SECTION 7

CRYPTOCURRENCY

7.1 MONEY

"In God we trust. All others pay cash."
Anonymous

The term **CRYPTOASSETS** is often used as an umbrella description for all cryptocoins and crypto tokens. However, coins and tokens are very different instruments. Cryptocoins are intended to be digital currencies whereas crypto tokens are often security-like instruments.

It's a whole new world! Let us begin with cryptocoins also known as cryptocurrencies. We will use the terms interchangeably.
In order to understand the basic concepts and properties of cryptocurrencies, we must first remind ourselves of some basic definitions of money.

COMMODITY MONEY is where the value of the currency is underpinned by some physical asset such as gold or silver. The USA, like the UK, used a **gold standard** until the 1970s. Then the American government broke the relationship between U.S.Dollar (USD) and gold (previously fixed at USD 35 per ounce). Why? Because the supply of gold grows very slowly, and the US government couldn't issue as much new money to meet their spending and inflation aspirations as they wanted to. No gold standard meant no limit to printing. Thus, they ended the gold standard.

What is a currency called when it has no value link to physical commodity reserves? Answer: Fiat currency.

FIAT CURRENCY is legal tender whose value is only backed by the government that issued it – via a fiat decree – simply decreeing ie. stating that the currency has worth.
Examples: the USD, Euro, GBP, and many other major world currencies. A fiat currency's value is underpinned by the strength of the government that issues it, not its worth in gold or silver.

Now let's start to explore the digital crypto world a little ....

CRYPTOCURRENCY

A technical definition of cryptocurrency may be accepted as decentralised and encrypted (using cryptology) digital money. It is used to explain the creation of monetary (value) units, and to verify the transfer of these units (funds) as stored on a blockchain. There are many types of cryptocurrency.

EG Bitcoin, Ethereum, Ripple, Litecoin

Their purpose is to act like money over the internet as a unit of account, store of value, and medium of transfer.
Like physical fiat currencies they have no intrinsic value. They are generally not backed by anything tangible. Therefore, they are only worth what people are willing to pay.

Today, most cryptocurrencies operate independently of government and central banks. That is unlikely to be the case moving forward; for example, the Singaporeans are leading the way with their Ubin project.
Note that many will use the term cryptocurrency to refer to

cryptocoins (digital coins).
We like the idea of cryptocoins as units of account and payment methods – helping to remove friction from the foreign exchange and payments world. But that is not the case or purpose behind many cryptocoins. The store of value motive, namely that their value may go up and down, is to us, very uncomfortable. We will come back to this later.

STABLECOINS

The happy medium? Stablecoins are cryptocoins that try to maintain the same VALUE over time by pegging themselves to some underlying asset such as a fiat currency or gold, for example, the Caribbean's BITT digital dollar standard and Tether. Does that mean you go into a bank and exchange one real green USD note for one, let us say, stablecoin USD? That is the theory but it is not quite working that way yet. What it also does not mean is that this is commodity money yet. Indeed, there is not a physical green USD note sitting in a vault to support every stablecoin USD issued. This is why we aren't talking about Facebook's Libra coin. We don't know yet what it's linked to, if anything!

CRYPTO (AKA DIGITAL) TOKENS

Like fiat currency (e.g. USD) or cryptocoins (e.g. Bitcoin) a crypto token has no intrinsic value. But, unlike fiat and cryptocoins, crypto tokens are not trying to be legal tender but are used to represent a specific single purpose.

There are two main types of token with very different features and motivations. They are however, generally created through

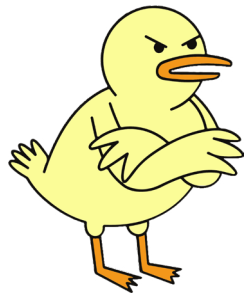
the same mechanism as cryptocoins: an Initial Coin Offering (ICO). Let's explore the basic types of token and come back to their creation afterwards.

SECURITY TOKENS (or tokenised securities)

Often issued to represent an early stage investment into a (technology) company in exchange for cryptocoins (eg Bitcoin) – we call this type of crypto token Security Tokens.

There is a lot of contention in the crypto community as to whether security tokens should be regulated. Generally, Tokenologists are anti-establishment and reject the idea of government-backed regulators, together with their laws and frameworks. Regardless of beliefs, given that we are in a hybrid world of physical and crypto, all stakeholders need to be protected (see later in this section).

For now, the accepted global practice is to regulate security investments, crypto or otherwise. So, the key question for us is whether all security tokens are financial investment securities? The simple answer is: if it looks, sounds and quacks like a duck then it probably is a duck, and the same applies to security tokens. **The Howey tests** help us to determine this.



THE HOWEY TEST comes from US legislation in 1946. Under these regulations, the SEC determines that a transaction is an investment to be regulated if:

1. It is an investment of money or similar;

2. There is an expectation of profit from the investment;
3. The investment is in a common enterprise;
4. Any profit comes from the efforts of a promoter or third party.

In the maverick world of crypto regulation, this feels like a four-letter word, so there is trouble ahead ....

The other main type of crypto token is a **UTILITY TOKEN**. These are used as a form of payment to access a company's product/services.

Here the confusion starts. Most utility tokens to date have been issued to raise 'money' via crowdfunding, in order to sponsor and support a plethora of projects. Many of these projects failed, or even lacked legitimacy. We will explore later some common-sense tests to apply when "supporting/ acquiring".

When a project is very early stage, and funds are needed to get it off the ground, utility tokens may be issued to raise the initial capital to start. As above, this is often through crowdfunding, and effectively emotionally pleading for project financing. 'Donors' don't always get anything back – maybe just a promise of goodwill, loyalty points, discounts, or (and here's the confusion) access to discounted security tokens if/when the project is successful. This latter example explains why some utility tokens are early stage security tokens, but this is not always obvious to determine.

However, the utility coin is increasingly commonly issued in order to raise funds to access a service or product. These

are not equity instruments but *single purpose* digital payment methods akin to a casino token, or the penny slot machine tokens in seaside arcades.

Some current real-world examples are listed below (hopefully they will still be "live" when you read this!):

NPXS TOKENS. PundiX make cryptocurrency transaction payment machines, and want to encourage retailers to use their machine in-store, in order to accept payment in their own cryptocurrency – the NPXS coin. PundiX reward retailers and clients with NPXS tokens that are redeemable for fiat, or the retailer's products. Hence, NPXS is both a coin and a utility token.

DOGECOIN. This was born as a 'joke' and was/is used to represent donations for charitable purposes. The donor is rewarded with a dogecoin which carries little value, but is a form of acknowledgement for their act of kindness.

ETHEREUM. The Ethereum token allows the developers to access their open source platform, and is heavily associated with the smart contract an Ethereum platform concept. This encourages blockchain developers to focus collectively and collaboratively on challenges for the Ethereum platform, such as scalability.

Ethereum faces significant competition from other blockchain platforms and protocols, such as Stellar, EOS, NEO and Waves.

Let's go back to the creation process for all crypto assets.

ICO (INITIAL COIN OFFERING)

We use this term when a (technology) company releases its own crypto assets, and sells or awards them to investors, supporters and clients, in exchange for cryptocoin or physical fiat money.
As we learnt above, the crypto asset can be a cryptocurrency i.e. coin, or a crypto security or utility token. Later in this section, we explain where and how they can be purchased, sold, held, and stored.

So we have learnt:

- ✓ Commodity currency is linked to a real asset like gold.
- ✓ Fiat currency has no intrinsic value (USD, Yen, GBP and Euro).
- ✓ Crypto Assets refers to ALL cryptocoins and crypto tokens. Cryptocoins are digital currencies and act like money OVER the internet as a unit of account, store of value and medium of transfer. They have no intrinsic value.
- ✓ Stable coins are cryptocoins where the value is linked (NOT underpinned) to another asset such as USD.
- ✓ Crypto tokens are NOT trying to be legal tender but are used to represent a specific single purpose.
- ✓ Security Tokens represent an early stage investment into a (TECH) company in exchange for fiat cryptocoins.
- ✓ Utility Tokens are used as a form of payment to access a company's product/services.

7.2 FIAT MONEY VERSUS CRYPTOCURRENCY

A debate which will run for some time concerns the relative merits of cryptocurrencies versus fiat money. Supporters of this new digital world will put forward many emotional, as well as practical, arguments regarding the benefits of cryptocurrencies vis-à-vis fiat money, and the cynical conventionalists will do the reverse. In light of this we have tried to consolidate the properties of both fiat money and cryptocurrency into a simple table, in order to illustrate their advantages and disadvantages.

It is our view that as a mechanism for payment and a medium of exchange, cryptocurrency is here to stay. Who hasn't queued up behind someone in a coffee bar who has used their phone to pay? To our children, the gold standard is something from a textbook, they are not as trusting in their governments or banking sectors as their elders.

Rather, they have grown up in a world where fiat money is digital – so it's all digital to them – Bitcoin, Euro, GBP or USD; they don't differentiate! They are predisposed to place more trust in a technological consensus network than politicians and bankers. We believe cryptocurrencies are not going away. Having said that, have we seen the Google and Amazon of cryptocurrencies yet? We think not. We also think it will be a bumpy road of 'Ask Jeeves' first.

As described in an earlier chapter, we don't subscribe to cryptocurrencies as an investment asset class; i.e. store of value. We do not agree that there are sufficient fundamentals (such as

reward for Proof Of Work) to support this capital appreciation and depreciation. We believe this is an Emperor's new clothes scenario. Yes, they can be finite in the quantity issued as per gold and the USD, but they can also be divided and 'fork', as they did so with Bitcoin Lite.

Firstly, let us explore the properties of real money versus cryptocoins to help us make an informed opinion.

PROPERTY	'FIAT' MONEY	CRYPTOCOINS	
1. Divisible	✓	✓	
2. Durable	✓	✓	Exists as a ledger
3. Fungible/Portable	✓	✓	
4. Verifiable/Recognisable	✓	✓	Through blockchain consensus
5. Limited/Scarce	✓	✓	
6. Decentralised		✓	No government or political manipulation
7. Peer 2 Peer		✓	Cannot be easily counterfeited
8. Anonymous		✓	Risk: KYC issues
9. Transparent		✓	
10. Trusted/ Programmability		✓	Risk is with poor/weak protocols and wallets
11. Easy to buy/sell		✓	
12. Very low transaction fees		✓	
13. Irreversible/Immutable		✓	

Prima facie, the properties of cryptocurrencies are the same, if not better, than fiat money from a payment mechanism and medium of exchange perspective. We will leave it here for now and explore some of these properties further, to enable readers to challenge and decide for themselves.

7.3 CRYTOCURRENCY STORAGE

As we learnt in the section on the blockchain and distributed ledgers, crypto assets are 'recorded' in a ledger that is shared or distributed, with all the participants. Therefore, everyone, with the right permission, receiving the same updates to the ledger, once the consensus protocol has been fulfilled, will be able to see the same transactions. We also learnt that this distribution and permissioning is controlled through cryptography in a blockchain.

Although consensus is transparent, and the transaction being validated and verified is also transparent, the actual identities of the participants behind the transitions are not transparent. Their real names, addresses and account numbers are not shared openly. Many of the Know Your Client (KYC) and regulatory issues originate from this oxymoron – transparency and trust is in the computers themselves and not the individuals behind them.

From a cryptocurrency perspective this is an important aspect to the safety of those buying, selling and storing their cryptocurrencies.

Cryptocurrencies are stored in a cryptocurrency wallet based on two cryptographic inspired concepts: an open public key and a private (password) key.

This is two-factor encryption, as explained in Section 2. The public key is 'open' because it's in the public ledger. That old 27-34 alpha-numeric character concept again. The public (key) address for a wallet is a bit like your sort code and account number in traditional banking. Therefore, it can be shared either in text, or as a QR Code.

The second concept is the private key. This is the password to access your cryptocurrency public key account, and instruct transactions. This is where a lot of the operational risk lies with hacking. The private password key will enable access to the public key wallet. We can understand this risk better when we understand the different types of wallet storage, and therefore, wallet providers.

There is a lot of choice for cryptocurrency **WALLET STORAGE**:

1. Local Hard Drive Software Wallet

A local wallet is created through downloading or installing software. **For example, Exodus**. Your wallet is totally anonymous, and therefore very safe. Your password doesn't live on the internet. However, lose or forget your private key, or lose or damage the hard disk, or the computer itself, and you've lost your cryptocurrency. This may be seen as quite high operational risk.

2. Hardware Wallet

This is a specific, single-purpose device which stores the private key, and thus the wallet. The private password key is never revealed, not even to the user. Once your transaction has taken place, the wallet is offline – you take the stick out. It can't be hacked or accessed. It's similar to a USB memory stick with a small screen. You plug it in, and execute your transaction. Providers include **LedgerNano S and The Trezor**. As above, lose the device and you've lost your wallet! A variation of the Hardware wallet is the **Paper Wallet**. You print off all the data for the transaction, both the public and the private key and keep it safe, preferably offline in a physical safe.

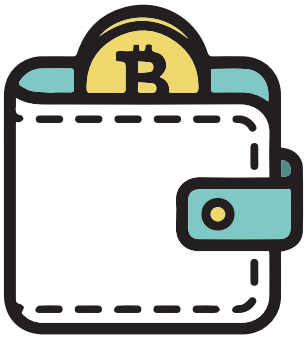
3. Cloud-hosted Wallet, aka Online Wallet, aka Exchange Wallet, or Internet Wallets

These are generally provided by cryptocurrency exchanges. The obvious benefits are that they are easy to set up and use. **Coinbase, Revolut, and GDAX are all examples of well-known providers**. The thing to remember is that you are giving permission to the wallet host provider to see or use your private key. Your wallet and private key are online; they are on the internet. Thus, they are only as safe as the wallet host provider's own cybersecurity standards. You therefore run the risk of the hosted company defaulting or being hacked. By definition, they are not totally anonymous either.

4. Mobile Software Wallets

Here you can set up your wallet by purchasing software to download/install to your phone. Examples include **Mycelium**.

As for advantages, in common with cloud-hosted it's easy to set up and use. Also, like Local Hard Drive Wallets, it's safe as the account security is not sitting on the internet, but instead on your phone. However, these wallets are only as secure as your phone!



WALLET SECURITY

When trying to understand cryptocurrency wallet security the crypto world use the concept of **Hot and Cold Wallets**.

A **HOT WALLET** is simply one that is connected to the internet, online, in the cloud, provided by an exchange, and the private key (password) is shared or owned by the wallet host.

By contrast a **COLD WALLET** is not connected to the internet, or can be disconnected. Hard Drive, Hardware and Mobile wallets are all example of cold wallets.

If you are storing large amounts of cryptocurrency then you would be well advised to do so in a **COLD** wallet.

7.4 ACQUIRING CRYPTOCURRENCIES

There are several mechanisms for acquiring, buying and selling cryptocurrencies. A brief overview is set out below:

I. **Peer2Peer** – where you buy / exchange directly with someone else for other crypto or fiat currency.
II. Via a **cryptocurrency exchange** – this is a website that is set up to facilitate trading. They provide you with a wallet capability and validate your ID.
III. **Barter**
IV. "**Mine**" Peculiar to Bitcoin, new Bitcoin is released every 10 mins for free and is awarded to the node (independent party on the bitcoin blockchain) who solves the complex algorithm first (but you will need tremendous computing power to win the race).

Exchanges are the most common today, so let's understand them a little better. These are virtual meeting places where you can buy and sell cryptocurrency efficiently at an agreed market price, determined through supply and demand thereby providing price discovery. Most Exchanges 'take' a fee for the exchange of currency, and provide verification if it is being exchanged for fiat currencies.

Some exchanges will provide bank or broker-like facilities including lending, trading on a margin, short-selling and may indeed integrate with banks. All subject to normal financial health, identity and credit checks.

Examples in alphabetical order: (do your own due diligence)

Binance (was China, now Malta – a full product capability).

BitMex (HK based – full product range and even facilitates margin trading).

Coinbase (user-friendly for novices and low notionals, based in San Francisco).

CoinMama (Israel-based, easy to onboard and with relatively high crypto purchase limits via credit card).

CRYPTO HEALTH WARNINGS

We do not want you to lose money through fraud or stupidity.

- ✓ Be very careful with passwords.
- ✓ Don't leave large cryptocurrency balances on the internet.
- ✓ Don't go big until you understand exactly what you are doing. Learn first.

- ✓ Always apply your common sense.
- ✓ Only do business with people you know or highly recommended websites.
- ✓ If it's too good to be true then it's too good to be true.
- ✓ Don't invest in projects that aren't clear – their purpose, who is behind it, what their milestones are. The list is long and obvious. A fool and their money are soon parted! Search reviews, ask the community, check the history, validate, and then do it all over again.
- ✓ The crypto community really is such – they care and share. There are some great bloggers, 'YouTubers' and columnists. Read, learn, ask.
- ✓ Don't just click on a link.
- ✓ Don't blindly trust an email is from who it says its from.
- ✓ If you can't afford it, don't do it!

That said, this is a new and exciting asset class, and we don't think it's going away. So get involved safely, and enjoy becoming a cryptologist !

SECTION 8

THE REGULATORY LENS