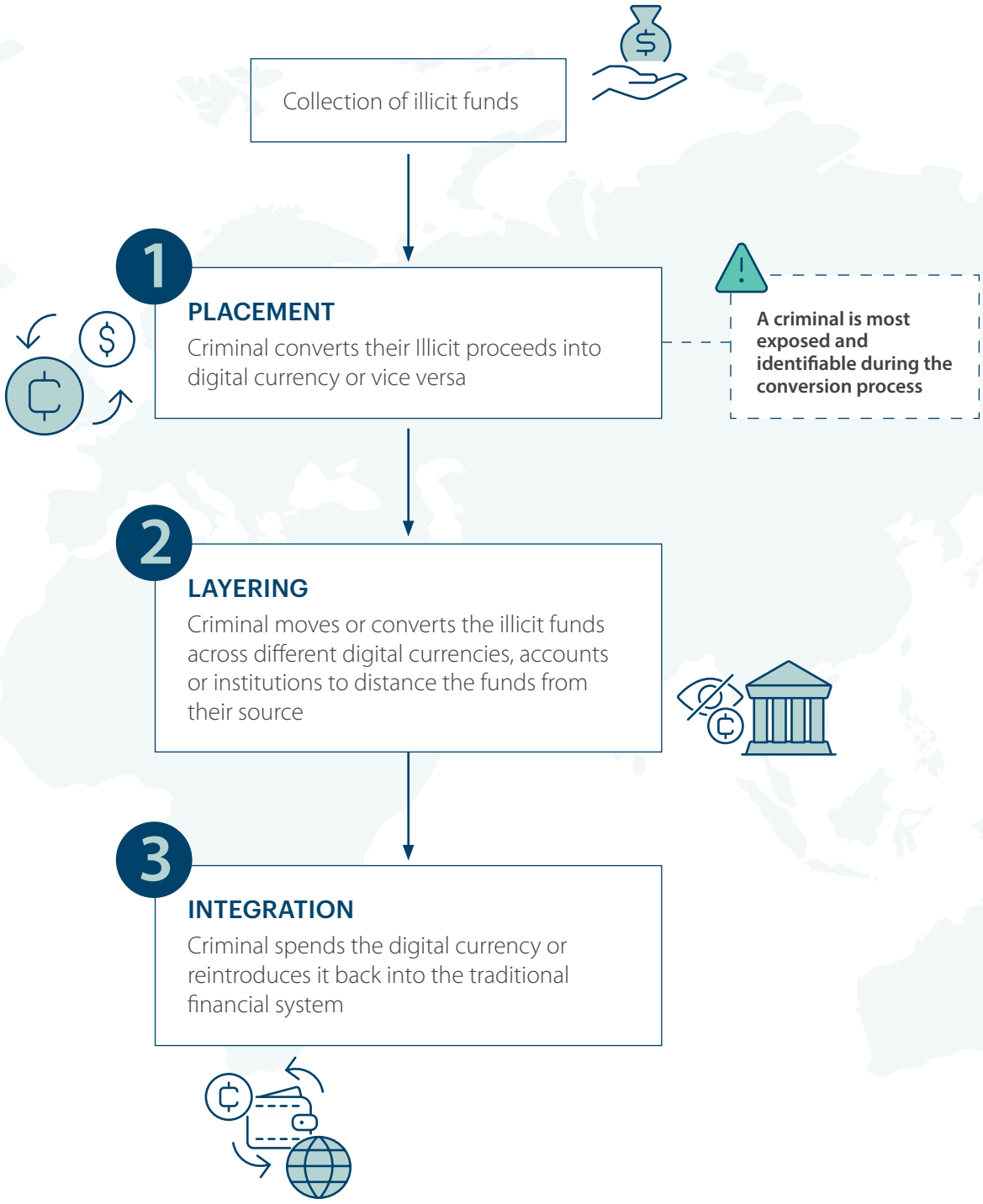
Criminals can take advantage of conversion services, such as **mixers**, decentralised finance, or **privacy coins** to increase their anonymity and make tracing the movement of funds more difficult.

Although conversion services and privacy coins operate outside of the traditional banking sector, blockchain analysis tools can be used to identify digital currency addresses connected to conversion services, creating an opportunity for financial service providers to identify transactions coming from or going to these services.

STAGE 3: INTEGRATION

Integration is the final stage of the money laundering cycle where the digital currency is either used for the purchase of goods and services or reintroduced into the traditional financial system. By this point, the criminal's objective is to have the funds sufficiently distanced from their illicit source with the intention of avoiding law enforcement detection.

EXAMPLE OF THE MONEY LAUNDERING METHOD USING DIGITAL CURRENCY



PURCHASE AND SALE OF ILLICIT PRODUCTS VIA DARKNET MARKETPLACES

The darknet is a hidden collective of internet sites that are not indexed by search engines and are only accessible via specialised software. The darknet includes marketplaces for the purchase of illicit goods and services, activists' networks, anonymous information databases for journalists, political chat rooms, artist platforms, as well as portals to anonymous whistleblowing networks.

Digital currency can be exploited by those seeking a decentralised, pseudo-anonymous and accessible financial path to obtain illicit products and services through darknet marketplaces.

TERRORISM FINANCING

Some terrorist groups have been known to fund terrorist activity using digital currency donations and crowdfunding, where small amounts are received from a large group of individuals.
The financing of terrorism may involve digital currency purchased with legitimate funds which are then utilised for funding of acts of terrorism.

CASE STUDY: TERRORISM FINANCING

In 2019, a number of terrorist groups used social media to request bitcoin donations to finance terrorism campaigns, misleading donors into believing such transactions were anonymous and untraceable. The terrorist groups' websites offered instructions on how to make donations from around the world.

Working together, international law enforcement agencies used the traceability of digital currency to dismantle three terrorist financing cyber-enabled campaigns.
The international agencies seized millions of dollars, 300 digital currency **wallets**, websites and social media pages all related to the terrorist groups.

SCAMS

The rise of public interest in digital currency has also resulted in a significant increase in scams targeting all demographics. In 2021, Scamwatch received over 10,412 reports of digital currency related scams, with losses of over $129.4 million[1]. Digital currencies are being used for a variety of scams including romance, investment, give away and job/employment scams as well as Ponzi schemes.

Scams can also involve individuals being coerced or unknowingly assisting in the movement of the proceeds of crime through digital currencies.

FAKE DIGITAL CURRENCY ENDORSEMENTS

In July 2020, the Australian government warned the public about celebrities unknowingly being used in endorsement scams involving digital currency trading schemes and fake **trading robots**.

Scammers create fake trading robot websites and advertise these through social media using false celebrity endorsements. An individual, trusting the celebrity endorsement, may click on the article or advertisement and be sent to a fake version of a legitimate website where they will be asked to deposit funds using various payment methods. When the individual attempts to withdraw their money the scammers will either cease all contact or demand further payment before the funds are released.

1 Australian Competition and Consumer Commission (ACCC). Number of of digital currency related scams and losses. February 2021.

TAX EVASION

Digital currencies can be used for tax evasion, in particular evading income tax. Individuals may attempt to avoid their tax obligations by not declaring trading in digital currency in their tax returns, making payments in digital currency to avoid GST or shifting value offshore in an attempt to avoid capital gains tax.

In Australia, a capital gains event can occur when a customer exchanges, trades, sells, gifts or converts digital currency.

It is likely that an individual attempting to evade taxation obligations will take advantage of layering through conversion services, privacy coins or move digital currency through online gambling platforms.

For more information on taxation of digital currencies, please visit the Australian Taxation Office website.

RANSOMWARE

Ransomware is a type of malicious software or **malware** that can encrypt files and render a victim's computer unusable. Criminals try to infect a computer or network with this malware and then demand a ransom to unlock or decrypt the victim's files. Criminals seek to make it as easy as possible for victims to pay. Payment is sometimes demanded in popular digital currencies due to their wide availability.

For more information, including ransomware financial indicators read the Detecting and reporting ransomware financial crime guide.

GENERAL CUSTOMER BEHAVIOUR AND FINANCIAL INDICATORS

The behavioural and financial indicators in this guide can be used to review profiling and transaction monitoring programs to target, detect and disrupt transactions associated with financial crime and money laundering through digital currencies.

Each indicator in this guide should trigger enhanced customer due diligence (ECDD).

Financial services providers, including DCE providers, should use a combination of the financial indicators, combined with knowledge of their business to monitor, mitigate and manage suspicious activity.

Where a suspicion is formed, financial service providers, including DCE providers must take steps to reduce any risk and submit an SMR to AUSTRAC.

IDENTIFICATION, VERIFICATION AND PROFILE INFORMATION

BEHAVIOURAL INDICATORS

- Customer is reluctant or declines to provide identification or personal information.
- Customer attempts to provide as little identity information as possible, including incomplete or insufficient identification information.
- Customer provides stolen, forged or fake documentation.
- Customer verification information is a photograph of data on a computer screen rather than the original document.
- Company beneficial ownership is difficult to establish.
- Customer provides documentation with identifiable alterations or of a low quality during on-boarding or when conducting ECDD.
- Customer on-boarding documentation is unable to be verified or does not match the details of the account.
- Customer acts on behalf of someone else (without disclosing the fact) or impersonates someone else.
- Customer appears to be using a **virtual private network (VPN)** or encrypted email in an attempt to hide their identity.
- Customer is known to law enforcement, via publicly available information.
- Customer frequently changes their identification information, including email addresses, internet protocol (IP) addresses, or financial information.
- Customer is difficult to contact, responds only via email or web chat, and at unusual hours.
- Customer uses a mail account provider known for high privacy features.
- Law enforcement or regulator interaction indicates that a customer is linked to illicit activity.
- Customer has adverse media or open source reports.

SOURCE OF FUNDS AND WEALTH

FINANCIAL INDICATORS

- Customer has unexplained wealth or the source of their funds does not match their profile.
- Customer purchases large amounts of digital currency not substantiated by available wealth or consistent with their profile.
- **Structuring** (or perceived structuring) of government issued currency deposits or digital currency withdrawals via **cryptocurrency ATMs** or retail locations.

BEHAVIOURAL INDICATORS

- Customer provides inconsistent explanations as to the source of funds or source of wealth that are used for the purchase of digital currencies.
- Customer provides documents that appear to have been altered or of low quality during on-boarding or when conducting ECDD processes.
- Customer requests higher limits inconsistent with their occupation or profile.
- Customer is reluctant or declines to provide source of funds or wealth.

ACCOUNT ACTIVITY

FINANCIAL INDICATORS

- Use of **chain-hopping** in an apparent attempt to obfuscate source or destination of funds.
- Multiple customers send funds to the same external wallet address (that is not a service).
- Publicly available information such as sanctions lists or analytical tools indicate a customer's wallets, or wallets the customer is transacting with, are associated or linked to illicit activity.
- Unusual transactions such as customer moving earnings through mixers, multiple conversions or layering through multiple exchanges prior to cashing out.
- Customers that regularly make significant profits or losses by transacting with the same subset of wallet addresses.

BEHAVIOURAL INDICATORS

- Multiple customer accounts are opened with either the same email address, phone number, IP address, residential address, postal address or on-boarding documents.
- Customer accesses their accounts from a high number of different electronic devices or IP addresses.
- Customer lacks knowledge or provides inaccurate information about the transaction, the source of funds, or the wallet address where they want to send the digital currency.
- Customer seems anxious or impatient with the time taken to make a large transaction.
- Customer is evasive as to the reason for the transfer.
- Customer wants to increase transaction limits shortly after opening an account.
- Customer creates or attempts to create separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed.
- Customer attempts to coerce or persuade staff to ignore reporting obligations or break normal protocol to conduct a transaction.
- Customer consistently conducts transactions under actual or perceived reporting thresholds.
- Customer gambles with digital currency or has transactions to/from gambling websites.
- Customer uses privacy enhanced digital currencies which do not appear to be used for investment purposes.
- Customer IP addresses do not match the state or country the customer resides in.

Some of the general indicators can also be indicative of money laundering through digital currencies.

CRIME TYPE SPECIFIC INDICATORS

ILLICIT ACTIVITY VIA DARKNET MARKETPLACES

FINANCIAL INDICATORS

- Blockchain analysis tools link a customer's transactions to darknet **clusters**, child exploitation clusters, mixers or high risk exchanges.
- Customer's wallet addresses show exposure to high-risk conversion services or darknet marketplaces.
- Use of, or donations to darknet explorers, including a platform enabling anonymised internet access indicating access to, and possible illicit purchases on the darknet marketplaces.

TERRORISM FINANCING

FINANCIAL INDICATORS

- Public information or blockchain analysis tools indicate a customer has transacted with websites or wallet addresses considered to be high risk for terrorism activities or proliferation financing.
- Transactions with sanctioned wallet addresses or people of interest listed on government websites, such as the Office of Foreign Assets Control (OFAC) or the Department of Foreign Affairs and Trade (DFAT).
- Transactions to crowdfunding or online fundraising campaigns linked to ideologically or religiously motivated violent extremism focused forums.
- Transfers to/from international exchanges with less stringent 'know your customer' processes, including those owned or hosted in high risk jurisdictions[2].
- Customer account receives multiple small deposits, which are immediately transferred to private wallets.

BEHAVIOURAL INDICATORS

- Social media (or online profiles/handles) indicate the customer holds ideologically or religiously motivated violent extremism ideologies or sympathies.

2 fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/

SCAMS

FINANCIAL INDICATORS

- IP address is linked to a high risk scam location.
- Customer receives government issued currency from bank accounts in a different name.

BEHAVIOURAL INDICATORS

- Customer does not fit the usual profile of a digital currency trader/investor, for example, a vulnerable customer or someone with limited knowledge of digital currency.
- An elderly or financially vulnerable customer engaging in high-volume digital currency transactions.
- Customer advises they are using their digital currency to participate in an investment opportunity.
- Customer shows little knowledge regarding digital currency during on-boarding but purchases digital currency quickly and sends the funds to another digital currency address.
- When engaging with a customer they sound coached when answering personal and on-boarding questions.
- Customer advises they are employed to purchase digital currency on-behalf of another individual or company.
- Customer advises they are sending funds to a friend or family in a high risk jurisdiction.

TAX EVASION

FINANCIAL INDICATORS

- Use of services that do not make commercial or economic sense. For example, a business moving earnings through mixers or an individual converting a digital currency multiple times prior to cashing out, incurring additional conversion fees.

BEHAVIOURAL INDICATORS

- Customer makes enquires about avoiding tax reporting obligations.
- Customer asks if personal or transaction information will be shared with the Australian Taxation Office.
- Customer requests to hide or delete transaction activity held.
- Customer sends or receives government issued currency to a wide range of related personal or business accounts at different institutions.

EMERGING FINANCIAL CRIME RISKS

NON-FUNGIBLE TOKENS

In 2021, creating and investing in non-fungible tokens, commonly referred to as NFTs, increased significantly. Unlike other **fungible** or interchangeable assets, such as government issued currency or digital currency, NFTs are blockchain-based digital assets that are designed to be one of a kind, making each asset non-interchangeable. Examples of NFTs include collectables as well as the representation of rights related to real-world items such as artwork.

As NFTs can be created by anyone, they present emerging risks which may enable criminal activity. For example, the value of NFTs are subjective so they can be purchased and sold for any value. This allows for criminal activities such as the laundering of funds which may have come from illicit activities.

DECENTRALISED FINANCE

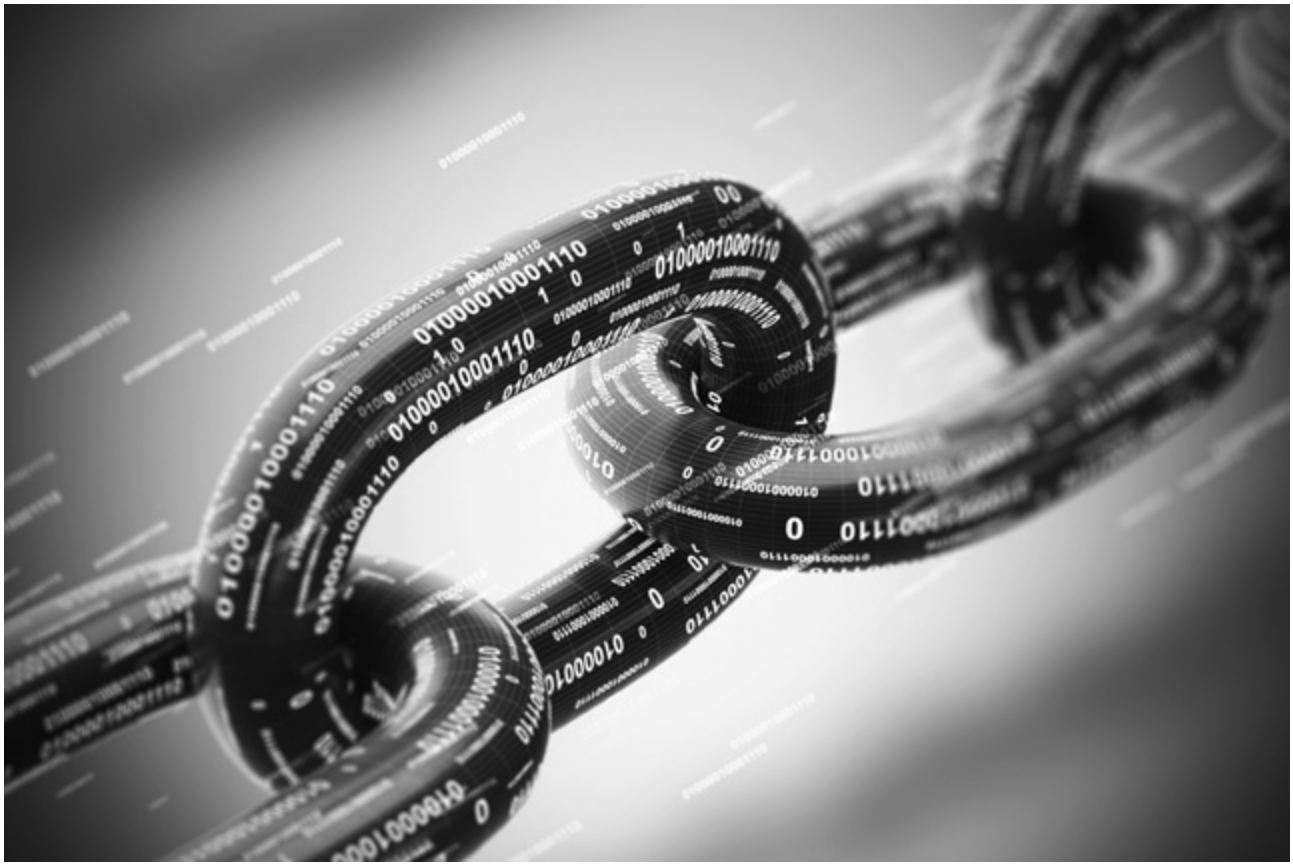
Decentralised finance, commonly known as DeFi, is an application or protocol operating via distributed ledger technology that facilitates financial activities (such as trading, loans and investments). It does not rely on intermediaries such as brokerages, DCE providers or banks. Instead, decentralised finance uses **smart contracts**.

DeFi uptake has surged over 2021, which has led to opportunities for it to be used for criminal activities, such as money laundering.

STAKING

Staking digital currency is the process of committing digital currency to support a blockchain network to verify transactions or to participate in decentralised finance protocols. Staking enables an individual to earn more digital currency over time, either as a result of network fees paid by users of the digital currency or by earning rewards, similar to a term deposit or bank account which earns interest.

Staking can be used by individuals in a completely decentralised manner to legitimately invest and earn profits from their digital currency. Criminals may seek to exploit this method to earn 'clean' digital currency while staking illicit digital currency.



PREVENTING THE FACILITATION OF CRIME THROUGH DIGITAL CURRENCIES

AUSTRAC recognises that most people engage with digital currency for legitimate purposes. However, financial service providers, including DCE providers, should assess and understand the risks associated with the services they offer.

To address these risks, financial service providers should identify and understand the associated money laundering and terrorism financing risks and have appropriate risk-based systems and controls in place as part of their AML/CTF programs.

REPORTING SUSPICIOUS BEHAVIOUR

Observing one of these indicators may not suggest illegal activity on its own. When you conduct further monitoring and observe other activity that raises suspicion, you should submit a suspicious matter report to AUSTRAC.

High-quality, accurate and timely SMRs give us the best chance to detect, deter and disrupt the criminal abuse of digital currencies to help protect Australians.

To find out more visit: austrac.gov.au/smr.

WHEN TO SUBMIT AN SMR TO AUSTRAC

If you see something suspicious and report it to police, you must also report it to AUSTRAC.

You must submit an SMR to AUSTRAC if you suspect on reasonable grounds that a customer is not who they claim to be, or the designated service relates to terrorism financing, money laundering, an offence against a Commonwealth, State or Territory law, proceeds of crime or tax evasion.

FOR MORE INFORMATION

If you have questions about your AUSTRAC compliance obligations, please email contact@austrac.gov.au or phone 1300 021 037.

ADDITIONAL RESOURCES

Further information about digital currencies and DCE providers can be found on the Financial Action Task Force website.

DCE providers can find industry-specific guidance on the AUSTRAC website.

GLOSSARY

NAME	DESCRIPTION
Chain-hopping	When a digital currency on one blockchain is exchanged for a digital currency on another blockchain. The value in one digital currency is moved from an asset on one blockchain to value in another digital currency on a different blockchain, hence the term 'chain-hopping'.
Cluster	A collection of addresses which blockchain analytic software determines are controlled by one entity.
Cryptocurrency ATMs (CATMs)	These ATMs allow the exchange of government issued currency for digital currencies and vice versa. These are also referred to as kiosks, crypto ATMs or bitcoin ATMs.
De-banking	Loss of or limitation of access to banking services.
Digital currency exchange (DCE) providers	In Australia, a DCE provider is an individual, business or organisation that exchanges government issued currency for digital currency or vice versa as part of operating a digital currency exchange business. DCE providers must be registered with AUSTRAC. In other jurisdictions, DCE providers are also known as Virtual Asset Service Providers (VASPs).
Digital currency	A digital representation of value that functions as a medium of exchange and a store of economic value. Digital currencies can be traded or transferred with other digital or government issued currencies, and can be used for the payment of goods and services or for investment purposes. References to digital currency in this financial crime guide includes 'crypto', 'cryptocurrency' and 'virtual assets'.
Distributed ledger technology	Also referred to as blockchain technology, refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that is spread across multiple entities or locations.
Fungible	A good or commodity that is interchangeable with something else of the same type and value. Commodities, common shares, and dollar bills are examples of fungible goods.
Malware	A type of malicious software that performs unauthorised actions on a victim's computer, for example encrypting files and rendering a victim's computer unusable.
Mixer	A service used to provide anonymity to digital currency transactions. A user's digital currency is mixed with the transactions of others before being redirected back to the user.

NAME	DESCRIPTION
Privacy coin	Digital currencies that provide enhanced anonymity by obscuring the amount, destination and origin of transactions.
Smart contract	A transactional protocol or computer program that automatically executes when relevant events tied to the agreement takes place and which operates on a distributed ledger or blockchain. No central authority or third party provider is needed for the smart contract to execute.
Structuring	A money laundering technique involving the deliberate splitting of transactions into smaller amounts in order to avoid actual or perceived threshold transaction reporting requirements.
Trading robot	A software program that an individual can set up to automatically trade digital currency on their behalf when specific market conditions are met. Often these robots are given access to the individual's account.
Virtual private network (VPN)	Provide online privacy and anonymity by creating a private network from a public internet connection. VPNs mask a user's IP address and establish a secure, encrypted connection.
Wallet	Store private keys and corresponding addresses (which enable the transfer or receipt of digital currency) under the control of an entity.

AUSTRAC.GOV.AU

1300 021 037

contact@austrac.gov.au