TALES FROM THE CRYPTO

Authored by: Alex Cooke – Schneider Financial Solutions

Alex Cooke is founder and CEO of litigation finance provider Schneider Financial Solutions, and recently completed the University of Oxford Blockchain Strategy Programme. Read this article to confidently engage in crypto discourse. There's a high chance you'll be asked about it.

For the uninitiated "crypto" is enticing, confusing and often a little scary. The crypto road is fraught with risk from setting up accounts on exchanges, to price volatility, let alone transferring assets from one wallet to another - especially when one wrong move could send your crypto to the land of the lost forever. That's right, there's no getting it back, no-one to call, and no Ombudsman or government to turn to. Crypto is not for the faint-hearted.

That being said, as an investor in crypto and a verifiable blockchain enthusiast, it does not surprise me to see crypto assets becoming increasingly prevalent in private client and matrimonial disputes; Bitcoin is after all "digital gold", and the current market cap across all crypto assets stands at just under $2 trillion. If Elon has his way, Dogecoin will be the future currency of Mars.

At last count crypto is responsible for 19 billionaires according to Forbes, which recently featured Binance's CEO "CZ" or Changpeng Zhao on its front cover. It is estimated that there are between 100-300 million Bitcoin users currently (noting that one wallet address does not equal one user).

Love it (like Michael Saylor) or hate it (like the European Central Bankers), crypto is going to become an increasingly common asset in our clients' portfolios, and I believe often the source and medium of their wealth.

Advisors can no longer afford a lack of understanding about cryptocurrency and how it works. In this article I will explain the basics which will hopefully get you started in thinking about the right questions to be asking your clients where crypto assets are involved.

BLOCKCHAIN

Cryptocurrency is intangible. As it does not operate through any traditional banking system, one of the main questions often asked is "where does it actually exist"? Whilst there are some (technical) exceptions, crypto assets exist on blockchains.

So, what exactly is a blockchain and why is this important? A blockchain is a decentralised and immutable digital ledger secured by a large, distributed network of nodes (computers with relevant software connected to the network), each holding an identical copy of the full ledger.

For a new transaction to occur and be entered into the ledger the majority of nodes must verify the transaction as true. So essentially a blockchain is a system for recording information in a way that makes it almost impossible to change the data or cheat the system.

According to Cointelegraph the number of active Bitcoin nodes in July 2021 exceeds 13,000.

Whilst I will concentrate on public blockchains in this article, it is important

to note that there are both private and public blockchains. The likes of Bitcoin, Etherium, Terra and Avalanche (to name but a few) are all public blockchains, meaning that they are fully decentralised, and transactions are visible, (if you know how to get the analysis).

Private blockchains on the other hand are centralised and as the name suggests entirely private. Sectors such as (non-decentralised) finance and healthcare use private blockchains.

Whilst often overlooked, at least 57 central banks are at various stages of creating digital versions of their own fiat currencies, known as Central Bank Digital Currencies (CBDC's). CBDC's will run through private government-owned blockchains with CBDC's held in secure digital wallets.

TERMINOLOGY

The terms "digital assets", "cryptocurrencies" and "tokens" are often used interchangeably, however there are differences. A "digital asset" is a non-tangible asset that is created, traded and stored in a digital format. "Cryptocurrencies" and crypto "tokens" are sub-classes of digital assets that utilize advanced encryption techniques, or cryptography, to ensure authenticity of the asset, as well as eliminating the potential for counterfeiting or double spending. So, what's the difference between a currency and a token?

A cryptocurrency, (for example Ether "ETH" on the Etherium blockchain), is issued directly by the blockchain protocol (the computer-coded rules that establish the structure of the blockchain) and is therefore the native asset of a blockchain that can be traded, utilised as a medium for exchange and used as a store of value. When completing transactions on blockchains, fees (known as "gas") will be incurred, which will be charged in the native currency. Cryptocurrencies will also be used to incentivise users to maintain the network security, i.e., for Proof of Work (PoW) consensus mechanisms, in return for verifying transactions a node will be rewarded in the native cryptocurrency.

Tokens on the other hand are units of value that blockchain-based organisations develop on top of existing blockchains and allow for interoperability across the blockchain's ecosystem. Building and maintaining your own blockchain is expensive and time consuming, therefore most protocols are built on top of existing major blockchains, (in the same way that if I wanted to create a taxi company, I don't need to set up a car manufacturing plant to build my own cars). Tether's USDC stable coin is a good example of an Etherium based (ERC-20) token.

There are four common traits of tokens:

- **Programmable – they run on software protocols, composed of smart contracts;**
- **Permissionless – they can participate within the ecosystem without special credentials;**
- **Trustless – no centralised authority controls the system; and**
- **Transparent – the rules of the protocol and its transactions are viewable and verifiable by all.**

The ease of building on top of existing blockchains and the interoperability of tokens, means that the number of new protocols is likely to continue to grow extensively.

DIGITAL WALLETS

A digital, or non-custodial wallet is used to store, send and receive cryptocurrencies and tokens on a blockchain. The wallet owner maintains control and security over their assets instead of a third-party custodian, such as a bank. Whilst no third-party custodian can prevent wallets making transactions, in very rare cases it would be possible for a wallet operator to prevent a particular wallet address from making transactions. Such action would be extremely uncommon and would likely involve a directive from the Courts.

A digital wallet has two primary components:

- **Private Key: denoted by a randomly generated series of numbers and letters that is only known by the owner; and**
- **Public Key: The public key can be given to anyone who wishes to send funds to that digital wallet.**

Through public key addresses, users can view transactions that occur "on-chain". This is a critical part of blockchain's transparency, and whilst the name of the person associated with a particular wallet address is never associated with that address on the blockchain, the balance of the wallet is easily verifiable along with the associated transactions to and from other wallets.

Digital wallets come in two forms:

- **Cold wallets: Hardware wallets that are not connected to the internet, making them more secure against hackers who are unlikely to get access to them offline; and**
- **Hot wallets: Digital wallets connected to the internet, such as MetaMask.**

ACQUISITION AND "HODLING" CRYPTO ASSETS

While Decentralised Finance (or DeFi) offers crypto investors and speculators significant opportunities to create (and lose) wealth through mechanisms such as staking and yield farming, for the purposes of this article I am going to refrain from going into the detail on these fascinating protocols and will focus on the more common and longer-term strategy of buying and holding, or "hodling" as it is now known in the cryptoverse due to a celebrated typo.

It is likely that the majority of clients will acquire their (non-CBDC)

cryptocurrencies and tokens (collectively "crypto assets") initially through a centralised exchange, such as Binance or Coinbase, however it is less likely that they will necessarily maintain the assets on that exchange.

For some, centralised exchanges are simply an "on-ramp" to convert fiat currency into crypto that will then quickly leave the exchange to a "hot" wallet such as MetaMask to be deployed into a decentralised exchange (DEX) such as Pancake Swap or Trader Joe. Such DEX's allow investors to acquire less-mainstream crypto assets or participate in token sales before listings on the larger centralised exchanges in the hope of locking in 100x+ returns. DEX's do not custody assets acquired through their exchanges, but rather the assets are transferred directly into the hot wallet, that likely lives on the owner's phone or computer.

Others will acquire their preferred crypto assets and then withdraw these assets from the centralised exchange to a cold storage wallet. Maintaining crypto assets on an exchange means that these holdings are potentially at risk from hacking or business risk (such as the failure of the exchange). To mitigate these risks, the majority of investors (both institutional or retail) will send their crypto assets to a cold wallet for safekeeping.

By way of example just 12.36% of all BTC (Bitcoin) in circulation is held on centralised exchanges. This means that the vast majority of BTC is currently being hodled off-exchange.

Given the effort, risk, and gas fees in moving crypto assets on and off exchanges, it is generally considered that assets held off-exchange are long term investment assets, whilst assets held on-exchange are available for trading.

The rapid growth in awareness in this ever-growing asset class and ease of access to major crypto through consumer banks is leading to mass adoption and bringing about an interesting challenge for private client practitioners, trustees, and executors. There will be an increasing need to consider and deal with vast ranges of crypto assets, held across multiple centralised exchanges, hot and cold wallets and throughout the metaverse(s). Considerations will need to be made as to how private keys may be held securely and anonymously until required, as well as strategies around the monetisation and liquidation of assets, as well as tax issues. In contentious disputes, practitioners will also have to consider how to identify where crypto assets are held and how they can be enforced against.