LEVEL

TWENTY SEVEN

CHAMBERS

LEVEL TWENTY SEVEN CHAMBERS

Cryptocurrency and the law

Michael May and Salwa Marsh

23 June 2022

	#	Name	Price	24h %	7d %	Market Cap
☆	1	Bitcoin BTC Buy	$20,382.10	0.18%	9.15%	$388,867,251,990
☆	2	Ethereum ETH Buy	$1,084.75	1.55%	11.03%	$131,570,836,580
☆	3	Tether USDT	$0.9991	0.01%	0.02%	$66,913,052,344
☆	4	USD Coin USDC Buy	$1.00	0.00%	0.03%	$55,883,639,955
☆	5	BNB BNB Buy	$218.00	0.84%	5.86%	$35,722,814,832
☆	6	Binance USD BUSD	$1	0.09%	0.05%	$17,553,163,163
☆	7	Cardano ADA	$0.4694	0.38%	10.70%	$15,846,645,541
☆	8	XRP XRP	$0.3243	0.55%	3.97%	$15,772,354,847
☆	9	Solana SOL Buy	$35.12	0.29%	2.17%	$12,073,853,384
☆	10	Dogecoin DOGE Buy	$0.06288	1.05%	3.74%	$8,360,336,825

>> Overview

> Bitcoin

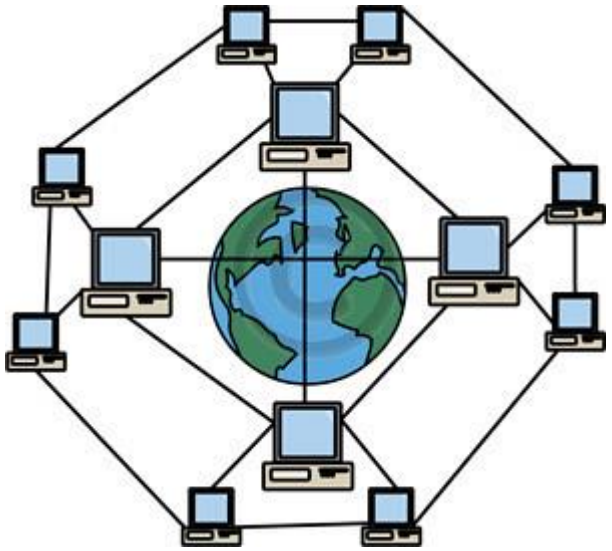
- Decentralisation
- Blockchains
- Proof of work mining
- Hashing
- Private/public key cryptography

> Other cryptocurrencies

- Proof of work
- Smart contracts and decentralised apps
- Tokens – NFTs, stable coins, CBDCs

> Cryptocurrency exchanges

>> Decentralisation



>> The problems of decentralisation

> Which version of the ledger is *the* ledger?

> How do you keep updating the ledger?

> What stops a person ‘spending’ twice?

>> Bitcoin – the solution

> Network of computers called miners

> Rules in the form of code

> Real world incentives

> Secure, amendable decentralised ‘source of truth’ in the form of a blockchain

>> Bitcoin – mining

> Add new valid blocks to the longest chain

> For a fee
- Transaction fees
- New BTC per block

> Requirements for valid blocks
- Identify previous block
- Details of transactions (inc payment to miner)
- A ‘nonce’ (number used only once)

>> Bitcoin – hashing

> Algorithmic encryption of data – digital ‘fingerprint’

> Features:

- Input of any size/content transformed to output that is uniform sized/content
- Deterministic – unique(ish) output governed by input
- Avalanche effect – small Δ in input = large Δ in output
- One-way – impractical to derive input from output

> Used in:

- Identification of previous block
- Validating the block (via the nonce)
- (other things)

>> Bitcoin – public/private keys

> No centralised password database

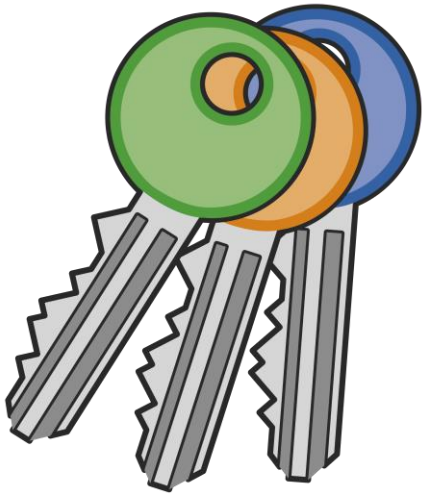
> Private key

> Public key

> Address

> Signature

>‘Wallet’

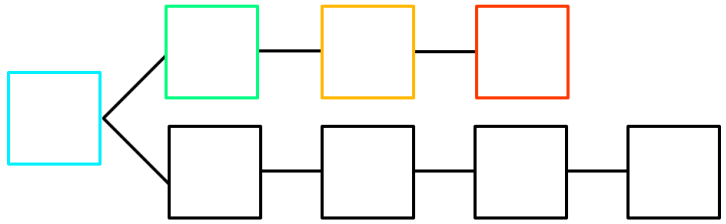


>> Bitcoin – how the blockchain develops

> Longest chain = consensus

> Deeper block = more secure

> Forks in the chain – resolve eventually by one becoming longer



> Impractical to re-write history

- Attackers can't keep up with the network without >50% of hashing power

>> Bitcoin

…We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.
…

- Bitcoin whitepaper, Satoshi Nakamoto

>> Bitcoin – legal issues

> Is it a currency?

- Unit of account of money
- See Currency Act 1965 s 9 –
  - … every sale, … every security for money, and every other contract, … dealing, matter or thing **relating to money**, or involving the payment of, or a liability to pay, money, … **shall**, **unless** it is made, executed, entered into or done according to **the currency of some country other than Australia**, be made, executed, entered into or done according to the currency of Australia …
- El Salvador?
- Effect?

>> Bitcoin – legal issues

> Is it property?

- *Quoine Pte Ltd v B2C2 Ltd* [2020] SQCA(I) 2
- *AA v Persons Unknown* [2020] 4 WLR 35
- *Ruscoe v Cryptopia Ltd (in Liquidation)* [2020] NZHC 728

>> Other cryptos

> Bitcoin limitations

- Transaction volume
- Energy consumption of proof of work mining
- Rudimentary

>> Other cryptos – key themes

> Layers

- Overcome transaction volume problem
- Layer X records net effect of transactions on layer Y

> Proof of stake mining

- Less energy
- Validators ‘stake’ crypto
- Provides yield opportunities
- Compromises decentralisation

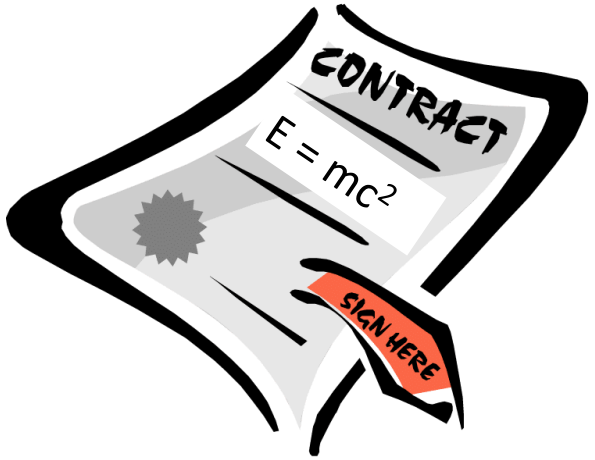
>> Other cryptos – key themes (cont'd)

> Smart contracts

- Computer programs run 'on-chain'

- 'Smart'?
  - If X then Y, otherwise Z
  - Apt for simple transactions
  - Uncertainty –bug or feature? (Lessig)

- 'Contracts'?
  - Executed not executory
  - Counterparties?



>> Other cryptos – key themes (cont'd)

> Decentralised apps (Dapps) – interfaces for smart contracts

> Decentralised exchanges (DEXs) – trade crypto
- Order book
- Market maker

> Decentralised finance (DeFi) – lend crypto

> Oracles
- Decentralised real-world data on chain
- Possible uses
  - Derivative contracts (options, futures, etc)
  - Decentralised insurance?

>> Other cryptos – key themes (cont'd)

> Single vs multiple tokens

> Issuance methodology
- organic
- initial coin offerings (ICOs)

> Non-fungible tokens (NFTs)
- Art, music, games etc

>'Stable' coins
- Centralised
- Algorithmic

> Central Bank Digital Currencies (CBDCs)

>> An example – Polkadot

> A chain of 100 parachains

> Token is DOT

> Each parachain slot is ‘auctioned’

> Bid by binding DOT to a developer in exchange fo developer’s token

>> Regulation

> Why regulate?

> What are the challenges?

> What are your obligations?

> Who regulates?

- ASIC?
- ACCC?

>> Regulation - “financial product”?

> General definition which is common to the Corporations Act and the ASIC Act

> Special definition for the purposes of each regime

>> Regulation - “financial product”?

> s 12BAA(1) ASIC Act, s 763A CA

12BAA Definition of *financial product*

*General definition of **financial product***

(1) Subject to subsection (8), for the purposes of this Division, a ***financial product*** is a facility through which, or through the acquisition of which, a person does one or more of the following:

(a) makes a financial investment (see subsection (4));

(b) manages financial risk (see subsection (5));

(c) makes non□cash payments (see subsection (6)).

(2) Subject to subsection (8), for the purposes of this Division, a particular facility that is of a kind through which people commonly make financial investments, manage financial risks or make non□cash payments is a ***financial product*** even if that facility is acquired by a particular person for some other purpose.

(3) A facility does not cease to be a financial product merely because:

(a) the facility has been acquired by a person other than the person to whom it was originally issued; and

(b) that person, in acquiring the product, was not making a financial investment or managing a financial risk.

763A General definition of *financial product*

(1) For the purposes of this Chapter, a ***financial product*** is a facility through which, or through the acquisition of which, a person does one or more of the following:

(a) makes a financial investment (see section 763B);

(b) manages financial risk (see section 763C);

(c) makes non□cash payments (see section 763D).

This has effect subject to section 763E.

(2) For the purposes of this Chapter, a particular facility that is of a kind through which people commonly make financial investments, manage financial risks or make non□cash payments is a ***financial product*** even if that facility is acquired by a particular person for some other purpose.

(3) A facility does not cease to be a financial product merely because:

(a) the facility has been acquired by a person other than the person to whom it was originally issued; and

(b) that person, in acquiring the product, was not making a financial investment or managing a financial risk.

>> Regulation - “financial product”?

> s 762C CA, see also ASIC Act s 5(1)

762C Meaning of *facility*

In this Division:

facility includes:

(a) intangible property; or

(b) an arrangement or a term of an arrangement (including a term that is implied by law or that is required by law to be included); or

(c) a combination of intangible property and an arrangement or term of an arrangement.

Note: 2 or more arrangements may be taken to constitute a single arrangement—see section 761B.

>> Regulation - “financial product”?

> s 12BAA(4) ASIC Act , see also s 763B CA

Meaning of ***makes a financial investment***

(4) For the purposes of this section, a person (the ***investor***) ***makes a financial investment*** if:

(a) the investor gives money or money's worth (the ***contribution***) to another person and any of the following apply:

(i) the other person uses the contribution to generate a financial return, or other benefit, for the investor;

(ii) the investor intends that the other person will use the contribution to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated);

(iii) the other person intends that the contribution will be used to generate a financial return, or other benefit, for the investor; and

(b) the investor has no day□to□day control over the use of the contribution to generate the return or benefit.

763B When a person makes a financial investment

For the purposes of this Chapter, a person (the ***investor***) ***makes a financial investment*** if:

(a) the investor gives money or money's worth (the ***contribution***) to another person and any of the following apply:

(i) the other person uses the contribution to generate a financial return, or other benefit, for the investor;

(ii) the investor intends that the other person will use the contribution to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated);

(iii) the other person intends that the contribution will be used to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated); and

(b) the investor has no day□to□day control over the use of the contribution to generate the return or benefit.

>> Regulation - “financial product”?

> s 12BAA(5) ASIC Act , see also s 763C CA

Meaning of ***manages a financial risk***

(5) For the purposes of this section, a person ***manages financial risk*** if they:

(a) manage the financial consequences to them of particular circumstances happening; or

(b) avoid or limit the financial consequences of fluctuations in, or in the value of, receipts or costs (including prices and interest rates).

763C When a person *manages financial risk*

For the purposes of this Chapter, a person ***manages financial risk*** if they:

(a) manage the financial consequences to them of particular circumstances happening; or

(b) avoid or limit the financial consequences of fluctuations in, or in the value of, receipts or costs (including prices and interest rates).

>> Regulation - “financial product”?

> s 12BAA(6) ASIC Act, s 763D CA

Meaning of ***makes non-cash payments***

(6) For the purposes of this section, a person ***makes non-cash payments*** if they make payments, or cause payments to be made, otherwise than by the physical delivery of Australian currency in the form of notes and/or coins.

763D When a person *makes non-cash payments*

(1) For the purposes of this Chapter, a person ***makes non-cash payments*** if they make payments, or cause payments to be made, otherwise than by the physical delivery of Australian or foreign currency in the form of notes and/or coins.

>> Crypto exchanges

> Getting crypto

- P2P
- Decentralised exchange
- Centralised exchange

> Topical

> Obvious focus for regulation

> KYC

> Proprietary questions in case of insolvency

Michael May

T +61 7 3008 3969

E MAY@LEVEL27CHAMBERS.COM.AU

Salwa Marsh

T +61 7 3008 3993

E SALWA.MARSH@LEVEL27CHAMBERS.COM.AU

level27chambers.com.au