Seminar transcript 23 June 2022: '**Cryptocurrency and the law**' Michael May and Salwa Marsh (barristers, Level Twenty Seven Chambers)

Michael May (MM): Welcome, everybody. We had an issue with the recording last night, so what you are about to hear for the next ten minutes or so is me redoing the first part of the presentation before we kick back into the recording.

The topic for tonight is cryptocurrency and the law. Our aim is to introduce some of the key technologies, explain some of the jargon and some of the [legal] issues that arise.

In putting this together, we have been acutely aware that our audience has a different level of knowledge about the underlying technology and applications. What we are trying to do is give an explanation that will make sense even if you have no background whatsoever, but hopefully using useful information and be able to understand the technology.

[Slide 3] This is a screen capture of the market cap of the top ten cryptocurrencies. You can see even just from this small list, which is probably very depressing, that there are a vast range of cryptocurrencies that do a vast range of different things. That is part of the challenge we had preparing this presentation, which is to try and give an explanation and a bit of an understanding of all those things. Necessarily, we are going to have to cover some areas in more detail than others.

[Slide 4] The way we are structuring the discussion is to first start by looking at Bitcoin. We are going to look at that in some detail for a couple of reasons. The first is that chronologically it was effectively the first cryptocurrency. Secondly, it has the biggest market cap, as we just saw. Thirdly, is that it is, in many ways, the simplest. The fourth is that it is the purest, in some ways, application of some of the concepts that we are talking about.

Through looking at Bitcoin, we are going to explain some concepts like decentralisation, blockchains, mining, hashing, and private/public key cryptography.

The next stage will then be to discuss more advanced cryptos. We are going to do that rather than by going through a whole range of different cryptocurrencies and just talk about some of the key [legal] things that arise. In the course of that, we will talk about things like smart contracts, NFTs, DPI, CBDCs and so on. Finally, we will talk very briefly, cryptocurrency exchanges.

DECENTRALISATION

MM: [Slide 5] The first point, in order to understand all cryptocurrencies we have to talk for a moment about decentralisation because it is a common thing that crops up in all of them. To understand what decentralisation is all about it helps to first think about centralisation. The paradigm case of centralisation would be the title's office in a Torrens Title System. In that kind of system, the Titles Office functions effectively as the sole source of truth as to who is the owner of land in the jurisdiction. It is administered by one central authority. The critics of decentralisation would point out that because of this system you are necessarily required to trust the third party. The third party is vulnerable to attack. So, if someone were to hack into the Titles Office computer system and change their records, that would change the issue. And it requires permission of the third party. That is, if you want to register a transaction of the respective land, the Titles Office has to agree to register the transaction. At the time when cryptocurrencies came about, which is sort from of ashes of the GFC [Great Financial Crisis], this was thought by creators to be a problem and decentralisation is the idea of avoiding centralised authorities and replacing them with a network where information is spread freely and there is no need to rely on that kind of third party.

[Slide 6] If you were to take a simple approach towards decentralising the Titles Office, in a sense, the first starting point would be to publish online the full register that the Titles Office has. In a sense, that already happens. You can search the register online, if you pay the fee. Assuming you made the whole thing public without the need for a fee and distributed amongst a network of computers around the world, the problem that decentralisation has to overcome is how do you update that ledger as new transactions need to be added and still keep it spread across the network? How do we know that which version of the various registers kept by different computers in the network is the accurate one and ensure that somebody does not transfer the land twice? Those are the kinds of problems that Bitcoin was created to overcome.

BITCOIN

MM: [Slide 7] The Bitcoin network involves a network of computers which are called miners - which we will come back to. That network is operating a form of code that creates rules, which generate real world incentives for miners and other people in the system to bring about a secure and reliable source of truth in the form of blockchain. Each block consists of information and a chain. A blockchain is a group of those blocks changing in effectively chronological order - we will talk more about that shortly. But critically, the system creates this blockchain without a need for centralisation.

The origins of Bitcoin are somewhat mysterious. It all started with a whitepaper prepared by a person, or persons, unknown going under the name of Satoshi Nakamoto. What happened was that paper was published on the internet, it was picked up by […] who effectively started developing the Bitcoin network and everything crucial there. You can think of Bitcoin as like a really big list containing all the details of all transactions played into Bitcoin. The analogy I can give is, if you imagine a really big bank statement for the whole world that contains all the details of every transaction on everyone's bank statement, except the details of the sender and recipient, effectively scrambled so that they cannot be understood. But critically, it is a publicly available list so that anyone can access it.

The unit of account in the Bitcoin network is called the Bitcoin, obviously. A critical feature of Bitcoin is that there is a limited supply of Bitcoin. So there will only ever be 21 million Bitcoins created. We will talk about the process by which they are created very shortly.

BITCOIN - MINING

MM: [Slide 8] The next thing we need to talk about is mining. I said a moment ago, the Bitcoin network consists of a network of computers which are called miners. Miners are basically computers that want to add the next block to the longest version of the blockchain. Why do they want to add a block to the blockchain? Because, in exchange, they get paid a fee. The fee really consists of two components. One is that for every transaction that is added to the blockchain, a very small transaction fee is paid by the sender for blockchain. So, the sum of all those fees is received by the miner that adds the block to the blockchain. The second component of the fee is that every time a new block is added to the Bitcoin blockchain a new amount of Bitcoin is generated. The amount that is generated to each new block changes over time. Originally, when Bitcoin started, it was 50 Bitcoins per new block. Every 210,000 blocks, which is basically every four years, the amount issued halves, so it halved from 50 to 25, then to 12.5. Currently, it is 6.25. So, every new block that is added generates a new 6.25 Bitcoins. In around 2024 it will halve again. Those are the fees that the miners receive when they add a block to the chain. We will talk about how that happens in a moment.

A way that happens is basically every proposed transaction to be added to the blockchain goes into a pool. The miners pick it from that pool as many transactions as they can fit into a block and want to get as many transactions in as they can because the more they fit the more transaction fees they get. Once they have compiled those transactions, they set about trying to create a valid block – we will talk about what is required for that block to be valid.

[Slide 9] What the miners are doing…You always hear the miners are running these complex calculations. But the complex calculations they are running is a process called 'hashing' which is the algorithmic encryption of data. I should not say encryption actually, it is an algorithmic process applied to data which gives the data a digital fingerprint. It is different from encryption because encryption is a situation where you can decrypt the data, you can work backwards: someone sends you an encrypted message, you decrypt it, and you can then read the message. Hashing does not work that way. Hashing only works one way. You can code it and you can find out what the resulting hash of that input information was, but you cannot work backwards.

These are the of key elements of it:

- It will take an input of any size. You can put any size information into this hash algorithm. When I say algorithm, it is a formula that is very complicated. Put an input of any size or any content - you can put words and numbers, you can quote the Bible, you could put a whole computer program in there, and we are going to come to that - anything. The hashing algorithm will then spit out a number that is of a fixed size. I come to the next point…

- Deterministic which means that if you put the same input into the hash algorithm you will get the same number out: you will always get the same number out. That is why it is sort of a signature for that input data.

- It also has the characteristic where if you make a very small chain, any change in the input data, the output hash will be completely different, it will completely scramble the numbers.

- Finally, it has this important thing that I mentioned a moment ago, where it is a one-way process. You cannot if you have got that output hash, you cannot mathematically work backwards from that to figure out what the input number was. You can only go from a number forward through the hash.

I should say in terms of sort of "cracking" this, you can never work backwards from the output to the input. The only way you could figure out the right input that gives the output when put through the hash algorithm is to try every combination of inputs, you would have to try every alteration to get the output. The way Bitcoin's security works is that that is impractical, from a timing perspective, when you compare the computer power of an attacker of the network versus the rest of the power in the network - we will talk about that in a second.

BITCOIN - HASHING

MM: This hashing idea comes up all the time in cryptocurrency and the one-way aspect of it is fundamentally important in a lot of cryptocurrency things. It comes up in, as I say, the format of a block. The first thing in the format of a block is to hash of the previous block. So, whatever the previous block was, you put an identifying number which is derived from hashing, running that whole block's information through the hash algorithm to spit out a number. I will show you what this looks like in a minute.

It is also used in the process of validating the block via the nonce - which I am going to talk about, and some other things.

At this point, I thought it might just help explain this hashing thing to see it work.

[Moves to web browser] The algorithm Bitcoin uses is SHA256. It is just a particular formula that does this process that we are talking about. There are others, as you can see on here. Basically, if I put in a particular input and press hash you see you get that sort of scramble of numbers and letters. If I change that just a small bit, then press hash, the number that results is completely different. You cannot sort of guess what the input was from the output. It is completely unconnected. The way a block looks conceptually, not literally, but would be something like this: [types on screen] “The hash of the previous block was bla bla bla. Michael sent one Bitcoin to Salwa and paid a fee of 0.001 BTC. Pay the minor 6.25 BTC. The nonce is one.” Then you hash that.

What the problem is that the computers are trying to solve, to add a valid new block is that the hash of the block needs to be below a particular number, called the difficulty level. So, this output in the form of numbers and letters is just a simplified way of writing a really, really big number: the output of the hash is just a number. This is a simple way of looking at it. So, the miners are trying to come up with a block that has a hash that is below a particular number. What they are doing when they are mining, the process that they are doing, is constructing the blocks. They pick up the transactions that they want to put in the block. Then they are just trying a bunch of different combinations of nonces that say “Our hash has to start with the letter A. Let's nonce that hash. That didn't work, let's change it to three. Hash. No, we got an E.” You keep doing that until you get an A. That is how you add a valid block to the blockchain. All the other computers on the network can do the same thing to check that your block is valid. They can put the same input into the hash algorithm and, if it spits out a valid answer, everyone on the network says that is a valid block added to the blockchain.

If I go back to our slides [Slide 10]. That is the hashing process. That is how a block gets added. I will talk about sort of what that does systemically in a second.

Another important part to understand about how the Bitcoin process works is the authorisation of transactions. So that bit in the block that says “The transactions with this have a lot going on there”. Most of the times when you have a password for something there is a centralised password database. Like your login code for Gmail, Gmail knows your password to log into Gmail. That is how they test whether you put the right password in. What that means is that if Google gets hacked, your Gmail password can get released to the world, and that happens sometimes. Bitcoin does not work that way. Bitcoin works by way of a password that can be verified without knowing what the password is. I can check that you have given me a valid password without having to know what your password was. That is called a private key. The private key is, again, basically a really, really, really big number. It is the thing that you keep secret because it is the way that you can control your Bitcoin in the network. An analogy that gets used, Bitcoin addresses being like email addresses, that is the thing you tell the public, and private keys are like your password to login to access your email.

Practically, they are maintained in what is called a wallet. It is very confusing terminology. Wallet is not the best term, I don't think, because what do you put in a wallet? Your money,

right? You do not store your Bitcoin in a wallet. What is stored in the wallet is the key, the really, really big, long number. The wallet interacts with the network to use that key to sign transactions to get them on the network.
Part of the way the process is able to verify transactions without knowing your password is what is called a public key. A public key is, again, mathematically derived from the private key. You put the private key into another complex algorithm, this one having something to do with elliptical curve math, which we won't go into, and it spits out a public key. Basically, again, it is one of those processes that only goes one way. You can, if you have the right private key, derive the public key, you cannot figure out the private key from the public. That public key is, again, through a similar mathematical process translated into an address. The public key is hashed into an address and that is like your email address. So, when you want someone to send you Bitcoin, you send it to that address and that address is mathematically derived from your private key so that when you try to spend it later, transfer it someone else, you need to have your private key to unlock it. That process of locking Bitcoin via your private key involves the creation of a signature, which we do not need to dwell on too much.

[Slide 11] As I said at the start, miners are trying to add blocks to the longest chain. The reason why they want to add blocks to the longest chain is because the longest chain is the valid chain. There could be other competing versions of the blockchain that are shorter than the longest one but none of the computers on the network will care about the shorter chain. You can see from the way the block is created, the blockchain is of the present time. The next block could be anything, it could have all sorts of different transactions. There could be, in theory, a point where two computers happen to solve the problem that we just talked about at the same time with different blocks. So you have got two competing versions of the blockchain. But the way that works itself out is, after a few blocks, one of those competing versions of the chain will end up being longer than the other. Whichever one is longest, that is the one that miners want to work on because that is the one where they can add a new block that says "Pay me some Bitcoin". That is what I mean by forks in the chain.

The second point up there [on the slide] is this idea that the further back in the blockchain your transaction is the more secure it is, because if someone wants to go back and rewrite history, say they send a Bitcoin to Salwa and then said "No, I don't like Salwa anymore. Sorry, Salwa. I'm sending it to Tamara instead." I am going back in the blockchain and rewrite that block. You could write a different valid block that instead of saying "Send it to Salwa" or "Send it to Tamara". You could spend time and figure out your nonce and get that working, you could create a valid block. The problem is, while you were doing that on this earlier version of the blockchain, all the other computers are adding to the real blockchain, the longest blockchain. For you to get them to switch over to your false chain, you need to catch up. The problem is that the time it takes to run that process to create a valid block just means that you will not be able to keep up. The computer power devoted to the rest of it will stop you from creating your competing wrong chain.

[Slide 12] This [quote on the slide] comes from the Bitcoin whitepaper. What they are talking about in the Bitcoin whitepaper is "We are proposing a solution to the double-spending problem…", it is a problem of like competing ledgers, "…using a peer-to-peer network." A bunch of computers around the world. "The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work." Proof-of-work is the fact that you need to change the nonce lots of times to get a block that is valid. That is the work that they are doing. It really is work, the computers require power. That is your cost as a miner, the cost of powering the computers. "The longest chain not only serves as proof of the sequence of events…" that is, they are chained together in the way that we talked about, "…but proof that it came from the largest pool of CPU power. As long as the majority of CPU power is controlled by nodes that are not cooperating to attack the network, they will generate the longest chain and outpace the attackers." In a nutshell, that is what Bitcoin is and how it works to overcome those problems we were talking about at the start.

BITCOIN – LEGAL ISSUES

MM: [Slide 13] To briefly touch on some legal issues about just Bitcoin itself. One thing I want to talk about briefly is, is it a currency? Salwa is going to talk about is it property? It depends on what you mean by currency. The only point I wanted to make about this is that in our *Currency Act* there is a provision. The *Currency Act* says the monetary unit of Australia is the Australian Dollar. It goes on to say every transaction relating to money shall, unless it is done according to the currency of some country other than Australia, be done in the currency of Australia. If you are going to do a transaction that involves paying money, if it is not in some other country's currency, it has got to be in Australian Dollars.

The phrase "the currency of some other some country other than Australia" I think is interesting. In the context where, as you are probably aware, in I think it was last year, El Salvador in fact made Bitcoin legal tender. I do not know whether that makes it the currency of some other country. That is, it is just legal tender in El Salvador. There are other things that are legal tender in El Salvador, like the US Dollar. Maybe *the* currency of some other countries is talking about an exclusive currency but I don't know. Maybe if you have an expert on El Salvador law they might tell you something about what the currency of El Salvador is. Even if it would fit within that…I am certainly not suggesting that that would mean that Bitcoin is legal tender. This is not the section that makes coins and banknotes legal tender, there is a different section that does that. I am not suggesting that you can go around paying your creditors with Bitcoin, unless they have agreed to it. But it might be read as giving, if you could fit the El Salvador connection into the currency of some country other than Australia, it might give it some sort of status as money which might be relevant for some legal purposes. You can think, for example, in the litigation context, there is a fundamental difference between money claim and debt claim, and the claim for return of some property or to have property transferred, including mitigation and things like that. It might be that that has some effect in relation to that. I suspect, probably the better reading of it is just that where it says unless it is made in the currency of some other country, what it is saying is, if transactions are in some other country's currency, they are not affected by this. It is not really saying anything about those transactions, but who knows. That was the point of our currency. Salwa is going to talk to you about property.

IS BITCOIN PROPERTY?

Salwa Marsh (SM): [Slide 14] This is another characterisation issue that is emerging that I think is a really important one. I am sure many of you will know that the question as to whether cryptocurrency is property has received some limited international consideration, although nothing in Australia yet. I have listed the key cases up there [on the slide]. I encourage you to read them if you are interested. But if you are only going to read one *Ruscoe* [*v Cryptopia Ltd (in Liquidation)* [2020] NZHC 728] is the one to read. But I will work through the prior cases just for some context.

Quoine [*Pte Ltd v B2C2 Ltd* [2020] SQCA(I)2] was a Singaporean case. There was some analysis as to the propriety nature of cryptocurrency at first instance but on appeal the court did not think that it was determinative of the issue and so they sidestepped that tricky issue. They have left us all wondering.

In the UK, *AA v Persons Unknown* [2020] 4 WLR 35 considered that question as well but in a really specific context, which was whether cryptocurrency was property for the purposes of awarding a proprietary injunction. The characterisation of cryptocurrency as property did not receive a great deal of consideration in the judgment. It is one of those judgments which decides a pretty significant thing but does so at a reasonably high level and it has been criticised by some of the commentators for having been a reasonably high-level analysis. This is why I say if you are going to read one case it is *Ruscoe v Cryptopia*. It is a New Zealand High Court case and it is the most recent, the most comprehensive and the most authoritative case. I think it would be fair to say that it would be pretty persuasive at least in Australia

Ruscoe v Cryptopia

SM: In that case, there were a variety of crypto currencies in issue but the case was in fact about a cryptocurrency exchange called Cryptopedia which went into liquidation following a number of hacks and a value of NZ$30 million was stolen. You will see in a lot of the litigation internationally and a lot of the cases that really make the news, security issues emerge, hacks emerge, and then we have questions as to bankruptcies and liquidation. This is really the context where a lot of these issues are being thrashed out.

There were about 800,000 account holders who had a positive cryptocurrency balance with the exchange at the time of the liquidation, so lots of people lost out. The liquidators in this case applied for direction as to whether the cryptocurrency was an asset for the purposes of the New Zealand *Companies Act* or common law because their interest was whether cryptocurrency could be held on trust, and whether in fact, in the circumstances of that case, the trust was made out. The dispute here was really between Cryptopedia's creditors and shareholders and account holders. The account holders submitted that the cryptocurrencies were intangible personal property. The liquidators and creditors said "no", they disagreed with that characterisation. The reason they did so is obviously because there are the implications for the distributions in the liquidation.

In that case, Justice Gendall…I think something that is quite important is the context of this case was that it was not a dispute between participants in a cryptocurrency system but creditors and account holders who were interacting with a company which was operating the exchange. First up, that is a particularly unique context. Ultimately, the Court held that cryptocurrencies were digital assets and they were a form of property capable of being held on trust. The question was approached at length in that case, initially, by way of analogy. A diverse array of assets were identified as potentially analogous and those were choices in action, non-enforceable debt claim, payments through banking systems, copyright, shares, licenses, exemptions, quotas, and a trustees right of indemnity. These are all sorts of amorphous concepts that in some way could be seen to be analogous. More importantly, before in the theory of property, which was stepped out in a classic articulation by Lord Wilberforce in *National Provincial Bank v Ainsworth* were analysed. Those four indicia are obviously not discrete, there is some overlap between them, but broadly speaking, they are that 1) there is an identifiable subject matter, 2) that it is identifiable by third parties, 3) that it is capable of assumption or being acquired by third parties and 4) that there is a degree of permanence or stability.

To step through each of those quite briefly, the first thing, the identifiable subject matter is really the public key identified by way of the public keys. The fact that it will be identifiable by third parties was said to be the operation of the private key. This idea of assumption by third parties was determined by reference to the existence of active trading markets that we are all familiar with. It was said that in terms of the degree of permanence and stability, the risk associated with cryptocurrency was comparable to any other form of property.

The judgment goes on to analyse some of the arguments against the characterisation of cryptocurrency as property. One of the key arguments is that it is not tangible property and it is not really a chosen action. But the court said that was a red herring, that it does not fit within the existing categories we are all comfortable with is not determinative of the issue.

The next argument against that characterisation of cryptocurrencies as property is this idea that information cannot be property. In that case, it was said that it is wrong to regard cryptocurrency as mere information, the whole purpose behind cryptocurrencies is to create an item of tribal value, not simply to record that it exists.

The final point dealt with by the court was this idea that if we legitimise cryptocurrency as property we are somehow facilitating criminal activity or we are legitimising something that should be seen as illegitimate. That was discredited because of the increasing mainstream and legitimate use of cryptocurrency.

The result of this case is an important one because, as we know, property is a foundational concept in bankruptcy, insolvency, succession, restitution, tracing, breaches of trust. In commercial law more generally, there are lots of implications as to that characterisation. More and more international jurisdictions have been legislating the status of cryptocurrency as property and I suspect we will keep seeing more of that.

I will hand back over to Michael who is going to start talking about some other cryptocurrencies. We have focused on Bitcoin so far but that is just the original gangster.

OTHER CRYPTOCURRENCIES

MM: [Slide 15] As I said, the way we are trying to break this up is to compare and contrast. There are some obvious limitations to Bitcoin. The first is the block size and the fact that a new block gets added on average every ten minutes means that the transaction volume is limited, you can only fit so much in so many blocks. The effect is that the maximum transaction volume on Bitcoin is around 3-8 transactions per second. Compare that to Visa, which is about 1700 per second. So, it is completely not scalable as a replacement for buying coffees and things like that. The things we are talking about are ways to try and develop the technology to maybe come into that sphere.

The second limitation is the proof-of-work mining, in the way I have talked about before, uses a lot of energy. That has its downsides.

The third thing is that it is fairly rudimentary. As I said, it is just a list of the movement of Bitcoin, it does not do anything more jazzy than that. Although there is a lot to create the list, in the decentralised way we talked about, it does not do much more than that.

[Slide 16] Newer cryptocurrencies diverged from this. One of the things that you will see in various cryptocurrencies is the introduction of different layers of blockchain. To help the scaling problem, what some other cryptocurrencies, or cryptocurrency networks, will do is have a base layer blockchain which is the big, secure one, and then you have less secure other chains where more transactions can be done. Effectively, what the base chain does is record the net effect of what happens in the other chains. So, you get sort of less security in one layer, but the capacity to handle greater volume.

Proof-of-stake mining. What we talked about with Bitcoin is proof-of-work mining, proof-of-stake does not work by having people go through the rigmarole of trying a lot of different nonces. Instead, the way that the person that gets to add to the blockchain is selected is by reference to them putting up a stake, that is an amount of the cryptocurrency related to that network. The effect of that is obviously to use less energy because you do not have all the computer resources competing to just add one block, you can have some of them doing something on one layer and another doing something on another layer. The person who stakes their cryptocurrency would typically get a return on that cryptocurrency as a share effectively of the transaction fees. So, it creates yield generating opportunities for investors. But, it compromises the decentralisation idea because a big part of the Bitcoin idea is that to mess with the network, you need to have an inordinate amount of computer power, which would cost an inordinate amount of money to create. In proof-of-stake cryptos, you just need the most of the crypto – we will talk in a moment about the ways that different cryptos are issued. I told you the way Bitcoin organically comes out every block, other cryptocurrencies do not work like that. They just get all issued at the start, like an IPO, called an ICO, initial coin offering.

SMART CONTRACTS

MM: [Slide 17] Another development to the rudimentary Bitcoin is smart contracts. A smart contract is a computer code that is on the blockchain of the particular cryptocurrency network that does stuff – we will talk about some things that some smart contracts do.

I have put there [on the slide], query whether they are smart and query whether they are contracts.

As to smart, the types of contracts we are talking about here are computer programs. All that they can do is operate in the "if this, then that" kind of way of doing things. That works really well for a whole bunch of really simple transactions that take place every day, think of every share trading on the ASX, that is a simple transaction that you could do with this "if this, then that" sort of way.

It really brings into focus, something that we, particularly litigation was, do not necessarily think about that much, which is that all the uncertainty that we have in our legal system is in some ways beneficial, it is a feature, not a bug. If you were to do a transaction that you would do in a typical contract, you have to work out every possible eventuality and provide for it in the program. That would be really expensive to do in lots of transactions. Most transactions, you do not want to worry about that. Let's just put a clause in that says, "the parties will act in good faith". If that guy is a jerk, we can have a fight about it and a court will decide if they breach the obligation. It is intentionally vague. You cannot really do that with cryptocurrencies. Although, I will come to a thing that might provide a way into that.

As to contracts, they are certainly not contracts in the sense of creating obligations, or at least that seems to be the way at the moment. That is, most contracts we think about are ones where someone has to do something in the future. But that is not the limit of the legal concept of a contract. We can have contracts that do not have future obligations, where the parties obligations are executed, they are performed at the time. A good example that is given by Professor Lawrence Lessig at Harvard, who has really interesting things to say about this sort of stuff, is a vending machine. You put money in, you get your can of coke transaction. That has no future obligations. He also makes the point that with your vending machine contract, the status of the contract has all sorts of extra consequences. There are implied terms in that contract. If the coke has a snail in it, or whatever, and you die, then that is something you can sue them about. There are all sorts of legal things that come along with that contract even though it does not have future obligations. So, the fact that they do not have future obligations does not rule them out.

One thing that does seem difficult for me is that in order to enforce rights you need to have a party that you can sue to do it. In a lot of crypto contexts you just will not know or have the capacity to identify who your counterparty is. In a sense, the way most of them work is that they are kind of self-executing, they do not need anyone's cooperation. Everyone does what they need to do at the start and the computer just decides how to allocate things.

DECENTRALISED APPS

MM: [Slide 18] That brings us to the world of decentralised apps, or "dapps", which are applications that run smart contracts, they are interfaces. One type of dapp is a decentralised exchange, or a DEX. That is an app that lets you trade crypto within a network. The smart contract will say "If you give me one Ethereum I will give you 100 Dogecoin, or whatever."

There are a couple of different ways those decentralised exchanges can work. They can either be an audible kind of thing where all they are doing is matching up someone who has some Bitcoin and someone who has some Ethereum and wants to swap them. Or they can work in a market maker way where a big institution says "I will run this kind of exchange. People can lodge Bitcoin, or crypto that they do not need right now and want to earn some income, and then give it to me, the market maker. And that will give me enough liquidity so that I can then do these swaps. I'll give it back to them at the end. But in the meantime, I can do these swaps." So you get decentralised exchanges in various ways. Those are fundamentally different from the kind of exchange that Salwa was talking about in that New

Zealand case which is a centralised exchange, that is not on a chain, it is real people, a real company doing things.

DEFI

MM: Another form of dapp is decentralised finance, DeFI, or another category of dapp. This is the world of lending crypto for interest. You can take your Australian Dollars and buy a cryptocurrency that gets you into a particular network. Once you are in that network you can lend that to somebody else, they have to pay interest. They usually have to put up security so that if they do not pay the contract executes itself by giving you their security instead of what they should have paid you back.

ORACLES

MM: Another kind of app I wanted to talk about is an Oracle. These are really interesting. At the moment, we are talking about magic internet tokens. They do have value on the market but people unsurprisingly are not that excited about say earning a yield in Ethereum, or Polkadot, or Kuduna, or whatever. They would rather earn dollars. Going beyond that, you would like to have a way for your smart contract to be able to interact with real world events. It would be cool to be able to have a smart contract where the outcome depends on say the price of the ASX200, or whatever that index is. You might want to have real world data about temperatures, anything, any real world data. What an Oracle is intended to do is, in a decentralised way, bring that outside information into the chain so that it can be used as part of a smart contract so that you can enter into a smart contract that is effectively an equivalent to a derivative.

You can also use this Oracle real world connection to create things like contracts of insurance. If you gave me an example where say all the farmers decided to put in X number of tokens into this smart contract and the smart contract says "If the Oracle tells me that there's been no rain in Queensland for six months, then I'll pay the Queensland people from this smart insurance contract." I don't think anyone is doing that yet but that is the idea. Oracles bring in information and they do it in a decentralised way. Importantly, you cannot have the Oracle be a central authority because then if you want to dodge your contract obligation you pay off the central authority to give wrong information to the chain. It works in a decentralised way, like the way we were talking about before.

TOKENS

MM: [Slide 19] Tokens on other cryptocurrency networks. Bitcoin just has Bitcoin as its token. Other networks have a whole bunch of different tokens and some of them within the one network have different tokens. So, you will have say on the Polkadot network Dot is the native currency, it is that thing that you have to get to be able to do anything on that network. But once you are on that network you can swap your Dot for something else, some other app's token that is on that platform. That means that once you have built the platform, the network, other people can come in and build on that network. Say you decided "I am going to run that insurance contract, that's going to be my business", you could build that on someone else's network and issue your own tokens to be in a currency for that dealing.

As I mentioned before, the issuance methodology differs from Bitcoin. Typically, they are often issued in the form of like an ICO. That brings all sorts of problems with it because the promoters of the network will typically reserve themselves a portion, like an IPO. They will reserve themselves a portion of the equity of the network which starts to make these other cryptocurrencies look a bit more like the kind of thing that regulators like ASIC and people like that are interested in, more than Bitcoin would.

NON-FUNGIBLE TOKENS (NFTs)

MM: Another variation on the token idea is the non-fungible token. Most tokens are like one Bitcoin is like any other Bitcoin, but NFTs are ones where you have something special about the token. You will have seen probably stuff about these artwork NFTs going for ridiculous prices, in a sense art goes for ridiculous prices so that is not particularly unique, but it does have some potentially interesting applications, particularly this stuff like digital rights management. So, say you are Taylor Swift and you say "I don't want to use Spotify or anything like that anymore. My new album is available on a smart contract. Every time you want to listen to one of my songs the smart contract will dock you five tokens, or whatever." That is how you could use NFTs to sidestep the existing providers of have that kind of information.

They are also used in games but I don't think that is particularly relevant for us.

STABLE COINS

MM: Stable coins. When you are doing DeFi and you want to borrow money and invest money, stable coins are tokens on a network that are designed to keep the same value as a fiat currency. They are basically a way of having an equivalent of your real money in the magic network. That is particularly important for DeFi because it means that instead of earning your interest denominated in Bitcoin, or Ethereum, or whatever, you earn it in US Dollars or Australian Dollars.

Stable coins have been in the news lately. There are different ways of doing them. One way is, again, a centralised way. An institution says "every time you give me money, I'm going to put that amount of money away in a bank account and issue tokens. I will only issue tokens to the value of the money. So the fact that I've got the money stashed away means that the token should trade at the value of the stuff we've got stashed away." The problem with the stashing away and the trusting of the person to stash away, also just the practicalities of the stashing away…If you are stashing away $100 million, you cannot just put it in a bank account, you need to invest it because if you put it all in a bank account you are just a creditor of the bank and you might rather be a creditor of someone else for $100 million. So, there are all sorts of controversies around centralised stable coins because nobody is sure about what assets they have backing them. Again, probably screams out for some kind of prudential kind of regulation in the future.

Another way of doing stable coins is algorithmic, which is where some market maker again do the arbitrage so that the token stays at the price of the currency that it is meant to be fixed to. The stable coin that blew up recently was one of those algorithmic ones and that is what is going on.

CBDCs

MM: Finally, CBDCs, central bank digital currencies. This is the idea that this technology that we are talking about is being considered to be adopted by countries as their official currency. China, for example, is considering using this technology to do a CBDC. Obviously, they would be completely different from Bitcoin in the sense that it would be centralised. It would have to be centralised, but the point is just to use some of the technology to do these things.

Imagine you are the ATO, think about how much the ATO hates cash. If every transaction in Australian Dollars was in the Australian CBDC the ATO could definitively find out how much tax you owe and it could probably make it a condition of the contract that every time someone transfers the CBDC they pay the tax so that tax collection goes out the window.

These are probably sometime off in the future, I would have said, but they are being discussed.

CAPITAL RAISING BY CRYPTOCURRENCY

MM: [Slide 20] I want to give an example of a capital raising via a cryptocurrency network very briefly, and then I will hand back over Salwa.

I should say, I know we are running short on time, if anyone in person needs to leave by all means and online.

An example of capital raising on one of these cryptocurrency networks. Polkadot is a network, the currency on it is called Dot and it is a blockchain of blockchains. It is a blockchain in that itself links up to 100 parachains. The idea here is that Polkadot is the environment in which people will compete to get a parachain to be able to run their particular program that they want to run their dapp. The way that you compete for a slot on the parachain is by way of an auction. The people who want a slot on the parachain need to get people to bond their Dot, their tokens in that currency, in support of their campaign for winning the next auction, and there is an auction every X days. What happens is, if you think "Oh, that's going to be a good app, that's going to make lots of money. I'll pledge my Dots to support that app." The way the transaction usually works is that in exchange for that…that ends up getting locked away for the duration of their occupation of the parachain but in exchange you will get the new token that this new promoter is going to be issuing when they set up their thing on the parachain. You can see how it is sort of an equity swap. In a sense, you have to move your money into one token, you then have to put that token into a smart contract that will have the effect that you get some different token proportional to the amount that you put in.

The point of this is to show some of the ways these things can be used to do stuff that we do already in our traditional legal contracts but in a slightly different way.

On that note, Salwa is going to talk about what are the big bad regulators would like to do with these wonderful technologies.

CRYPTOCURRENCY REGULATION IN AUSTRALIA

SM: [Slide 21] One of the key questions for us today is about regulation and typically, what the need for regulation is. There are some pretty obvious answers to that.

Firstly, consumer protection and investor protection looms very large. I have a great statistic for you. The Federal Trade Commission in the US reported that American consumers lost more than US$80 million on cryptocurrency investment scams between October 2020 and March 2021, that is just six months and ten times the amount lost in that six months in the prior year. Particularly interesting is that US$2 million were lost to scammers specifically tells us a bit about the scale and nature of the problem from a consumer investor protection perspective.

The concern as well extends to is the volatile nature of cryptocurrency, issues with transparency, issues with valuation, custody and also liquidity. The liquidity concerns you really want to know is the really classic examples of what happens when things go wrong. Probably the best and the most well-known example is the Mt. Gox example, a Japanese Bitcoin exchange, which at its height was the world's largest Bitcoin market but nonetheless had notorious operational issues and security issues which ultimately led to it filing for bankruptcy because it was just simply unable to meet payment obligations. You may have heard of somebody doing historic credit litigation that follows that collapse.

You could add that there are a lot of unethical practices, illegal schemes, scams, in addition to the well-known nexus between cryptocurrency and crime. There are lots of examples of cryptocurrency being used for money laundering, for trading goods, and also the UK case I referred to earlier had a person unknown.

I think there is a general acceptance that from a regulatory perspective, regulation from a tax perspective, money laundering perspective and counterterrorism financing perspective, it is middle of the bar. There are, of course, other regulatory goals, which target a lot of those issues already raised and I will focus on those. But, as is well-known, regulation of cryptocurrency is really difficult, there are a number of niche factors of cryptocurrencies that make regulation hard which in some ways make cryptocurrencies attractive.

There is the cross-border element. The fact there is a significant amount of decentralisation. You are dealing with anonymity and unknow entities. It is really hard for regulators to identify the respondent or defendant.

Also, the fact that, I think it is probably fair to say, that existing frameworks have not always been, obviously, not designed to deal with cryptocurrency, but they have not really been updated with new ways to deal with cryptocurrency. I would like to talk about these frameworks from an Australian perspective. I think you will see that there is some discomfort as to how they deal with cryptocurrency.

There are two key questions here. The first is, who regulates? Which is a big question in Australia.

The second question, which interacts with the first in a really interesting way, is, what is regulated?

I will give you a bit of an indication of both of those.

As to the question of who regulates from this consumer protection and investor protection perspective, that depends very much on the relevant statutory regime that is in place. There are a suite of obligations that fall under ASIC's standard and those are the obligations that are tied to the *Corporations Act*, usually for the purposes of the licensee, and the *ASIC Act* which is not really targeted at consumer protection. In a sense, it is the ASIC regime, we will call it this for convenience, which encompasses both the *Corporations Act* and the *ASIC Act* obligations.

Then the ACCC regime is targeted at consumer and competition law. But for present purposes, they are the obligations you find relevant to consumer law which are contained in the *Competition and Consumer Act*, I will call that the ACCC regime for convenience.

Now, which of the regimes you fall under is actually a pretty difficult question and that question requires you to identify what are all the regulatory subjects, what it is that is being regulated? That is quite a difficult question to answer generally depending on the nature of business. The regulatory subject could be the actual cryptocurrency, it could also be an exchange or the company that runs an exchange. It could be a network or a system. Or it could be other technology that is associated with cryptocurrency, wallets, apps, or other platforms by which you can interact with cryptocurrency and cryptocurrency systems and networks. Really, the question we have to answers is, what thing is being regulated? As a business owner or as somebody who plays in the space, that is an important question, because if you identify the thing you can identify the regime.

The critical question for present purposes is whether there is a financial product at play. That is, of course, a term used in the *Corporations Act* and the *ASIC Act*. If there is a financial product at play, there are specific obligations that follow from that conclusion. If there is no financial product, probably the fallback position is ACCC regulation under the Australian consumer law and the *Australian Competition Act* as well.

Many commentators have suggested that ASIC is, of course, the natural regulator of cryptocurrency. That is consistent with the *ASIC Act* which provides that some of the goals of ASIC is to strive to regulate financial systems, so ASIC is the natural and obvious regulator. But, as is clear, it is necessary for the regulatory subject to fall within that regime, so that is one of the questions you have got to ask.

In some ways, there are some obligations that any business will owe irrespective of whether they are regulated by the ASIC or ACCC regime. Those sorts of obligations are mirror obligations, such as misleading and deceptive conduct, unconscionable conduct, there are mirror obligations across those regimes. But, of course, there are specific obligations which fall under the ASIC regime which are particularly relevant for present purposes. If there is a financial product, there is probably an obligation to hold a financial services licence. There is not a complex regime or relevant section but the upshot is, making to market a financial product, or dealing with a financial product, will require a financial services license. I refer you to s 911A(1), s 761A and 776A of the *Corporations Act* to look at the relevant provisions there. Dealing in a financial product would include acquiring, disposing or issuing under s 766C. I think that is probably likely to encompass things like running an exchange and initial coin offerings. Equally, making to market would be another way through and the definition in the relevant section is s 766D of the Act. I think when making to market a financial product is likely to encompass cryptocurrency exchanges.

I think ultimately, if you find yourself regulated by those regimes, the key takeaway is you need to be licenced and there are a number of obligations that come with being licenced which are contained in the *Corporations Act*. Also, a particularly big one is s 9128 of the *ASIC Act* which is that license holders do that is necessary to ensure financial services are provided efficiently, honestly and fairly, which would be a wide-ranging obligation. Of course, then there would be difficulty that the failure to comply with those obligations can lead to suspension or termination of a licence. So that is something you need to be aware of.

Another thing to bear in mind is that ASIC has issued a guidance note, which is number 225, about crypto assets. It is an interesting read. What it seems to accept is that some crypto assets and ICOs can be financial products. It also accepts not all of the will be. What that hits home is that you do need to go through the process of identifying whether your business is caught by the regime.

WHAT IS A FINANCIAL PRODUCT UNDER THE ASIC AND CORPORATIONS ACTS?

SM: This is a good opportunity to consider what is financial product. That is not an easy question to answer. The approach that I have taken is to look at the uniform core of that definition in both the *Corporations Act* and the *ASIC Act*. Both those acts define a financial product relatively in the same way, for a number of purposes. There are, of course, extremities in terms of the way each act applies. If you picture a Venn diagram, there is the *Corporations Act* and the *ASIC Act* and there are core of things that are financial products in both and there are inclusions and exclusions in the perimeters but I won't deal with those for present purposes. But I will deal with subsection one of both definitions.

There is a lot of literature out there about regulation of cryptocurrency as managed investment schemes, securities and derivatives. That is another way home to attract regulatory obligations but for present purposes, I am going to focus on the key definition, the core definition of a financial product.

[Slide 23] You will see here [on the slide], I have extracted the key definition. You will see that in both s 763A of the *Corporations Act* and 12BAA of the *ASIC Act* it is framed in the same way, which is to say that a financial product is a facility through which, or through the acquisition of which, a person does one or more of the enumerated actions in the subsection of each. We will go through each of those. Before we do, there are important thresholds.

[Slide 24] Interestingly "facility" is not defined in the *ASIC Act*. It is defined in the *Corporations Act*. The *ASIC Act* tells us that, for most purposes, a financial product under the *Corporations Act* is also a financial product under the *ASIC Act*. So, I think there are good arguments that we can incorporate the *Corporations Act* definition into the *ASIC Act*. If you accept that proposition, you will see that the threshold question as to whether there is a facility, by pointing to one of three things. Firstly, intangible property - this is where the characterisation of cryptocurrency as property looms large and particularly important. Secondly, an arrangement – I think that is a broad word and one that theoretically could encompass a number of things we have been talking about. It seems to be pretty wide and seems to have application of a number of permissioned or centralised cryptocurrency structures but also arguably unpermissioned or decentralised structures, because of the requirement consensus. Having said that, there is an obvious regulatory difficulty in terms of enforcement when you have a decentralised or unpermissioned structure. The fact that those structures might fall within the definition like 'no practical utility' if there is no clear respondent or defendant. Nonetheless, I think that is a pretty broad, a pretty poorly framed way through to bring any number of structures within the definition of facility. The third meaning could be a combination of intangible property or arrangement. I think it is clear to say nonetheless, that is a pretty broad definition and could capture any number of structures.

[Slide 25] Assuming you have got a facility, then you need to identify whether it falls within one of the three enumerated acts within subsection one on each of those definitions.

The first is, making a financial investment. Interestingly, this definition, in a sense, requires an investor to give money or money's worth to another person and for any of the enumerated acts to apply. I think for present purposes the thing that is interesting is an investor needs to give money or money's worth to someone else to do something with. In that sense, this definition is probably more likely to apply to permissions or centralised exchanges. This limb has been said to potentially be a way around some of the concerns about whether managed investment schemes apply to cryptocurrency because there is no requirements of pooling of assets. This is probably one of the limbs we should watch.

[Slide 26] Secondly, of course, is managing financial risk, which applies a little bit less obviously to cryptocurrency. Michael referred earlier to the possibility of smart insurance contracts and I think there is probably an argument that that sort of a structure would fit under this limb. Again, something to watch.

[Slide 27] Finally, they mention non-cash payments. In a lot of the literature this seems to be the big limb that everyone sees as the one to keep an eye on. Orthodox examples of non-cash payments are things like cheque accounts, traveller's cheques, stored value card. You can see that there is a bit of an analogy that can be made to cryptocurrency and so while there is a debate as to whether it would strictly apply to cryptocurrency, which is a double stored currency but also facilitates the transfer of valuable intangible property is nonetheless I think could very well be the basis upon which cryptocurrency is more within the ASIC regime. Of course, there is no case law for any of this, it is necessary to read the confirmed principles as to whether the product in question falls within any of these definitions.

I hoped this gives a bit of flavour for the sorts of things to keep an eye out for. One other thing to raise is that there is a bit of literature about whether cryptocurrencies are managed investment schemes. There is a recent case in New South Wales which is the *Commissioner of Police v Bigatton* [2020] NSWSC 245 where there was no real analysis as to whether cryptocurrency fell within the meaning of a managed investment scheme. But, that case was a proceeds of crime case so there is a requirement to establish whether there is a reasonable suspicion for the purpose of that act and the court accepted that cryptocurrencies might be a managed investment scheme, without any real analysis, but nonetheless pretty lengthy.

We do not have time to talk about initial coin offerings, which makes me sad.

MM: I am sure everyone here is sad.

CRYPTOCURRENCY EXCHANGES AND LEGAL ISSUES

MM: [Slide 28] We were going to talk briefly about exchanges but we have sort of spoken about that along the way. Exchanges are the way you get crypto. One way you could get crypto is just asking a friend to send it to you, you don't have to have anything official. The other way is a decentralised exchange, a DEX, the one that runs on the chain, or a centralised exchange, which is a company where you give them money, and they will transfer you different types of cryptocurrencies in exchange for the money.

It is an obvious focus for regulation because it is the onramp that you can regulate quite easily. The regulation that exists at the moment includes the usual KYC things. So, if you want to open an account with a centralised exchange, they will ask for a copy of your passport and your license and all that sort of stuff. It is like opening a bank account or a share trading account.

As we touched on already, it creates very interesting questions about proprietary interests in the event of insolvency: are the currencies that you have sitting on the exchange, that you have not transferred to your private wallet, are they ones that you have some proprietary interest in that gives you priority over other creditors? It is already topical. But particularly with the sort of gyrations in the market at the moment, I think that is probably going to tip some exchanges into liquidation. So, we might have more questions to answer about that proprietary status of different cryptocurrencies.

I am conscious we are well over time. If anyone has any questions we are more than happy to take them. As I say, if people have to go, we certainly understand that as well. That is the end of the substance for now. Does anyone have any questions? No one's brave. Very good. You are welcome to stick around for a drink and have a chat. But thank you very much for coming along.