CHARTERED ACCOUNTANTS
AUSTRALIA + NEW ZEALAND

DavidCo Limited
CHARTERED ACCOUNTANTS

Level 2, Shortland Chambers
70 Shortland Street, Auckland
PO Box 2380, Shortland Street
Auckland 1140
T +64 9 921 6885
M +64 21 639 710
E arun.david@davidco.co.nz
W www.davidco.co.nz

WEEKLY COMMENT: FRIDAY 12 AUGUST 2022

1. For the next few weeks I am going to review the taxation of cryptoassets (the term used by Inland Revenue to refer to virtual currencies) in New Zealand. I begin this week by looking at the underlying concepts, as summarised by the OECD in the October 2020 publication "Taxing Virtual Currencies – An Overview of Tax Treatments and Emerging tax Policy Issues" OECD (2020), OECD, Paris.

OECD Overview of tax treatments on taxing virtual currencies

2. Cryptoassets are digital assets (commonly known as coins or tokens) that use cryptography to secure transactions and verify the transfer of the coins or tokens. Instead of relying on a financial institution to verify transactions, cryptoasset transactions are confirmed by computers operating on the currency's network (distributed ledger technology).

3. The OECD notes that the expression 'cryptoassets' is commonly considered by regulators and researchers to cover three main categories of digital financial assets that are based on distributed ledger technology (DLT).

4. These categories are:

   (a) **Payment tokens** (also known as cryptocurrencies or virtual currencies), which are intended to operate most similarly to traditional fiat currencies, and are usable as a means of exchange for goods or services, and possibly also as a store of value and unit of measurement (e.g. Bitcoin, Litecoin and Ethereum, stablecoins and central bank digital currencies or CBDCs);

   (b) **Security tokens** are designed as tradeable assets that are held for investment purposes, and classified as a security (or equivalent) under applicable laws (e.g. Spice, BCAP); and

   (c) **Utility tokens**, whose primary use is to facilitate the exchange of or access to specific goods or services, and may, for instance, act as a licence to allow the holder access to a particular service, as a pre-payment or voucher for a good or service (e.g. Storj, a token that provides access to a peer-to-peer network cloud storage service).

5. "Virtual currencies" are not considered as similar to fiat currency in most countries – the official, sovereign currency being legal tender. Virtual currencies are the most widely-known forms of crypto-asset and include the very well-known Bitcoin as well as Ethereum. The term "virtual currency" also includes more recently developed forms of payment tokens that are backed with real assets (e.g. securities or fiat currencies), which aim to be more stable and that are therefore called "stablecoins". Finally, another evolution of virtual currencies is the concept of a "central bank digital currency" (CBDC), which would be

backed by public authorities and which is under consideration in a number of countries to provide an alternative to other forms of virtual currencies.

6. In October 2020, the OECD Financial Action Task Force (FATF) defined a "virtual asset" as "a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes". Nevertheless, the term crypto-asset is commonly used to refer to types of digital financial assets that are based on distributed ledger technology (DLT) and cryptography as part of their perceived or inherent value.

7. The World Bank Group defined DLT (in 2020) as "a novel and fast-evolving approach to recording and sharing data across multiple data stores (ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes". The technology allows for transactions and data to be recorded and shared in a synchronised and decentralised way across network participants. The key advantage is that transactions between network participants do not necessarily need an intermediary or central party to be processed.

8. **Blockchain** is a specific kind of DLT, which underpins many different applications, including many of the virtual currencies, such as Bitcoin. "A 'blockchain' is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called 'blocks' that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner.

9. DLTs can rely on different consensus mechanisms to validate any new operation or transaction occurring on the network. The most commonly-used consensus mechanisms are the following:

   (a) **A proof of work system** is based on mathematical equations, typically hard to solve but whose solutions can be easily checked. Solving the mathematical problem involves computational efforts – resulting in high energy consumption, whereby each validator (called a 'miner') makes calculations to verify the transaction and share their results with the network, working on a competitive basis since a reward is credited to the miner who finds the solution first. Proof of work is for instance used with the Bitcoin blockchain, and currently most DLTs.

   (b) **A proof of stake system** assigns shares of validation rights to users according to the stake they have in the blockchain. In such a system, validators are not called miners – but 'forgers' or 'stakers'. Stakes can be measured differently (amount of tokens owned, holding period, amount of assets locked in the blockchain as collateral). Forgers or stakers must have a minimum stake in the blockchain to be able to participate in the verification process: they 'stake' their own tokens to have the right to verify a transaction, and are credited a transaction fee or new tokens. No mathematical equations are therefore required to verify a transaction. This makes the verification process considerably more energy efficient than a proof of work mechanism. Proof of stake is for instance used with the Peercoin blockchain.

   (c) **Other consensus mechanisms** exist but are less common, including 'delegated proof of stake' – whereby token holders can vote to designate who they wish to be a block validator – and 'proof of authority' – whereby validators do not stake their tokens, but rather their reputation: if they prove to be unreliable, they are not allowed to validate blocks any longer.

10. A typical "lifecycle" of a unit of virtual currency is as follows:

(a) **Creation:** When a new virtual currency is created, one of the first steps is to ensure that it is available in the hands of potential users. This can occur in a number of ways, including through airdrops, an initial token offering, mining and/or forging:

(i) **Airdrops:** an airdrop is the distribution of tokens without compensation (i.e. for free), generally undertaken with a view to increasing awareness of a new token, particularly amongst "influencers", and to increase liquidity in the early stages of a new token project. The New Zealand tax treatment of an airdrop will be covered in a later *Weekly Comment*.

(ii) **Initial Token Offering (ITO):** also known as an Initial Coin Offering (ICO), an ITO involves the issuance of a new token, which is often issued in exchange for one of the major virtual currencies e.g. Bitcoin, or in some cases, fiat currency. The majority of ITOs to-late 2020 involved the issuance of utility tokens, rather than security tokens or virtual currencies. While initially common, ITOs have been considerably less frequent in 2019 and 2020 than in earlier years, in part due to the efforts of the United States' Securities and Exchange Commission and other national agencies in regulating ITOs. The declining use of ITOs also reflects the evolution of the market with fewer players in a position to compete with well-established virtual currencies such as Bitcoin and Ether.

(iii) **Mining:** refers to the process in some distributed-ledger protocols by which transactions of virtual currencies are verified and are added to the blockchain-based ledger (record of transactions). The "miner" (the person on the network undertaking the necessary computer processes by being the first to solve complex equations, typically under a 'proof of work' protocol) may be entitled to (i) a mining reward, paid through new tokens, and/or (ii) a protocol transaction fee, which is a percentage of the value of the transaction being processed and is paid from that transaction. For the existing blockchains, in particular for virtual currencies, creating and releasing new blocks to a chain is mainly achieved through mining as the most popular blockchains are based on a 'proof of work' mechanism (e.g. Bitcoin, Ethereum – for now, and Dash). To maintain a limited and finite supply (possibly for other reasons), virtual currencies are designed with a fixed upper limit on how many tokens can be mined. For example, Bitcoin's maximum supply has been capped at 21 million tokens since its inception in 2009 – there were over 18 million in existence as of July 2020.

(iv) **Forging:** this is often termed more commonly as staking and refers to the process through which transactions are verified when a DLT uses a 'proof of stake' mechanism, as described above.

(b) **Storage:** In order to hold a token, users require a wallet. Each wallet consists of one, or multiple, digital wallet addresses. In 2020, the main types of digital wallets for holding crypto-assets could be grouped into four categories:

(i) **Hot custodial wallet:** a wallet that is connected in some way to the internet (i.e. "hot") and which is managed by a third party (e.g. TrustVault), whereby the third-party holds the user's private keys – these are a form of cryptography that allows the user to access the wallet, which is an element of security.

(ii) **Hot non-custodial wallet:** also connected to the internet, the user downloads a software application to create the wallet on their own computer, whereby the user retains control of their private keys. Examples include Copay and Electrum.

(iii) **Cold hardware wallet:** a physical device (similar to a USB/flash drive) that is kept offline (i.e. "cold") but which can be connected to an online computer when needed (e.g. Trezor and Ledger Nano S).

(iv) **Cold paper wallet:** pieces of paper on which the digital address and private key are recorded. They can be generated by downloading a piece of software, which is then run on an offline computer and printed, before deleting the wallet before the computer is re-connected to the internet. (e.g. Paper Wallet and Walletgenerator.net).

(c) **Transfer:** The wallets use asymmetric cryptography based on a key-pair made up of a public and private key, to maintain the security of any token transactions. The digital wallet address is a cryptographically encoded version of the public key. The accompanying private key is kept confidential to the user. Transactions are completed as follows:

(i) When executing a transaction the sender "signs" the transaction using their private key. Using the public key, the receiver, as well as all the other users on the network, can verify the private key to confirm that the right sender indeed approved the transaction and has the funds available to make the transaction.

(ii) Transactions are validated and then compiled into a block with other transactions, time-stamped and "confirmed", adding the blocks in chronological order to the blockchain ledger.

(d) **Exchange:** In order to find potential token purchasers or sellers, a user may use a virtual currency exchange or an over the counter (OTC) broker through a peer-to-peer network or a third-party intermediary. (Exchange platforms and brokers – also known as Virtual Asset Service Providers (VASPs) – are regulated in the EU where Know-Your-Customer (KYC) due diligence applies to entities providing services of holding, storing and transferring virtual currencies.) These services may facilitate the exchange of one unit of virtual currency for goods and services, for another type of virtual currency, for another type of crypto-asset, or for fiat currency:

(i) **Virtual currency Exchange:** an (online) service allowing customers to trade virtual currencies for other assets, either fiat currency or other crypto-assets. At this stage, these services are predominantly still custodial (e.g. Coinbase, Kraken), although some non-custodial exchanges (essentially online "peer-to-peer" thus limiting or removing the role of a centralised intermediary) exist, although levels of adoption are low.

(ii) **Over the Counter (OTC) broker:** this refers to a process of brokering an "off-market" exchange of tokens in exchange for either fiat currency or for other crypto-assets. Such transfers may either be offline "peer to peer" exchanges, or be brokered by a third-party intermediary. They are often used for the transfer of a large value of tokens to secure a specific market price by avoiding price slippage while the transaction takes place. The use of OTC brokers is becoming more

common and it is generally accepted that volumes of transactions are higher via OTC brokers than via exchanges.

(e) **Evolution of a token:** As the rules relating to the functioning of each type of virtual currency are established by the underlying protocol that is shared by all of the users of that token, most changes to how the token functions requires a change to that protocol. These might be, for example, changes that would improve the speed at which transactions can be processed by changing how much information can be included in each block on the chain. These changes are known as forks in the chain and require users to update the protocol software they are running. In order to implement a fork, a majority of users running the protocol must agree to the change. There are two main types of fork:

(i) **A hard fork:** (sometimes also referred to as a "chain split") changes the protocol code to create a new version of the blockchain alongside the old version, thus creating a new token which operates under the rules of the amended protocol while the original token continues to operate under the existing protocol (for example, the July 2017 hard fork of Bitcoin that saw the creation of the Bitcoin Cash token alongside Bitcoin). The New Zealand tax treatment of a hard fork will be covered in a later *Weekly Comment*.

(ii) **A soft fork:** also updates the protocol, however, it is intended to be adopted by all users on the network and thus no new coin is expected to be created (e.g. the August 2017 Segwit fork to the Bitcoin protocol).

Characterisation as property for NZ tax purposes

11. Inland Revenue notes that in New Zealand, cryptoassets are treated as a form of property for tax purposes. While there are different types of cryptoassets, the tax treatment depends on the characteristics and use of the cryptoassets. It does not depend on what they are called. As discussed in more detail in next week's *Weekly Comment*:

(a) Cryptoassets are not subject to GST when they are bought or sold, but do have GST implications when they are received as payment for normal business activities;

(b) Crypto assets are not financial arrangements.

12. Inland Revenue notes that the cryptoasset sector is still developing and there is currently no standard terminology used. Cryptoassets is the term Inland Revenue uses. They are also known as:

(a) Cyptocurrencies;

(b) Cryptographic assets;

(c) Digital financial assets;

(d) Digital tokens;

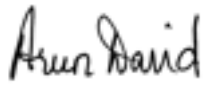
(e) Virtual currencies.

13. Similarly to the OECD, Inland Revenue distinguishes between:

    (a) **Payment tokens:** Cryptoassets that are intended to be a means of payment or exchange, for example Bitcoin and Litecoin, are often called payment tokens, exchange tokens, intrinsic tokens or simply cryptocurrencies;

    (b) **Security tokens:** Cryptoassets that represent existing property or financial assets, and so mirror securities like shares or debt, are often called security or asset tokens; and

    (c) **Utility tokens:** Cryptoassets that are more like traditional payment vouchers are often called utility tokens because they can be used to gain direct access to specified goods or services.



Arun David, Director,
DavidCo Limited