RAHSIA ALTCOIN

Panduan Asas 6 ALTCOIN Yang Terunggul

OPERASI

eBook

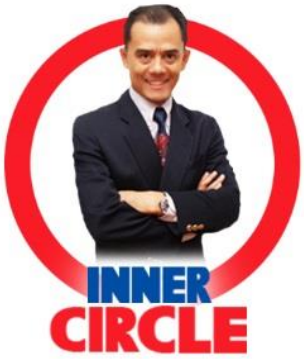
Azizi Ali

MBA ChFC IFP

Dapatkan petunjuk dan bimbingan secara

peribadi daripada Mentor Jutawan #1 Malaysia.

Sertai program Inner Circle sekarang!



www.InnerCircle.my

Diterbitkan oleh True Wealth Sdn Bhd
Tel: 03-7805 4051
Emel: info.tw@MillionairesPlanet.com
Laman Web: www.RahsiaAltcoin.com

Edisi Pertama

10 9 8 7 6 5 4 3 2
22 21 20

Buku ini dihasilkan untuk memberi pengajaran dan menyalurkan maklumat umum mengenai subjek yang dibincangkan. Ia tidak boleh dianggap sebagai mengandungi nasihat kewangan, pelaburan, sekuriti atau perakuan sekuriti.

Segala strategi yang digariskan dalam buku ini mungkin tidak sesuai bagi individu dan tiada jaminan dikeluarkan untuk menghasilkan satu keputusan.

Tiada jaminan dibuat berkenaan ketepatan atau kesempurnaan maklumat yang terkandung di dalam buku ini. Penulis dan penerbit secara khusus tidak bertanggungjawab terhadap apa juga liabiliti, kerugian atas risiko, peribadi mahupun sebaliknya, yang berlaku akibat, secara langsung atau tidak langsung.

AZIZI ALI

RAHSIA ALTCOIN

OPERASI

PANDUAN ASAS 6
CRYPTOCURRENCY TERPILIH

KANDUNGAN

PENGENALAN

Ianya bermula dengan Bitcoin.

Bitcoin telah dilancarkan pada bulan Januari 2009 oleh Satoshi Nakamoto dan dalam proses itu, menjadi *cryptocurrency* yang pertama di dunia.

Di awal hari-harinya, penyokong Bitcoin merupakan *developer*, pakar kriptografi, pakar teknologi dan *hacker*. Dalam kata lain – *computer nerds*! Tetapi konsep pembayaran digital *peer-to-peer* yang tidak memerlukan orang tengah dan tidak di bawah kawalan mana-mana kerajaan atau entiti kewangan memang amat menggiurkan! Dan apabila ditambah dengan konsep *blockchain* yang merupakan lejar atas talian yang terbuka, telus, tidak boleh diubah suai dan kekal selama-lamanya, sudah tentu Bitcoin menarik perhatian semua orang yang mencintakan ketelusan, keadilan, efisiensi dan kemajuan.

Dengan peredaran masa, semakin ramai orang mula menyedari akan kebaikan dan kelebihan Bitcoin, lalu mereka pun mula berjinak dengannya. Jumlah pengguna, peniaga dan perkhidmatan sokongan bertambah dan Bitcoin pun merebak di serata dunia!

Tidak lama kemudian, beberapa individu sedar yang mereka boleh mencipta *cryptocurrency* mereka sendiri, yang mempunyai ciri-ciri yang lebih baik daripada Bitcoin. Lalu mereka pun melancarkan *cryptocurrency* yang lebih baik itu. Ini termasuklah Namecoin (yang merupakan Altcoin yang pertama) dan Litecoin.

Beberapa individu lain pula melancarkan *cryptocurrency* yang mempunyai tujuan-tujuan tertentu. Satu contohnya ialah Monero yang berkhusus kepada sekuriti dan privasi.

Dalam masa yang sama, beberapa individu lain pula sedar yang konsep *blockchain* boleh diaplikasikan kepada banyak benda yang lain, dan tidak perlu dihadkan kepada *cryptocurrency* semata. Jadi lahirlah Ethereum.

Bak kata perpatah Inggeris, *the floodgates were opened*!

Sepertimana kugiran The Beatles melancarkan fenomena *The British Invasion* pada tahun 1964 – di mana artis-artis dari Britain dan muzik mereka mula berkumandang di peti radio dan televisyen di seluruh dunia – Bitcoin telah melancarkan fenomena *cryptocurrency* bermula tahun 2011.

Puluhan, ratusan dan sekarang ribuan *cryptocurrency* telah dilancarkan! Jumlah *cryptocurrency* semasa saya menulis buku ini sudah melebihi 5,400! Jumlah ini sudah tentu akan lebih tinggi waktu anda membacanya.

Baik. Itu jumlah *cryptocurrency*.

Apa yang lebih pentingnya ialah apakah mereka berguna, bernilai, dan bolehkah kita menjana wang dengannya?

Jawapannya ialah BOLEH! Sudah tentu boleh.

Lihat sahaja pulangan berikut:

Nilai Bitcoin telah naik daripada kosong pada tahun 2009 kepada $19,000+ pada hujung tahun 2017! Sebenarnya, pulangan ini adalah pulangan infiniti sebab modal permulaannya adalah kosong. Tetapi untuk memberikan angka, pulangannya ialah 190,000,000% atau 509% setahun (dengan kiraan modal permulaannya ialah $0.01).

Ethereum pula bermula dengan nilai $0.43 semasa pelancarannya pada bulan Julai 2015. Nilainya berlegar pada paras tersebut sepanjang 2015 dan 2016 sebelum meroket bermula bulan Mac 2017 dan naik setinggi $1,422 pada bulan Januari 2018! Jadi Ethereum telah memberikan pulangan 330,597% atau 1,389% setahun!

Ripple telah didagangkan buat kali pertama pada 4 Ogos 2013 dengan harga $0.01. Seperti Ethereum, nilainya berlegar pada paras tersebut sehingga tahun 2017 apabila nilainya turut meroket dan naik setinggi $384 pada bulan Januari 2018! Jadi Ripple telah memberikan pulangan 38,300% atau 626% setahun!

Saya tidak tahu mana-mana produk pelaburan yang telah memberikan pulangan yang begitu tinggi dalam sejarah dunia!

Dan sebelum anda menjerit yang nilai semua *cryptocurrency* ini telah jatuh menjunam dengan ketara pada tahun 2018 dan 2019 (sesetengahnya jatuh hingga 80%!), poin yang saya hendak berkongsi di sini ialah pulangan yang telah mereka berikan ialah *insane*!

Jika ia berlaku sebelum ini, pulangan yang sama juga boleh berlaku pada hari esok.

Saya sambung ceritanya lagi.

Daripada idea yang hanya disebut-sebut oleh komputer *geeks* semata, Altcoin kini digunakan di serata dunia dan menjadi sebut-sebutan jutaan manusia!

Salah satu bukti penggunaan dan penerimaan Altcoin telah berkembang dengan pesat ialah nilai pasaran kedua-dua Bitcoin dan Altcoin pada bulan Mei 2013 hanyalah $1.37 bilion. Angka ini naik kepada $3.8 bilion pada bulan Mei 2015, melompat kepada $72 bilion pada bulan Mei 2017 dan $245 bilion semasa saya menulis buku ini (Mei 2020).

Lagi satu realitinya ialah Altcoin akan terus berkembang. Fakta ini tidak boleh ditolak oleh sesiapa. (Jika mereka menolaknya pun, ianya tidak mengubah fakta tersebut! Ada perkara dalam kehidupan ini yang betul sama ada anda percayanya atau tidak dan sama ada anda bersetuju dengannya atau tidak!) Malah jumlah penggunanya dan jumlah

penerimaannya oleh dunia akan bertambah dengan ketara pada hari-hari yang akan datang.

Jadi anda tidak perlu bimbang yang Altcoin akan pupus esok hari!

Tetapi sudah tentu ceritanya tidak semuanya indah belaka. Seperti kebanyakan produk baru, Altcoin telah melalui beberapa insiden negatif dalam usianya yang masih muda ini. Ini termasuklah menjadi mata wang untuk penjahat membeli produk dan servis '*underground*'.

Dan oleh sebab jumlah wang yang berlegar dalam dunia *cryptocurrency* ini masuk berbilion-bilion Dolar, ianya didiami juga oleh *scammer*, *hacker*, penipu dan pencuri. Mereka ini bukan sahaja wujud tetapi sentiasa mencari peluang untuk mengebas wang anda. Dan apabila saya tulis 'sentiasa', maksudnya 24 jam sehari, 7 hari seminggu!

Peluang untuk buat wang besar memang wujud dalam dunia *cryptocurrency*. Dalam masa yang sama, peluang untuk kehilangan wang besar juga memang wujud dalam dunia *cryptocurrency*!

Jawapannya adalah dengan mendapatkan ilmu yang secukupnya sebelum anda melangkah masuk ke dalam dunia ini.

Berita baiknya ialah buku ini merupakan langkah pertama dan pembuka tirainya.

Jadi baca buku ini sampai ke akhirnya. Dapatkan ilmu asas tentang Altcoin dan kemudian buat keputusan anda sendiri.

Semoga buku ini dapat menolong anda membina kehidupan yang lebih baik untuk diri dan keluarga.

Amin!

Penafian

Altcoin wujud di internet. Dan sepertimana produk lain yang wujud di internet, Altcoin boleh berubah dengan sekelip mata. Hari ini okay, besok boleh jadi tidak okay!

Oleh sebab itu, berikut adalah beberapa penafian tentang kandungan buku ini:

a) Maklumat mungkin berlainan

Dalam usaha menulis buku ini, saya telah melakukan banyak kajian. Ini termasuklah membaca banyak buku tentangnya, membaca artikel-artikel di internet, menonton video di YouTube, menyertai beberapa program di Udemy dan bertanya kepada beberapa individu yang terlibat di dalam dunia *cryptocurrency*.

Walaupun kebanyakan maklumat itu adalah sama, ada beberapa maklumat yang berlainan. Buku A kata begini sementara buku B pula kata begitu! Maka ada beberapa maklumat dalam buku ini yang mungkin berbeza dengan maklumat yang anda peroleh di internet atau buku-buku lain.

b) Situasinya mungkin berlainan

Penafian kedua ialah situasinya mungkin berlainan semasa anda membaca buku ini. Situasinya adalah tepat semasa saya menulis buku ini tetapi oleh sebab semuanya boleh bertukar dengan cepat di internet, situasi mungkin berlainan semasa anda membacanya. Sila ingat poin ini semasa anda membaca buku ini.

c) Fahamkan istilah ‘Altcoin’ sebagai ‘Altcoin terpilih’

Anda perlu ingat yang jumlah Altcoin melebihi 5,400 sekarang! Jadi apabila saya tulis sesuatu pernyataan berkenaan Altcoin di dalam buku, ini tidak bermakna pernyataan tersebut boleh diaplikasikan kepada semua 5,400 Altcoin yang wujud! Situasi mungkin wujud yang membuatkan pernyataan tersebut tidak boleh diaplikasikan kepada sesetengah Altcoin.

Jadi apabila anda nampak perkataan ‘Altcoin’ dalam buku ini, fahamkannya sebagai Altcoin terpilih! Atau dalam bahasa Inggerisnya, *read Altcoin as selected Altcoins*.

d) Saya mungkin memiliki sesetengah Altcoin yang ditulis

Saya mungkin memiliki sesetengah Altcoin yang ditulis di dalam buku ini. Saya tidak mengesyorkan mana-mana Altcoin termasuk Altcoin yang saya miliki itu. Saya berkongsi ilmu; apa yang anda buat dengan ilmu itu berada di tangan anda sendiri. Anda yang membuat pilihannya dan andalah yang memikul tanggung jawab akan semua keputusan kewangan dan pilihan pelaburan anda.

e) Istilah dalam bahasa Inggeris

Walaupun saya mahu menggunakan bahasa Melayu dalam buku ini, realitinya Altcoin ialah produk dari barat dan hampir 100% istilah yang digunakan berkaitannya – proses mendaftar, membeli, menyimpan dan menjual – adalah dalam bahasa Inggeris. Walaupun saya boleh mengalih bahasa kebanyakan istilah tersebut, ia akan nampak pelik, berbunyi pelik, malah ramai pembaca yang mungkin tidak faham apa yang saya maksudkan. Oleh itu, saya membuat keputusan untuk mengekalkan dan menggunakan beberapa istilah bahasa Inggeris di dalam buku ini. Jadi jika ada sesiapa yang mengeluh dia tidak faham bahasa Inggeris, ini jawapannya – anda tidak sepatutnya melabur dalam Altcoin kerana bahasa Inggeris ialah bahasa utama dalam dunia Altcoin! Dan jika anda tidak faham bahasa Inggeris, anda pasti akan menanggung kerugian kerana anda mungkin akan tersalah tekan butang, tersilap sana, tidak faham itu dan tidak faham ini ketika melakukan transaksinya.

Sila ambil perhatian juga yang saya menggunakan nilai Altcoin dalam nilai Dolar Amerika – simbolnya $ – dalam buku ini supaya datanya kekal konsisten. Ini pasti akan menolong anda memahaminya.

f) Buku ini ialah asas-asas tentang Altcoin

Akhirnya, saya perlu terangkan bahawa saya bukan seorang pakar teknologi, bukan *webmaster*, bukan *hacker*, bukan *developer* dan bukan *miner*. Saya merupakan seorang usahawan, pengguna dan pelabur Altcoin, seperti anda dan ramai pembaca lain. Lagipun, buku ini ditulis untuk pembaca awam yang ingin mempelajari asas-asas tentang Altcoin. Jadi buku ini menggunakan bahasa yang mudah difahami, senang dibaca dan mempunyai jawapan yang *straight to the point*! Malah tidak ada penerangan teknikal atau rumit dalam buku ini. Jadi sesiapa yang hendak tahu dengan panjang lebar tentang *hashrate*, *port 8333*, *Finney attack* dan sebagainya, mereka perlulah mendapatkan maklumat tersebut di tempat lain.

Ada faham?

Baik.

Sekarang, kita bermula!

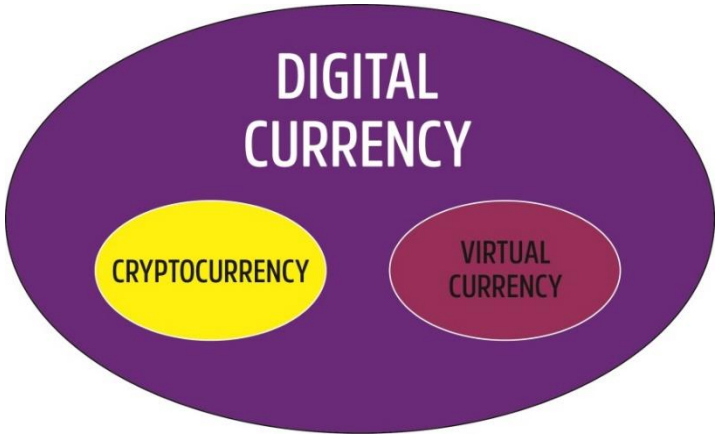
1. APAKAH ITU *CRYPTOCURRENCY*?

Kita bermula daripada asasnya.

Berikut ialah definisi *cryptocurrency* mengikut Wikipedia:

'*Cryptocurrency* (atau mata wang kripto) ialah aset digital yang direka bentuk untuk berfungsi sebagai medium pertukaran menggunakan kriptografi bagi menjamin transaksi dan mengawal penciptaan unit tambahan mata wang. *Cryptocurrency* dikelaskan sebagai subset mata wang digital dan juga dikelaskan sebagai subset mata wang alternatif dan mata wang maya.'

Jadi *cryptocurrency* ialah (1) aset digital, (2) berfungsi sebagai medium pertukaran, (3) menggunakan kriptografi untuk tujuan sekuriti, dan (4) ianya adalah subset kepada mata wang digital.



Grafik 1.1: *Cryptocurrency* adalah subset kepada mata wang digital

Ini bermakna kita boleh berkata yang *cryptocurrency* ialah sejenis mata wang digital tetapi mata wang tidak digital tidak semestinya *cryptocurrency*! (Saya rasa penjelasan ini telah memeningkan anda!)

Bagaimanapun, tidak ada siapa yang akan mentertawakan anda jika anda memanggil mata wang digital sebagai *cryptocurrency* dan sebaliknya. Kita di Malaysia ini tidak kisah sangat akan benda-benda kecil macam ini, betul tak?

Cryptocurrency yang pertama ialah Bitcoin. Malah semua Altcoin yang terbit selepas Bitcoin memang merupakan *cryptocurrency*.

Untuk pengetahuan tambahan anda, kriptografi bermaksud ‘tulisan rahsia’ (berasal dari bahasa Greek). Jadi kriptografi merupakan praktis (dan juga kajian) merahsiakan maklumat dalam bentuk tulisan. Selalunya, maklumat itu ialah maklumat yang sensitif seperti rahsia negara, data kewangan serta maklumat ketenteraan. Kriptografi telah wujud beribu-ribu tahun, malah sejak zaman pemerintahan Rom purba lagi.

Hari ini, kriptografi menggunakan teknologi komputer dan digunakan untuk maklumat ketenteraan, mesin ATM, kata laluan komputer dan *cryptocurrency*.

Dan untuk menjelaskan situasi dengan sejelas-jelasnya, kriptografilah yang menyebabkan *cryptocurrency* menjadi berguna. Tanpa kriptografi, bukan sahaja *cryptocurrency* tidak akan berguna; malah ianya mungkin tidak akan wujud langsung!

2. APAKAH ITU ALTCOIN?

Jawapan pendek kepada soalan ini amat mudah: Altcoin ialah semua *cryptocurrency* yang bukan Bitcoin!

Atau dalam kata lain, mereka merupakan alternatif kepada Bitcoin.

Baik. Sekarang saya berikan jawapan panjangnya pula:

'Altcoin' adalah gabungan dua istilah: '*alt*' dan '*coin*'.

'Alt' menandakan 'alternatif' dan '*coin*' menandakan (pada dasarnya) '*cryptocurrency*'.

Selepas kejayaan Bitcoin, mata wang digital *peer-to-peer* lain pun muncul dalam usaha untuk meniru kejayaan itu. Dan untuk membezakan mereka daripada Bitcoin, istilah Altcoin pun dicipta dan digunakan untuk menerangkan semua *cryptocurrency* yang baru ini. Istilah ini masuk akal pada waktu permulaannya kerana jumlah Altcoin itu sedikit. Malangnya, tidak lama kemudian, jumlah Altcoin meningkat dengan ketara. Malah, mereka muncul bagaikan pekerja asing di Malaysia – banyak, cepat, pelbagai jenis dan rupa dan hampir tidak terkawal!

Dan kerana istilah 'Altcoin' bermakna semua *cryptocurrency* yang bukan Bitcoin, ini bermakna yang terdapat lebih 5,400 Altcoin semasa anda membaca buku ini! Ini termasuklah yang terkenal dan popular seperti Ethereum, Ripple, Binance Coin, Tether dan Litecoin kepada yang kabur seperti Mixin, Tap dan Centrality kepada yang *scam* seperti OneCoin, Visa Coin dan Speed Coin.

Pada umumnya, mereka menonjolkan diri mereka bukan sahaja sebagai alternatif kepada Bitcoin tetapi alternatif yang lebih baik daripada Bitcoin. Ya, semuanya mengaku mereka adalah yang lebih baik daripada Bitcoin!

Dan oleh sebab terdapat lebih daripada 5,400 Altcoin semasa ini, istilah Altcoin itu mungkin sudah menjadi *overkill*. Ini adalah kerana *coin-coin* tersebut mempunyai banyak perbezaan di antara satu dengan lain sehinggakan mungkin persamaan yang ada hanyalah mereka merupakan *cryptocurrency*! Semuanya mempunyai pasukan pemaju mereka sendiri, penggunaan alternatif mereka sendiri serta peluang pelaburan untuk pelabur.

Anda sudah pening?

Usah gentar wiraku, kerana semuanya akan menjadi lebih jelas di akhir buku ini.

Teruskan pembacaan anda!

3. MENGAPAKAH JUMLAH ALTCOIN INI BEGITU BANYAK SEKALI?

Seperti yang saya jelaskan sebelum ini, selepas melihat kejayaan Bitcoin yang mendapat sambutan yang hebat daripada pelabur di seluruh pelusuk dunia, *cryptocurrency* lain pun muncul dalam usaha untuk meniru kejayaan itu. Dan kebanyakannya menawarkan beberapa kelebihan jika dibandingkan dengan Bitcoin. Sebagai contoh, Litecoin dilancarkan pada bulan October 2011 oleh Charlie Lee, bekas Pengarah Kejuruteraan di syarikat CoinBase. Litecoin ialah *fork* daripada Bitcoin yang mempunyai beberapa perbezaan termasuklah masa penjanaan blok 2.5 minit (lawan 10 minit untuk Bitcoin), jumlah maksimum *coin* 61 juta (lawan 21 juta untuk Bitcoin), algoritma *hashing* yang berbeza (Scrypt dan bukan SHA-256), dan GUI yang diubah suai.

Beberapa *coin* baru juga dilancarkan untuk tujuan-tujuan tertentu seperti Ripple (XRP) yang diciptakan untuk menjadi pilihan penyelesaian yang paling pantas dan berkesan untuk institusi kewangan, Monero (XMR) yang menawarkan tahap privasi yang paling tinggi sementara Ethereum (ETH) dan Neo yang dibangunkan untuk memperluaskan penggunaan teknologi *blockchain* di luar industri kewangan.

Dan dengan peredaran masa, proses untuk melancarkan *coin-coin* baru ini menjadi lebih senang, cepat dan murah.

Poin yang terakhirnya adalah kerana tidak ada undang-undang di kebanyakan negara yang mengehadkan pelancaran *coin-coin* baru ini. Malah, jika ada undang-undang yang mengehadkan pelancaran *coin-coin* baru ini pun tidak ada gunanya kerana ianya tidak boleh dikuatkuasakan pun!

Semua poin-poin ini bak memberikan lampu hijau untuk sesiapa yang berminat untuk melancarkan *coin* mereka!

Bagaimanapun sebab utama mengapa jumlah Altcoin ini begitu banyak sekali adalah senang sekali – ianya memberi peluang untuk ramai orang terutamanya mereka yang melancarkan *coin* tersebut untuk buat wang besar. Dan jumlah wangnya memang besar – masuk berbilion-bilion Dolar. Siapa yang tak nak?

Cakap-cakap pasal wang besar ini, anda juga boleh melancarkan *coin* anda sendiri jika anda mahu. Ianya tidaklah begitu susah!

4. APAKAH PERBEZAAN DI ANTARA '*COIN*' DAN 'TOKEN'?

Anda mesti mendengar istilah '*coin*' dan 'token' digunakan dalam dunia *cryptocurrency*. Anda mungkin bertanya mengapa terdapat dua istilah dan apakah perbezaan di antara kedua-duanya?

Berikut ialah jawapannya:

Sebenarnya *coin* dan token ialah dua konsep yang berbeza. Bagaimanapun istilah '*coin*' dan 'token' sering digunakan sebagai sinonim dan malah ramai orang menganggap mereka boleh ditukar ganti – sepertimana kita gunakan istilah 'wang' dan 'duit'.

Situasi ini mungkin timbul kerana *cryptocurrency* bukan sahaja merupakan subjek yang baru tetapi ianya juga berubah dengan pantas dan pesat. Jadi timbullah istilah-istilah baru yang membawa kepada salah faham dan seterusnya salah guna istilah-istilah tersebut.

Contoh yang ketara adalah bagaimana semua *coin* dan token dianggap sebagai *cryptocurrency*, walaupun kebanyakan daripada mereka tidak digunakan sebagai mata wang dan malah tidak pernah dimaksudkan untuk menjadi mata wang pun!

Menurut definisi, mata wang ialah medium pertukaran, unit akaun dan nilai simpanan. Bitcoin mempunyai semua ciri-ciri ini, jadi istilah '*cryptocurrency*' adalah wajar dalam kes ini. (Ingat yang Bitcoin adalah *cryptocurrency* yang pertama.)

Malangnya kejayaan Bitcoin ini bermakna semua produk-produk yang muncul selepasnya (kira anak, cucu dan cicit Bitcoinlah!) dilabelkan sebagai *cryptocurrency* juga, walaupun kebanyakan mereka tidak memenuhi ciri-ciri mata wang. Jadi *coin* dipanggil *cryptocurrency*, dan malah token turut dipanggil sebagai *cryptocurrency* juga. Kekeliruan ini berterusan hingga ke hari ini kerana (a) ramai orang masih keliru dengan *cryptocurrency* (b) mereka malas nak belajar tentangnya! Jadi inilah sebabnya mengapa ramai orang membeli token walaupun tujuan asal adalah untuk membeli *coin*!

Teruskan pembacaan anda untuk mendapat penerangannya:

Coin

Coin (yang juga sering disebut sebagai Altcoin) ialah wang digital. Ianya dicipta dengan menggunakan teknik kriptografi dan ianya menyimpan nilai dengan peredaran masa.

Dan sepertimana yang anda sudah maklum, Bitcoin ialah contoh *coin* yang paling terkenal. Bitcoin menggunakan sistem *blockchain* – sebuah lejar digital dan umum di

mana semua transaksi dapat dilihat. Data disimpan secara kolektif dan dikongsi antara peserta rangkaian *blockchain* dan sama menariknya, data tersebut kekal buat selama-lamanya! Jadi sistem *blockchain* menjamin ketelusan dan mengurangkan penipuan.

Terdapat beberapa *coin* seperti Litecoin dan Namecoin yang berdasarkan protokol asal Bitcoin yang dicipta oleh Satoshi Nakamoto. Ada juga terdapat *coin* yang beroperasi di *blockchain* yang dicipta khusus untuk kegunaan mereka – contohnya ialah Ripple, Zcash dan Dash.

Seperti yang disebut sebelum ini, *coin* mempunyai ciri-ciri yang sama seperti mata wang: mereka *fungible* (boleh diganti dengan aset yang sama), boleh dibahagi, diterima, mudah alih, tahan lama dan mempunyai bekalan yang terhad.

Ciri-ciri utama *coin* ialah:

1) mereka terikat kepada *blockchain* awam yang terbuka; sesiapa sahaja dibenarkan untuk menyertai dan mengambil bahagian dalam rangkaian,
2) mereka boleh dihantar, diterima atau dilombong.

Jadi rumusannya *coin* tidak dimaksudkan untuk melakukan apa-apa fungsi melainkan bertindak sebagai wang.

Token

Token merupakan wakil kepada aset atau utiliti tertentu yang diterbitkan oleh sesuatu projek. Ia biasanya wujud di atas platform *blockchain* yang lain.

Token pada dasarnya boleh mewakili apa-apa sahaja aset yang *fungible* dan boleh diperdagangkan. Ini termasuklah dagangan komoditi ke poin *loyalty* ke tiket konsert ke hak mengundi ke *cryptocurrency* lain.

Proses mencipta token adalah lebih mudah daripada mencipta *coin* kerana tidak ada keperluan untuk mengubah kod daripada protokol tertentu atau mencipta blok dari awal. Apa yang perlu dilakukan untuk mencipta token ialah mengikut templat standard blok – seperti yang wujud di platform Ethereum.

Seperti yang disebut sebelum ini, token wujud dan beroperasi di atas platform lain, umpamanya Ethereum. Jadi perbezaan utama di antara *coin* dengan token ialah *coin* menggunakan *blockchain* sendiri sementara token dihoskan di atas *blockchain* yang lain.

Token biasanya dicipta dan diedarkan kepada orang awam melalui Initial Coin Offering (ICO). Empat contoh token yang popular ialah Binance Coin (BNB), EOS (EOS), Tron (TRX) dan OmiseGo (OMG). Platform yang digunakan untuk pembangunan token termasuklah Omni, NEO, Qtum dan Waves. Bagaimanapun, platform yang paling popular ialah Ethereum.

5. APAKAH ITU *WALLET*?

Wallet, seperti namanya, ialah tempat di mana anda menyimpan *cryptocurrency* anda – Bitcoin dan juga Altcoin. Sebenarnya, *wallet* ini tidak wujud secara fizikal. Ianya wujud dalam bentuk maya, jadi mungkin lebih baik untuk anda memikirkannya sebagai akaun digital *coin* anda.

Setiap *wallet* mempunyai dua data yang penting. Data yang pertama ialah *public address* (alamat) yang mempunyai kombinasi 26+ angka dan huruf (contoh: 1BvPTEYstWetqTFn7Au4m2GFg5xJaNVN3). Dan sepertimana anda memberikan e-mel anda kepada orang lain supaya mereka dapat menghantar e-mel kepada anda, anda berikan *public address* ini kepada penghantar supaya mereka dapat menghantar *coin* yang berkenaan kepada anda. Ambil perhatian, anda boleh menjana *public address* yang berbeza dalam satu *wallet*.

Apabila anda hendak menghantar *coin* pula, anda hantarkan *coin* itu kepada *public address* si penerima.

Data yang kedua ialah *private key* anda. *Private key* ini adalah kata laluan (*password*) anda untuk mendapat akses ke dalam *wallet* anda. Ianya ialah bukti yang andalah tuan punya *coin* yang terdapat di dalam *wallet* tersebut. Ianya juga membolehkan anda melakukan transaksi serta menghantar *coin* keluar dari *wallet* anda.

Saya perlu mengingatkan yang anda perlu berhati-hati dengan data *private key* anda. Pertamanya, anda perlu merahsiakannya. Poin ini adalah amat kritikal sebab jika ada orang mendapat data tersebut, mereka sudah mempunyai akses kepada *wallet* anda dan boleh mengebas semua *coin* di dalam *wallet* tersebut. Keduanya, anda juga perlu membuat backup. Jika anda terlupa atau kehilangan data tersebut, anda tidak akan dapat akses ke *coin* anda dan ini akan mengakibatkan anda kehilangan *coin* itu buat selama-lamanya!

Tahap sekuriti berbeza bagi *wallet* yang berbeza. *Wallet* yang digunakan secara harian mempunyai akses yang pantas (dan oleh itu, tahap sekuriti yang minimal) sementara terdapat juga *wallet* yang mempunyai tahap sekuriti yang lebih canggih.

Terdapat empat jenis *wallet*:

1) *Wallet software*: *coin* anda disimpan dalam apps yang terletak di *hard drive* komputer anda.
2) *Wallet* web: *wallet* anda disimpan oleh sebuah syarikat *online*.
3) *Wallet hardware*: anda simpan *coin* anda di dalam sebuah peranti (*device*) fizikal.
4) *Wallet* kertas: anda cetak data *coin* di atas kertas.

Yang mana satu menjadi pilihan anda bergantung kepada tujuan anda berinteraksi dengan *coin*, bajet dan lokasi anda. Sebagai contoh, jika anda melakukan banyak jual beli (anda seorang *trader*), maka *wallet online* merupakan pilihan terbaik untuk anda kerana ia tidak memerlukan banyak kerenah atau birokrasi untuk membuat pembelian.

Sudah tentunya anda boleh mempunyai *wallet* yang berbeza. Sebagai contoh, ramai orang menggunakan *wallet* web dan juga *wallet hardware*. *Wallet* web digunakan untuk menjual beli (kerana mudah dan cepat) dan *wallet hardware* digunakan untuk menyimpan Altcoin (kerana ianya lebih selamat).

6. APAKAH PERBEZAAN ANTARA *HOT WALLET* DAN *COLD STORAGE*?

Hot wallet ialah jenis *wallet* yang sentiasa *online*. Ianya mempunyai talian sambungan yang aktif kepada rangkaian *coin* anda, dan anda boleh membuat pembelian, membuat deposit serta mengeluarkan *coin* dengannya. Jadi ianya sentiasa panas!

Cold storage ataupun *wallet hardware* ialah *wallet* yang *offline*. Dua contoh *wallet cold storage* ialah Trezor dan Ledger Nano S. Kedua-duanya datang dalam bentuk USB.

Grafik 6.1: Ledger Nano S

Anda hanya akan menyambungkan *wallet cold storage online* apabila perlu sahaja, selalunya apabila anda hendak memindahkan *coin* daripada hot *wallet* anda.

Selalunya, pengguna akan menyimpan sedikit *coin* dalam *hot wallet* untuk kegunaan harian sementara kebanyakan *coin* yang lain disimpan dalam *cold storage*.

Tindakan begini dibuat adalah untuk tujuan sekuriti. *Coin* yang disimpan dalam *hot wallet* terdedah kepada serangan *hacker*. Ya, walaupun dengan pelbagai tahap sekuriti, selagi mana *wallet* itu *online*, ianya terdedah kepada serangan *hacker*. Dan jika *hacker* itu berjaya membolos masuk ke dalam *hot wallet* anda, mereka pasti akan menyapu bersih semua *coin* anda!

Oleh sebab itulah anda perlu menyimpan kebanyakan *coin* anda dalam *cold storage* kerana ianya selamat daripada serangan *hacker*.

Mungkin ini boleh menolong anda: fikirkan *hot wallet* sebagai akaun semasa sementara *cold storage* sebagai dana rizab!

7. DI MANA UNTUK MENDAPATKAN *WALLET*?

Kebanyakan *exchange* menyediakan *hot wallet* untuk kemudahan pelanggan mereka. Selalunya mereka menguatkuasakan 2FA/MFA (*two factor authentication*) seperti Google Authenticator atau Authy apabila anda mahu mengeluarkan wang, dan mungkin juga meminta *passphrase* untuk menambahkan lagi tahap sekuriti.

Ada juga syarikat yang menawarkan *hot wallet* walaupun mereka bukan *exchange*. Exodus menawarkan *hot wallet* yang berada di *desktop* komputer anda sementara StrongCoin menawarkan *hot wallet* di server mereka. Blockchain.info juga menawarkan perkhidmatan *hot wallet* di server mereka; malahan *wallet* Blockchain.info merupakan *wallet* yang paling popular di dunia dengan lebih 46 juta *wallet* sewaktu buku ini diterbitkan!

Seperti yang telah dijawab sebelum ini, dua contoh *wallet cold storage* jenis *hardware* ialah Trezor dan Ledger Nano S. Anda boleh mendapatkan *wallet cold storage* ini dengan membuat pesanan di laman web syarikat berkenaan ataupun di laman web ejen-ejen mereka.

Grafik 7.1: Trezor

Kita berjumpa lagi dalam bab berikutnya.

8. BAGAIMANA CARANYA UNTUK MEMBELI ALTCOIN?

Wah! Nampaknya anda sudah tidak sabar-sabar lagi hendak berdagang Altcoin!

Baik. Anda boleh membeli *coin* daripada *exchange* atau daripada individu yang boleh anda temui di *marketplace*.

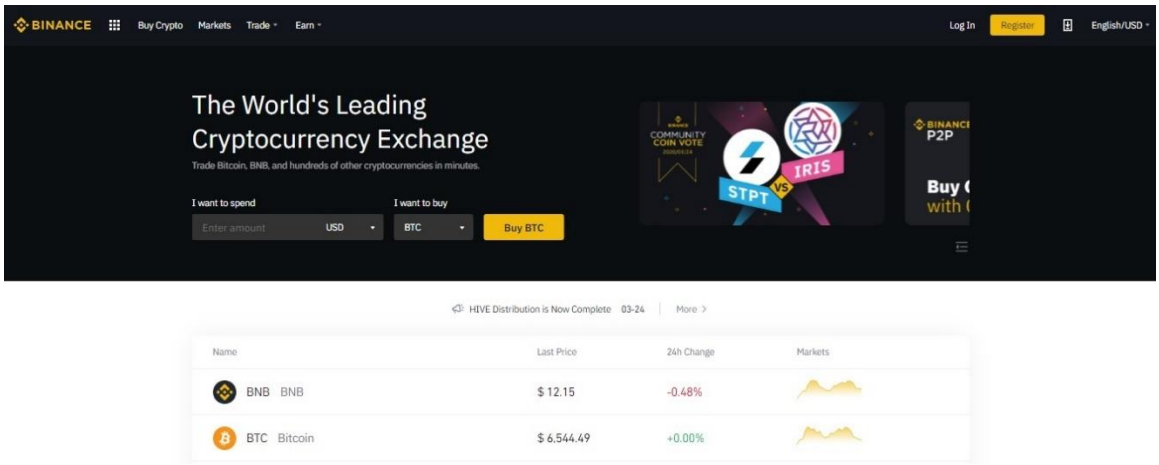
Bayaran yang diterima ialah dalam bentuk tunai, kad kredit, kad debit, pemindahan perbankan dan malah Altcoin yang lain. Cara bayarannya bergantung kepada lokasi (negara) anda dan daripada siapa anda membelinya.

Walau bagaimanapun, langkah pertama yang anda perlu lakukan untuk membuat pembelian adalah dengan mendapatkan *wallet*. (Sila rujuk jawapan tentang *wallet*.)

9. APAKAH ITU *EXCHANGE*?

Sepertimana pengguna menjual beli saham di bursa saham, *exchange* ialah laman web di mana pengguna boleh menjual beli Bitcoin dan Altcoin.

Contoh *exchange* ialah Luno, Binance, Coinbase, LocalBitcoins, Kraken dan BitPanda. Ambil perhatian yang hanya beberapa *exchange* sahaja yang beroperasi di kebanyakan negara di seluruh dunia (contoh: CoinBase dan LocalBitcoins). Kebanyakan *exchange* beroperasi hanya di beberapa negara tertentu sahaja (contoh: Luno yang beroperasi di Afrika Selatan, Singapore, Indonesia dan Malaysia sahaja).



Grafik 9.1: Laman web Binance.com

Untuk bertransaksi di *exchange* tertentu, pengguna perlulah mendaftarkan diri dengan *exchange* tersebut dahulu. Selalunya mereka akan bermula dengan proses pengesahan identiti.

Apabila proses pengesahan itu berjaya, barulah akaun dibuka untuk pengguna. Mereka kemudiannya perlu memindahkan dana ke dalam akaun ini sebelum mereka dapat membeli *coin*. Ada juga *exchange* (contohnya Luno) yang mengehadkan jumlah transaksi bergantung kepada tahap pengesahan diri pengguna. Lebih banyak maklumat yang diberikan oleh pengguna, lebih tinggilah jumlah *coin* yang mereka dapat berjual beli.

Cara untuk mendeposit dana ke dalam *exchange* mungkin berbeza mengikut *exchange* yang berbeza. Cara tersebut termasuklah pindahan atas talian, *direct bank-in*, draf bank, kad kredit, kad debit dan *wire transfer*.

Pengguna yang ingin mengeluarkan wang dari akaunnya pula boleh menggunakan opsyen yang disediakan oleh *exchange* seperti pindahan atas talian, PayPal, *direct bank-in*, cek atau kad kredit.

Sudah tentu pihak *exchange* tidak membuat semua kerja ini dengan percuma! Mereka juga mendapat habuan mereka. Habuan yang pertama adalah melalui fi yang dikenakan kepada pengguna setiap kali mereka membuat transaksi membeli dan menjual *coin*. Habuan yang kedua adalah melalui fi yang dikenakan kepada pengguna untuk mendeposit dan mengeluarkan wang dari akaun mereka. Selain fi transaksi dan yuran pemindahan dana, pengguna juga boleh dikenakan fi penukaran mata wang. Jumlah semua fi ini bergantung kepada polisi *exchange* berkenaan.

Saya perlu menambah yang tidak semuanya indah belaka dalam dunia Altcoin.

Satu masalah yang boleh timbul apabila anda menggunakan *exchange* ialah sekiranya *exchange* tersebut menghadapi masalah kewangan atau masalah dengan bank, wang anda (yang berada dalam pegangan mereka) mungkin turut sama tersangkut dalam masalah itu.

Untuk pengetahuan anda, Mt. Gox (satu *exchange* yang popular pada awal-awal usia Bitcoin) menghadapi masalah ini sebelum *exchange* itu menutup operasi dan kemudiannya diisytiharkan bankrup.

Masalah yang kedua ialah perkhidmatan *exchange* tersebut mungkin disekat oleh kerajaan tempatan. Sebagai contoh, akaun bank Luno di Malaysia telah disekat oleh Lembaga Hasil Dalam Negeri (LHDN) pada tahun 2018. Sekatan itu antara lainnya menyebabkan pengguna tidak dapat mengeluarkan wang mereka yang berada di dalam akaun bank Luno. Dalam kata lain, wang itu tersangkut dalam akaun Luno. (Saya sendiri menjadi mangsa dalam insiden ini. Wang saya juga tersangkut dalam akaun Luno – hampir RM30!)

Dan sudah tentu masalah terbesarnya ialah anda boleh kehilangan semua *coin* yang disimpan dalam *wallet* yang dipegang oleh *exchange* tersebut jika *exchange* itu digodam. Insiden begini telah berlaku berkali-kali. Antara insiden *hacking* yang paling ketara ialah apabila *exchange* Mt.Gox digodam pada tahun 2014 (kerugian bernilai $450 juta) dan apabila *exchange* Binance digodam pada tahun 2019 (kerugian bernilai $40 juta).

Saya perlu menambah yang anda tidak perlu risau sangat tentang semua risiko-risiko di atas kerana kita memang mempunyai jawapannya – simpan kebanyakan *coin* anda dalam *hardware wallet*!

Saya sambung cerita dalam bab seterusnya.

10. BAGAIMANA CARANYA UNTUK MEMBELI ALTCOIN DI MALAYSIA?

Sebenarnya, anda boleh membeli Altcoin daripada kebanyakan *exchange* yang beroperasi di internet. Ini termasuklah Binance, Coinbase, BitQuick, BitBargain dan CoinCorner. Tetapi oleh sebab semua *exchange* ini tidak menerima ringgit Malaysia, anda perlu menukar ringgit kepada bentuk mata wang yang mereka terima terlebih dahulu (selalunya Dolar Amerika, Pound sterling, Euro ataupun Bitcoin) untuk membuat pembelian tersebut. Jadi leceh sikitlah!

Semasa buku ini diterbitkan, terdapat hanya tiga digital *asset exchange* yang dibenarkan oleh Surunhanjaya Sekuriti untuk beroperasi di Malaysia – Luno.com, Sinegy.com dan Tokenizemalaysia.com. (Terdapat lebih 20 *exchange* yang diarahkan untuk menghentikan operasi mereka pada bulan Jun 2019.)

Apa yang bagus tentang ketiga-tiga *exchange* ini ialah mereka menerima ringgit. Jadi anda hanya perlu depositkan ringgit ke dalam *wallet* dan kemudiannya anda boleh terus membuat pembelian.

Bila anda jual *coin* pula, anda boleh terus menerima ringgit dan kemudian pindahkan wang itu ke dalam akaun bank anda. Cepat dan mudah.

Oleh sebab proses pembelian dan peraturan antara ketiga-tiga *exchange* ini berbeza, anda perlu log masuk ke laman web *exchange* yang berkenaan untuk mengetahui langkah sebenar untuk membuat pembelian.

Nota: Akaun bank Luno telah digantung oleh Lembaga Hasil Dalam Negeri pada bulan Januari 2018. Waktu itu Luno tidak boleh menerima wang yang didepositkan oleh pelanggan mereka dan pelanggan juga tidak boleh mengeluarkan wang dari *wallet* di Luno kepada akaun bank mereka. Ini bermakna susahlah untuk pelanggan menjual beli melalui Luno. Bagaimanapun, Luno sudah pun kembali beroperasi dan malah merupakan *exchange* yang paling popular di Malaysia.

Berita yang lebih baiknya ialah anda juga mempunyai satu alternatif untuk menjual beli Altcoin di Malaysia – Remitano.com. Oleh kerana Remitano bukanlah *exchange* tetapi merupakan satu *peer-to-peer marketplace*, undang-undang yang wujud di Malaysia sekarang mungkin tidak melindunginya! Dalam bahasa Inggerisnya: *peer-to-peer marketplace may fall into a grey area*.

Tetapi apapun sebabnya, Remitano beroperasi di Malaysia (dan banyak negara lain) dan malah adalah amat popular!

Dalam masa yang sama, jenis-jenis Altcoin yang boleh dibeli di Luno dan Remitano adalah terhad buat masa ini. Sebagai contoh, semasa buku ini diterbitkan, anda hanya boleh membeli Bitcoin, Ethereum, EOS, BNB, Cardano, Stellar dan Tron di Remitano.

Jika anda ingin membeli Altcoin yang lain, umpamanya Nexo, anda terpaksalah membelinya di *exchange* yang berpangkalan di luar negara. Dan selalunya, anda terpaksa mendepositkan Dolar Amerika ataupun Bitcoin ke dalam *wallet* anda di *exchange* tersebut dahulu sebelum boleh menjual beli. Sebagai contoh, anda buka akaun dan seterusnya *wallet* di Binance.com. Anda deposit Bitcoin ke dalam *wallet* anda di sana, dan kemudian barulah anda boleh membeli Nexo dengan menggunakan Bitcoin yang berada dalam *wallet* anda itu.

Jadi oleh kerana tidak semua *cryptocurrency* disenaraikan di semua *exchange*, ini bermakna anda perlulah mendaftar dengan beberapa *exchange* yang berbeza jika anda ingin mendapatkan pelbagai *cryptocurrency*.

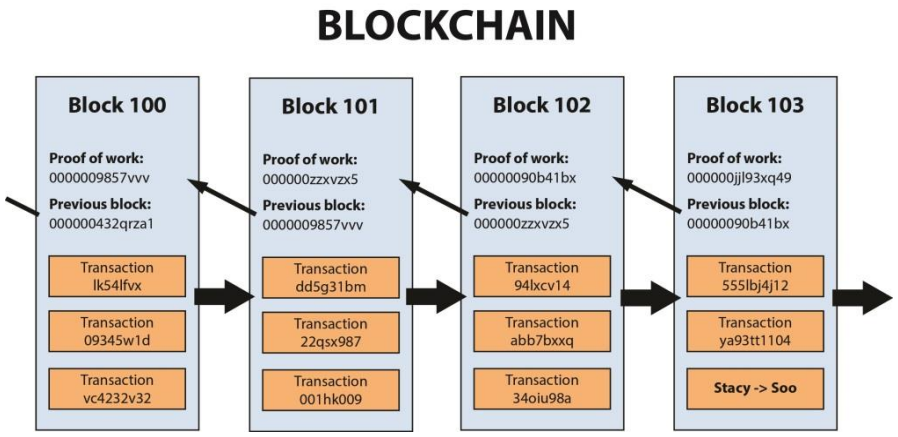
Cryptocurrency yang lebih popular seperti Bitcoin, Ethereum, Litecoin dan Dash mungkin ada di *exchange* yang sama. Tetapi jika anda ingin membeli Altcoin yang samar, maka anda perlulah membuka akaun di *exchange* yang lain.

Bunyinya mungkin rumit sikit tapi realitinya tidak begitu. Ingat yang anda hanya perlu menekan butang di komputer atau di telefon sahaja untuk menjual beli Altcoin. Anda bukannya perlu berhujan panas di sawah untuk menjana semua wang ini!

11. APAKAH ITU *BLOCKCHAIN*?

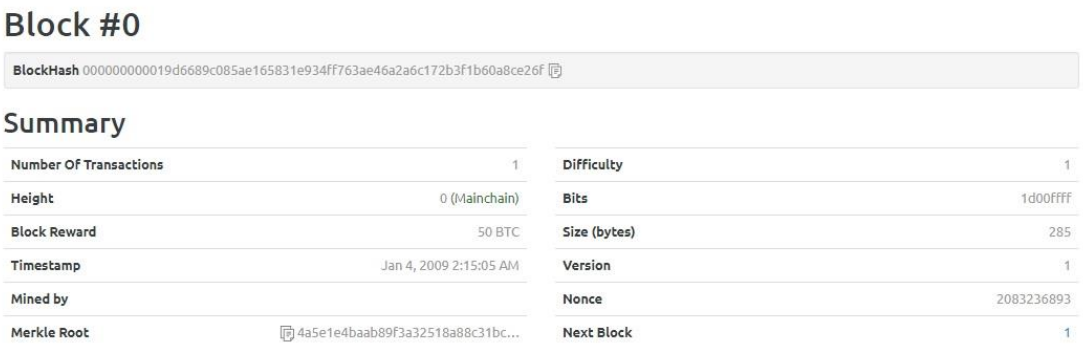
Saya akan menggunakan Bitcoin untuk menjawab soalan ini. Anda tidak perlu risau kerana jawapan yang sama boleh diaplikasikan kepada Altcoin juga.

Seperti yang saya ceritakan dalam jawapan tentang *mining*, koleksi komputer-komputer *mining* mengumpulkan beberapa ratus transaksi urus niaga Bitcoin yang belum diproseskan ke dalam satu blok dan menukarkannya kepada masalah matematik. Apabila kumpulan *miner* berjaya menyelesaikan masalah matematik tersebut, mereka akan memberikan kelulusan untuk blok tersebut ditambah kepada lejar. Mereka kemudiannya akan memulakan usaha untuk menyelesaikan masalah matematik di blok yang berikutnya. Jadi blok itu bersambung-sambung. Itulah sebabnya blok-blok itu ditermakan sebagai *blockchain*.



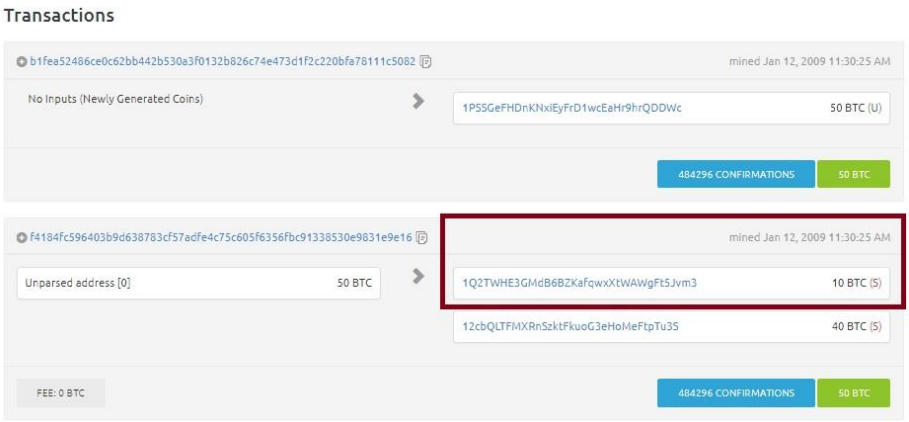
Grafik 11.1: Graf *Blockchain*

Sebenarnya *blockchain* ini ialah lejar di mana semua transaksi Bitcoin direkodkan. Tetapi berlainan dengan kebanyakan lejar yang maklumatnya dirahsiakan, *blockchain* ialah lejar awam yang telus dan terbuka. Jadi semua transaksi Bitcoin direkodkan dan boleh diakses oleh sesiapa. Saya ulang ya, kerana poin ini amat penting dan juga menarik: semua transaksi Bitcoin direkodkan dan boleh diakses oleh sesiapa sahaja. (Jika anda ingin melihatnya dengan mata anda sendiri, sila login ke https://blockexplorer.com.) Sebagai contoh dan untuk hiburan anda, grafik 11.2 ialah *screenshot* terbitan Bitcoin yang pertama dalam sejarah. Blok #0 ini (kini dikenali sebagai Genesis Block) diterbitkan oleh pengasas Bitcoin Satoshi Nakamoto pada pukul 2.15 pagi 4 Januari 2009. Seperti yang tertera dalam *screenshot* tersebut, ganjaran Nakamoto ialah 50 Bitcoin.



Grafik 11.2: Blok #0 Bitcoin (juga dikenali sebagai Genesis Block)

Berikut pula merupakan transaksi Bitcoin yang pertama (jika kita menolak transaksi yang dibuat oleh Nakamoto kepada dirinya sendiri). Transaksi tersebut disahkan dalam blok #170 pada 12 Januari 2009 dan merupakan ganjaran 10 Bitcoin yang diberikan oleh Nakamoto kepada Hal Finney.



Grafik 11.3: Blok #170 Bitcoin

Lagi satu poin yang menarik adalah setelah sesuatu transaksi direkodkan dalam sesuatu blok dan blok tersebut disahkan oleh para *miner*, ianya menjadi teramat susah untuk transaksi tersebut diedit, diubah atau dibatalkan oleh sesiapa. Dan apabila enam blok berikutnya telah disahkan oleh para *miner*, ianya menjadi mustahil untuk transaksi dan blok tersebut diedit, diubah atau dibatalkan.

Kedua-dua poin ini menjadikan Bitcoin telus, terbuka, adil dan saksama.

Sesiapa yang tak jatuh hati dengan Bitcoin selepas membaca ayat di atas merupakan seorang (a) penjahat, (b) yang telah mati, atau (c) penjahat yang telah mati!

Sudah tentunya cerita tentang *blockchain* tidak akan sempurna jika saya tidak menyentuh tentang Ethereum.

Seperti Bitcoin, Ethereum ialah rangkaian *blockchain* awam. Walaupun terdapat beberapa perbezaan teknikal di antara kedua-duanya, perbezaan yang paling nyata ialah Bitcoin dan Ethereum berbeza dari segi tujuan dan keupayaan. Bitcoin menawarkan hanya satu aplikasi di *blockchain*nya – sistem wang tunai elektronik *peer-to-peer* yang membolehkan pembayaran Bitcoin atas talian. *Blockchain* Ethereum pula menumpukan kepada menjalankan kod pengaturcaraan sebarang aplikasi *decentralized*.

Inovasi teras Ethereum, Ethereum Virtual Machine (EVM) ialah perisian lengkap Turing yang berfungsi di rangkaian Ethereum. Ia membolehkan sesiapa sahaja untuk menjalankan sebarang program, tanpa mengira bahasa pengaturcaraannya. Jadi EVM membuatkan proses membina aplikasi *blockchain* lebih mudah, cepat dan efisien daripada sebelumnya.

Dan sepertimana anda sudah tahu, peluang yang ditawarkan oleh Ethereum disambut dengan rakus dan gembira oleh pemaju. Ratusan dan malah ribuan aplikasi telah dicipta di *blockchain* Ethereum!

Saya sambung cerita sikit: konsep *blockchain* yang merupakan lejar awam yang telus, terbuka, boleh diakses oleh sesiapa tetapi tidak boleh diedit atau ditukar, dan kekal selama-lamanya membuatkannya begitu menarik kepada dunia. Dan mana-mana perkhidmatan yang berpusat boleh di-*decentralized*-kan dengan menggunakan Ethereum. Jadi sekarang konsep *blockchain* dikembangkan dalam pelbagai industri termasuklah muzik (menjejak hakcipta), hartanah, perpustakaan, jaringan sosial, *cloud storage* dan malah proses mengundi!

Berikut ialah contoh empat syarikat/organisasi yang menggunakan teknologi *blockchain* di luar industri kewangan:

- Voatz adalah platform mengundi mudah alih yang menggunakan teknologi *blockchain*. Berpangkalan di Amerika Syarikat, Voatz membuatkan penyertaan pilihan raya lebih senang dan mudah dengan membolehkan pengundian melalui *smartphone*.

- Syarikat Lemonade menggabungkan *artificial intelligence* dan *blockchain* untuk membantu pengguna membeli insurans penyewa dan insurans pemilik rumah pada kadar yang berpatutan.

- IBM ialah syarikat terbesar di dunia (buat masa ini) yang menggunakan teknologi *blockchain*. Syarikat gergasi ini sedang memimpin jalan bagi bisnes-bisnes untuk mengintegrasikan *hyperledger* dan *cloud* IBM ke dalam sistem mereka.
- Learning Machine telah mencipta Blockcerts – rangkaian *blockchain* di mana pengguna boleh menyimpan semua dokumen pencapaian dan kelayakan mereka (resume, sijil profesional, sejarah pendidikan) dengan selamat.

12. BOLEHKAH TRANSAKSI ALTCOIN DIBATALKAN?

Sepertimana transaksi Bitcoin yang telah berlaku dan disahkan tidak boleh dibatalkan, begitulah juga situasinya dalam Altcoin.

Saya akan menggunakan contoh Bitcoin sekali lagi di sini. Dan lagi sekali juga, konsep yang sama boleh diaplikasikan kepada semua Altcoin juga.

Transaksi yang berlaku di blok berikutnya mungkin masih boleh diedit. (Saya perlu tambah yang peluang untuk situasi ini berlaku adalah amat tipis kerana si *hacker* perlu menguasai lebih 51 peratus daripada kuasa daya semua komputer dalam jaringan Bitcoin!)

Sebagai contoh, kita berada di blok 100 sekarang. Transaksi berikutnya ialah blok 101 (sudah tentu!). Apabila blok 100 disahkan oleh para *miner*, transaksi yang berlaku di blok tersebut mungkin masih boleh diedit (walaupun peluang untuk situasi ini berlaku adalah amat tipis sekali). Tetapi setelah enam blok berikutnya disahkan, dan kita sampai ke blok 106, semua transaksi dalam blok 100 memang tidak dapat diedit, ditukar, dibatalkan atau diubah lagi. Ianya kekal sehingga ke akhir zaman!

Situasi ini menerangkan mengapa sesetengah bisnes menunggu enam pengesahan (blok) berlaku sebelum memenuhi sesuatu pesanan.

Kesimpulannya ialah semua transaksi Bitcoin yang telah diambil tidak boleh dibatalkan. Malah transaksi itu tidak boleh ditarik balik walaupun blok itu belum mendapat pengesahan daripada pihak *miner*. Sebaik sahaja anda menghantarnya, Bitcoin itu pergi buat selama-lamanya! Tidak ada jalan kembali di sini, *bro*!

Oleh sebab itulah situasinya, anda perlu periksa dan periksa sekali lagi yang jumlah Bitcoin dan alamat penghantaran itu adalah betul kerana sebaik sahaja transaksi itu berlaku, ianya kekal untuk selamanya!

Ya, ini memang kes yang serius, *bro*! Jadi berhati-hatilah sebelum menekan butang '*send*' itu, ya!

Perbezaan antara Bitcoin dan Altcoin di sini adalah mungkin jumlah dan masa pengesahan blok sahaja. Proses yang lain serupa sahaja.

13. BOLEHKAH ALTCOIN DIGODAM?

Salah satu isu penting dalam dunia internet ialah tahap sekuriti. Dan oleh sebab Altcoin wujud di internet, isu sekuriti adalah amat penting dan malah kritikal.

Jawapan kepada soalan "Bolehkah Altcoin digodam?" ialah, "Tidak boleh!"

"Mengapa tidak boleh?" Inilah soalan yang sering ditanya oleh pengkritik-pengkritik Altcoin. Mereka tidak percaya atau tidak mahu percaya yang Altcoin tidak boleh digodam!

Jawapan pertamanya adalah kerana Altcoin wujud dalam rangkaian (*network*) yang *decentralized* dan tidak mempunyai pusat untuk *hacker* menyerang protokolnya. Walaupun pengguna individu boleh digodam, tetapi serangan itu tidak akan menjejaskan rangkaian Altcoin itu sendiri. Malah jika semua pengguna Altcoin di Malaysia digodam pada masa yang sama, rangkaian Altcoin akan terus beroperasi seperti sedia kala!

Jawapan keduanya adalah kerana rangkaian Altcoin menggunakan tahap kriptografi yang tinggi untuk memastikan integriti *blockchain* dan transaksi-transaksi Altcoin. Walaupun tahap kriptografi itu boleh digodam secara teori, ianya adalah mustahil untuk dilakukannya kerana ia memerlukan gabungan kuasa pemprosesan kesemua super-komputer yang wujud di dunia dan mengambil masa beratus-ratus tahun hanya untuk mempunyai peluang melakukannya. Dalam kata lain, situasi ini tidak akan berlaku!

Sebenarnya, para *hacker* telah cuba untuk menggodam Bitcoin sejak dari tahun 2009 lagi! Dan saya pasti ada *hacker* yang masih terus-menerus mencuba untuk menggodam Bitcoin dan Altcoin sampai sekarang – kerana ganjaran yang amat besar menunggu mereka sekiranya mereka berjaya melakukannya. Ini termasuklah *hacker* yang terulung di dunia juga. Tetapi sehingga hari ini, tidak ada siapa yang berjaya melakukannya.

Jadi sekali lagi, ianya adalah mustahil untuk rangkaian Altcoin digodam.

Apa yang boleh (dan pernah) berlaku ialah pengguna individu, *exchange* dan pembekal *wallet online* diserang *hacker*. Serangan ini mengakibatkan mereka kehilangan Bitcoin dan Altcoin yang mereka simpan di *wallet online* tersebut.

Sebagai contoh, *exchange* Mt. Gox (sebuah *exchange* yang popular satu masa dulu) telah digodam pada tahun 2014 yang mengakibatkan kehilangan 650,000 Bitcoin.

Kes penggodaman yang terkini berlaku pada bulan Februari 2020 di mana seorang pelabur di China telah kehilangan Bitcoin (BTC) dan Bitcoin Cash (BCH) yang bernilai $42 juta. Apa yang menariknya ialah kes penggodaman itu berlaku melalui proses *sim swap* telefon! Apa yang menambah menariknya ialah fakta si pelabur menyimpan data

cryptocurrency yang bernilai $42 juta itu dalam telefon beliau! Ramai orang akan berkata yang si pelabur ni memang nak cari penyakit!

Kes penggodaman Altcoin yang paling serius berlaku pada tahun 2016. Pada tahun 2016, satu DAO (Decentralized Autonomous Organization) telah mengutip $150 juta dalam IPO untuk mengusahakan *smart contract* di platform Ethereum. Bagaimanapun, DAO tersebut telah dieksploitasi pada bulan Jun apabila Ether bernilai $50 juta telah digodam seorang *hacker*. Insiden ini telah mencetuskan pertikaian yang kronik dalam komuniti crypto mengenai sama ada Ethereum harus melakukan *hard fork* untuk mengembalikan dana yang terjejas. Akibat pertikaian ini, rangkaian Ethereum berpecah dua: Ethereum (ETH) diteruskan pada blok yang telah di-*forked*, manakala Ethereum Classic (ETC) diteruskan pada blok asal.

Akhirnya, inilah rumusan bab ini – sepertimana rangkaian Bitcoin tidak boleh digodam, rangkaian Altcoin juga tidak boleh digodam.

14. APAKAH PERBEZAAN ANTARA POW, POS DAN DPOS?

Sebelum menerangkan apakah itu POW, POS dan DPOS, saya akan terangkan dulu kepentingan konsensus algoritma dalam dunia *cryptocurrency*.

Konsensus algoritma bukan sahaja penting tetapi ianya merupakan salah satu asas dalam dunia *cryptocurrency*. Ini adalah kerana konsensus algoritma menentukan segalanya daripada keselamatan rangkaian ke kelajuan pengesahan hingga ke keramahan alam sekitar! Konsensus algoritma menentukan bagaimana urus niaga disahkan, diluluskan dan direkodkan dalam *blockchain* dan bagaimana rekod tersebut dikekalkan untuk satu tempoh yang tertentu.

Oleh sebab *cryptocurrency* tidak mempunyai pusat dan pekerja, tugas untuk mendapatkan konsensus algoritma itu dilakukan oleh rangkaian pengguna yang dipanggil sebagai '*node*' atau lebih terkenal sebagai '*miner*'. Dan mereka ini perlu bersetuju dengan kesahihan data yang ditambahkan pada lejar berpandukan kepada set peraturan yang telah ditetapkan dalam sesuatu *blockchain*. Persetujuan dan kesepakatan perlu dicapai daripada majoriti *node* untuk mendapatkan konsensus.

Perenggan di atas ini dipersetujui oleh semua yang terlibat dalam dunia *cryptocurrency*. Tidak ada masalah di sini.

Apa yang menjadi masalah dan perdebatan (yang masih berterusan sehingga kini!) ialah jenis proses untuk mencapai persetujuan tersebut. Dan buat masa ini, terdapat empat jenis proses yang berbeza iaitu *Proof Of Work* (POW), *Proof Of Stake* (POS), *Delegated Proof Of Stake* (DPOS) dan yang terkini, Platform Generasi Ketiga (PGK).

Proof Of Work (POW)

Konsensus algoritma yang pertama dalam dunia *cryptocurrency* ialah POW yang muncul bersama-sama dengan Bitcoin pada tahun 2009.

Seperti namanya, *Proof Of Work* memerlukan setiap *miner* yang berjaya menambahkan blok membuktikan bahawa mereka telah melakukan usaha menyelesaikan masalah kriptografi di *blockchain*. POW ini adalah juga satu cara untuk meningkatkan tahap sekuriti rangkaian daripada serangan spam dan *Distributed Denial Of Services* (DDOS).

Sistem POW meletakkan para *miner* untuk bersaing sesama mereka untuk mencipta blok transaksi yang berikutnya. Setiap *miner* menggunakan sumber komputasinya sendiri untuk menyelesaikan masalah kriptografi yang kompleks. *Miner* yang berjaya menyelesaikan masalah tersebut akan mengesahkan transaksi dan kemudian

menambahkan blok di *blockchain*. Dan *miner* tersebut menerima *cryptocurrency* yang disertainya itu sebagai ganjaran untuk masa dan tenaga yang telah dibelanjakan. Sebagai contoh, buat masa ini, *miner* Bitcoin yang berjaya menambah blok menerima ganjaran 12.5 Bitcoin.

Sistem ganjaran ini memberi insentif kepada *miner* untuk menghasilkan penyelesaian yang tepat dan memastikan rangkaian tetap terjamin.

Walaupun POW merupakan teknologi yang canggih semasa ianya diperkenalkan, sistem POW mempunyai beberapa batasan dan kekurangan. Ianya perlahan, tidak *scalable*, memerlukan kos yang tinggi (untuk membeli komputer ASIC) dan menggunakan kuasa elektrik yang tinggi.

Dan untuk menambahkan masalahnya, sistem POW ini menjadi semakin berpusat sejak beberapa tahun kebelakangan ini dengan kewujudan kumpulan perlombongan gergasi seperti AntPool dan BTC.com yang menguasai industri *mining* (hampir 50% daripada kuasa *hash*). Dan oleh kerana kedua-dua *mining pool* tadi dikuasai oleh syarikat Bitmain, ini bermakna POW sekarang menjadi amat berpusat. Ini boleh menimbulkan masalah kerana ia mewujudkan satu pusat kegagalan.

POW digunakan oleh lebih 100 *cryptocurrency* termasuklah Bitcoin, Bitcoin Cash, Litecoin, Dogecoin, Monero dan Ethereum (buat masa ini).

Proof Of Stake **(POS)**

POS muncul pada tahun 2012 sebagai penyelesaian kepada masalah kos, masalah ketidakcekapan dan kerentanan terhadap *centralization* yang menghantui POW. Premis asasnya adalah daripada membeli peralatan yang mahal untuk melombong, setiap '*validator*' atau lebih dikenali sebagai '*forger*' (kedua-dua istilah ini menggantikan istilah '*miner*' di POW) membeli *coin* yang digunakan dalam rangkaian *blockchain* yang mereka sertai itu. Situasi ini sudah tentu lebih baik untuk *coin* tersebut kerana bukan sahaja *coin* itu digunakan tetapi disokong oleh pengguna-pengguna rangkaian itu sendiri. (Ramai *miner* dalam sistem POW tidak memiliki *coin* yang mereka lombong itu! Mereka melombong tetapi tidak menggunakan *coin* tersebut.)

Di bawah algoritma POS, mereka yang ingin menjadi *forger* dalam sesuatu ekosistem akan mengunci beberapa *coin* mereka sebagai tanda kepentingan mereka di dalam sistem tersebut. Kemudian, *forger* yang spesifik dipilih untuk mengesahkan blok baru setiap beberapa saat atau minit. Dan untuk menambahkan tarikannya, *forger* yang memegang lebih banyak *coin* mempunyai kuasa yang lebih besar dalam POS. Dalam kata lain, pemilihan menjadi *forger* memihak kepada mereka yang mempunyai *coin* yang banyak.

Sistem in meningkatkan tahap sekuriti kerana mereka yang telah banyak melabur dalam rangkaian akan memastikan *coin* dan rangkaian tersebut kekal selamat kerana merekalah yang akan menanggung kerugian yang terbesar sekiranya berlaku sebarang kecelakaan.

Satu lagi poin positif ialah kos komputasi dalam sistem POS adalah jauh lebih rendah jika dibandingkan dengan POW. Malah kerja komputasi POS boleh dilakukan oleh komputer biasa sahaja; tidak ada keperluan membeli alat dan komputer yang mahal seperti di sistem POW.

POS digunakan oleh lebih 100 *cryptocurrency* termasuklah Binance Coin, Dash, NEO, Digibyte, OmiseGo dan Waves.

***Delegated Proof Of Stake* (DPOS)**

Salah satu perkembangan menarik dalam *blockchain* adalah kemunculan sistem *Delegated Proof of Stake* (POS). DPOS telah diperkenalkan pada tahun 2014 oleh seorang jurutera *blockchain* bernama Daniel Larimer. Daniel sedar bahawa proses melombong Bitcoin membazir tenaga dan juga masa. Beliau juga sedar bahawa perlombongan Bitcoin akan menjadi berpusat pada masa akan datang, dikuasai oleh kumpulan perlombongan gergasi.

Di samping itu, beliau mahu membina sebuah sistem yang mampu menampung kelajuan transaksi yang tinggi, mungkin mencapai 100,000 transaksi sesaat! Sistem Bitcoin terlalu perlahan kerana cara ia dicipta dan sistem POW yang digunakan. Beliau memutuskan untuk mencipta dan membina sebuah sistem baru yang menggunakan tenaga elektrik yang sangat sedikit, cepat bagaikan kilat dan juga sangat selamat. Daniel menamakan sistem baru ini, *Delegated Proof Of Stake* atau DPOS.

Apa yang menariknya ialah DPOS menggunakan sistem demokrasi!

Ini adalah kerana pemilik token di dalam komuniti sesuatu *cryptocurrency* membuat pengundian untuk memilih wakil yang dipanggil sebagai *delegate* atau *witness*. Dan oleh sebab tugas utama *delegate* ialah untuk menjamin keselamatan rangkaian *cryptocurrency* tersebut, pemilik token perlulah membuat pemilihan tersebut dengan berhati-hati – sebiji macam pilihan raya umum juga!

Dalam beberapa versi DPOS, *delegate* perlu menunjukkan komitmen mereka dengan mendepositkan dana (*coin*) sebagai cagaran di dalam akaun keselamatan yang dikunci masa. Jika mereka berlaku pelik atau berniat jahat, *coin* tersebut akan dirampas! Jadi sistem ini juga menambahkan tahap sekuriti rangkaian.

Seperti dalam sistem POS, pemilik yang mempunyai lebih banyak token akan lebih mempengaruhi rangkaian daripada orang yang mempunyai token yang sedikit. Dan apabila jumlah peserta bertambah, ia menjadi lebih sukar dan sukar untuk kekal sebagai *delegate* yang dibayar disebabkan persaingan yang meningkat.

"Mengapa seseorang itu mahu menjadi seorang *delegate*?" Anda mungkin bertanya.

Jawapannya adalah kerana beliau dibayar untuk menjadi *delegate*. Sebagai contoh, dalam *blockchain* Steem, 100 *delegate* teratas mendapat bayaran dan malah 20 teratas mendapat gaji tetap! Jadi ramai peserta yang nak jadi *delegate*!

Sekiranya *delegate* mula berlaku pelik, atau tidak melakukan tugasnya dengan baik, para peserta boleh mengundi mereka keluar, dan mengantikannya dengan *delegate* yang baru. Proses pengundian ini juga berterusan, jadi para *delegate* perlulah melakukan tugas mereka dengan baik secara konsisten.

DPOS dikatakan lebih adil kerana kewujudan sistem pengundian ini.

DPOS ini juga lebih efisien jika dibandingkan dengan POW. Sebagai contoh, masa yang diperlukan untuk mengesahkan blok dalam Lisk hanyalah 10 saat berbanding dengan 10 minit dalam Bitcoin.

Istilah '*mining*' juga tidak digunakan dalam DPOS; ianya digantikan dengan '*forging*' sepertimana dalam sistem POS.

Malangnya walaupun POS dan DPOS mempunyai beberapa kelebihan jika dibandingkan dengan POW, kedua-dua sistem ini pun masih boleh menjadi *centralized*. Oleh sebab kuasa mengundi berpihak kepada mereka yang memiliki jumlah *coin* yang banyak, yang secara langsungnya bermakna entiti yang kaya seperti bank, syarikat gergasi, *billionaires* dan malah agensi kerajaan, ini bermakna merekalah yang akan menguasai *coin* tertentu. Ini membawa kepada *centralization*.

DPOS digunakan oleh lebih 20 *cryptocurrency* termasuklah Steem, EOS, NEO, TRON dan Tezos.

Platform Generasi Ketiga (PGK)

Saya rasa anda pasti sedar yang ketiga-tiga sistem POW, POS dan DPOS masih mempunyai kekurangan. Dalam kecanggihan masih ada kekurangannya! Ini termasuklah masalah *scalability* dan *centralization*.

Jadi ianya tidaklah menghairankan apabila beberapa individu dan kumpulan telah mencipta sistem konsensus algoritma mereka sendiri untuk menangani masalah dan kekurangan yang wujud dalam ketiga sistem algoritma tadi. Mereka (dan juga kita!) mahukan konsensus algoritma yang mempunyai semua ciri-ciri idaman tanpa kekurangan yang wujud sekarang.

Lalu muncullah Platform Generasi Ketiga (PGK) yang digunakan oleh beberapa Altcoin terkini. Platform ini menggunakan pendekatan-pendekatan unik yang mempunyai banyak kelebihan dan tanpa kekurangan yang wujud di dalam sistem POW, POS dan DPOS.

PGK menawarkan ciri-ciri berikut:

- Transaksi segera.
- *Scalability* yang hampir tanpa had.
- *Decentralization* yang hampir tanpa had.
- Penggunaan kuasa yang amat minimal.
- Pemindahan data yang selamat.
- Tiada fi!

Jadi PGK ini merupakan platform idaman!

Berikut ialah contoh-contoh platform PGK dan *coin* yang menggunakannya:

- Tangle – IOTA.
- Block Lattice – Nano.
- Side-chain scaling architechture – Cardano.
- Stellar Consensus Protocol – Stellar.
- Proof of Importance – NEM.

Besar kemungkinannya yang *coin-coin* yang menggunakan PGK ini akan menjadi lebih popular pada masa depan!

15. MENGAPAKAH *DECENTRALIZATION* ITU PENTING?

Anda akan sering terjumpa istilah '*decentralization*' dalam dunia *cryptocurrency*. (Saya sendiri telah menyebutnya berkali-kali dalam buku ini!) Malah hampir semua *cryptocurrency* akan menyebut istilah ini di laman web dan *whitepaper* mereka. Jadi anda mungkin hairan mengapa ia menjadi kata kunci dan mengapa ia begitu kritikal?

Apa-apa yang *centralized* bermakna ianya mempunyai pusat. Atau markas di mana keputusan dibuat dan rekod disimpan. Situasi ini menyenangkan kerja, merendahkan kos operasi dan paling utama, memudahkan kawalan. Malangnya, *centralized* juga bermakna ianya mudah untuk diceroboh, dan juga senang untuk penyelewengan berlaku.

Decentralization adalah sebaliknya: tidak ada pusat dan malah rekod disimpan di banyak tempat yang berbeza. Ini tidak bermakna tidak ada kawalan; kawalan itu masih ada, cuma ianya diselenggarakan oleh sistem dan banyak mata.

Decentralization adalah penting kerana ia menghapuskan kegagalan dan kawalan tunggal. Malah satu, dua atau sepuluh poin boleh diserang atau gagal tetapi ianya tidak memberi kesan kepada sistem tersebut. Situasi begini membuat penyelewengan dalaman serta serangan luar tidak praktikal kerana ianya akan memerlukan kos yang tinggi dan kerja yang amat banyak.

Platform ini juga tidak memerlukan pembabitan orang tengah yang membawa kepada kos yang lebih rendah untuk pengguna.

Satu contoh sistem yang *decentralized* ialah internet. Kegagalan satu, sepuluh malah seribu komputer pun tidak akan menjejaskan operasi internet.

Begitulah juga situasi dengan *cryptocurrency* yang *decentralized*. Oleh sebab *node coin-coin* tersebut berjumlah ratusan atau ribuan komputer yang terletak di serata dunia, kegagalan satu, sepuluh malah seribu *node* pun tidak akan menjejaskan operasi *coin* tersebut. Penyelewengan, penyubahatan dan pencerobohan oleh orang dalam juga susah berlaku dan malah mungkin tidak boleh berlaku langsung!

Inilah sebabnya *decentralization* menjadi kata kunci dalam dunia *cryptocurrency*.

Semasa saya menulis buku ini, Bitcoin mempunyai 11,000 *node* (jumlah yang tertinggi dalam dunia *cryptocurrency*) sementara Ethereum mempunyai 9,000 *node*. Jadi kedua-dua *coin* ini dikira amat *decentralized*.

Coin yang sebaliknya pun wujud juga! Sebagai contoh, EOS mempunyai 21 *node* sementara NEO mempunyai hanya 7 *node*!

Jadi agak-agaknya *coin* yang mana satu yang akan menjadi sasaran penjahat – *coin* yang mempunyai 11,000 *node* atau yang mempunyai 7 *node*?

16. BAGAIMANA HENDAK MENGIRA *DECENTRALIZATION*?

Terdapat empat faktor untuk mengira *decentralization*:

1) Jumlah *voting node* yang tinggi

Jumlah *voting node* menentukan tahap *decentralization* sesuatu sistem. Lebih tinggi jumlahnya, lebih *decentralized*. Seperti yang dinyatakan sebelum ini, Bitcoin mempunyai lebih 11,000 *node* sementara Ethereum mempunyai 9,000 *node*. Walaupun kedua jumlah tersebut tidaklah sempurna, tetapi tahapnya sudah boleh dikira sebagai bagus.

Jumlah *node* 1,000 dikira okay sahaja. Jadi ini bermakna mana-mana *coin*/token yang mempunyai *voting node* kurang daripada jumlah ini macam bagi cukup syarat sahaja.

Dan sudah tentunya, NEO, Ark dan XRP yang mempunyai hanya beberapa dozen *voting node* adalah teramat *centralized*.

2) *Trustless* dan *permissionless*

Network yang memerlukan kebenaran dan kepercayaan (seperti EOS, Lisk dan XRP) boleh berfungsi dengan lebih cepat kerana koleksi *node* dalam sistem begini boleh meluluskan transaksi dengan cepat (kerana *node-node* itu sudah mempercayai sesama mereka). Malangnya, situasi ini menjadikan sistem tersebut amat *centralized* dan juga kurang selamat.

Sebaliknya, *node* di dalam *network* yang *trustless* dan *permissionless* tidak mengenali sesama mereka. Identiti mereka kekal sebagai rahsia. Jadi *node-node* ini tidak dapat membina kartel. Inilah situasi yang kita semua kehendaki.

Ini bermakna *network* yang *trustless* dan *permissionless* adalah lebih *decentralized*.

3) Tidak ada *mining* atau *staking pool*

Ya, poin di atas itu betul – tidak ada *mining* atau *staking pool*!

“Tapi Bitcoin dan banyak *coin* yang lain mempunyai *mining* atau *staking pool*. Bagaimana tu?” Anda mungkin bertanya.

Jawapannya adalah kerana semua *coin* POW yang mempunyai *mining* atau *staking pool* sebenarnya berada di dalam situasi *centralized* juga. Situasi ini timbul kerana 45% kuasa undian berada di tangan syarikat Bitmain (yang menguasai AntPool dan BTC.com – dua *mining pool* Bitcoin yang terbesar di dunia).

Ini bermakna yang sesiapa yang ingin menjadi maharaja dunia (!) hanya perlu menguasai Bitmain selama beberapa minit dan kemudian mendapatkan 5% lagi kuasa undian dari tempat lain, dan mereka sudah menguasai Bitcoin dan malah semua *coin* POW!

Walaupun situasi di atas menjadi situasi idaman untuk bakal maharaja itu, ianya menjadi situasi celaka untuk orang lain!

4) Pembahagian bekalan yang serata

Terdapat dua sebab mengapa pembahagian bekalan *coin*/token yang serata adalah penting dalam sesuatu sistem.

Dalam sistem POS di mana jumlah *coin* yang anda miliki menentukan undian (lebih banyak *coin* memberikan lebih banyak kuasa undi), fakta ini menjadi amat penting. Oleh sebab kuasa dimiliki oleh sesiapa yang mengawal 51% daripada kuasa undian, ini bermakna mereka yang memiliki lebih daripada angka ini akan mengawal *coin*/token tersebut dan boleh melakukan apa sahaja. Jadi situasi ini adalah tidak *decentralized*.

Dalam sistem di mana undian tidak bergantung kepada jumlah *coin* yang dimiliki (contohnya POW), ia memberi peluang kepada mereka yang memiliki jumlah *coin* yang banyak untuk memanipulasikan harga. Sebagai contoh, mereka boleh menjual *coin* secara borong yang menyebabkan harga *coin* itu menjunam, dan kemudiannya mereka membeli balik *coin* tersebut sewaktu harganya rendah. Situasi ini juga membawa kepada *centralization*, yang membuatkan *coin* tersebut kurang menyerlah sebagai mata wang.

Rumusannya ialah hampir semua *cryptocurrency* gagal tiga daripada empat faktor ini. Contohnya ialah EOS, Ontology, Lisk, Ark, Stellar, NEO dan XRP, yang *permissioned*, *trusted*, mempunyai hanya 20-50 *node* dan lebih daripada 50% daripada bekalan dikuasai oleh satu entiti. Satu-satunya kriteria yang mereka tidak miliki ialah *mining pool*.

Semua *coin* POW gagal kerana pembahagian bekalan yang tidak serata serta mempunyai *mining pool* walaupun mereka adalah *permissionless*, *trustless* dan mempunyai bilangan *node* yang tinggi.

Semua *coin* POS juga gagal kerana pembahagian bekalan yang tidak serata walaupun mereka adalah *permissionless*, *trustless*, mempunyai bilangan *node* yang tinggi dan tidak mempunyai *mining* atau *staking pool* (kecuali Cardano yang mempunyai *staking pool*).

Hanya segelintir Altcoin yang mempunyai semua empat faktor *decentralization*: Elastos, Holochain, IOTA, Nexus dan QuarkChain.

17. APAKAH MAKSUD '*PERMISSIONLESS*', '*TRUSTLESS*' DAN APAKAH PERBEZAAN ANTARA KEDUA-DUANYA?

Seperti istilahnya, '*permissionless*' bermakna kita tidak perlu meminta atau mendapat kebenaran daripada mana-mana pihak untuk menambah blok di *blockchain*. Ini bermakna sesiapa sahaja boleh menambah blok di *blockchain* tersebut.

'*Trustless*' pula tidak bermakna *coin*/token atau *blockchain* tersebut tidak boleh dipercayai! Maksud *trustless* di sini ialah kita tidak perlu mempercayai *node-node* yang lain untuk mendapatkan konsensus dan untuk sistem tersebut berfungsi. Semuanya berfungsi dengan sempurna tanpa penipuan atau penyelewengan (kerana sistemnya menghapuskan keperluan untuk kepercayaan). Jadi kepercayaan tidak menjadi sesuatu keperluan dalam sistem tersebut.

Ini bermakna yang *trustless* adalah sejenis *permissionless*. Perbezaan antara kedua-duanya ialah *permission* atau kebenaran selalunya diberikan oleh satu pihak yang selalunya merupakan syarikat yang mencipta *blockchain* tersebut (contoh Ripple, Stellar, NEO dan EOS) sementara kepercayaan diberikan oleh semua *node* dalam sistem tersebut.

Seperti yang saya sebut sebelum ini, sebenarnya *network* yang memerlukan kebenaran dan kepercayaan boleh berfungsi dengan lebih cepat kerana koleksi *node* dalam sistem begini boleh meluluskan transaksi dengan cepat (kerana *node-node* itu sudah mempercayai sesama mereka). Malangnya, situasi ini menjemput pembentukan kartel. Dan apabila kartel wujud, *network* tersebut boleh diporakperandakan dengan senang dan cepat kerana satu atau dua ahli boleh mempengaruhi *node-node* yang lain.

Tiga contoh *network* yang *trustless* dan juga *permissionless* adalah Bitcoin, Ethereum dan Litecoin.

Lima contoh network yang memerlukan *trust* dan juga *permission* ialah Ripple, List, Stellar, NEO dan EOS.

18. APAKAH PERBEZAAN ANTARA '*MINING*' DENGAN '*FORGING*'?

Saya bermula dengan istilah *mining* atau melombong dulu.

Mining

Dalam sistem kewangan tradisional, wang diterbitkan oleh Bank Negara (di Malaysia) dan staf bank merekodkan setiap deposit dan wang keluar dari akaun bank.

Tetapi Bitcoin, seperti yang kita tahu, tidak diterbitkan oleh mana-mana autoriti kewangan atau kerajaan. Bitcoin juga tidak mempunyai akauntan untuk merekodkan semua transaksi yang berlaku dalam rangkaian mereka.

Jadi bagaimana Bitcoin dicipta? Dan bagaimana semua transaksi Bitcoin diluluskan dan direkodkan?

Jawapannya ialah kedua-duanya berlaku dalam proses *mining*.

Para *miner* memproseskan transaksi (memeriksa, meluluskan serta merekodkan) Bitcoin dengan menggunakan komputer mereka untuk menyelesaikan masalah matematik. Proses ini diistilahkan sebagai *mining*. Jadi *mining* merupakan cara bagaimana Bitcoin baru diterbitkan dan juga cara bagaimana semua transaksi Bitcoin direkodkan.

Dan untuk menjelaskan situasi dengan sejelas-jelasnya, *mining* inilah satu-satunya cara bagaimana Bitcoin diterbitkan. Ini bermakna semua Bitcoin yang telah wujud dan akan wujud semunya terbit melalui proses *mining*. Jadi semua cara-cara untuk mendapatkan Bitcoin termasuk pembelian, *faucet* dan hadiah sebenarnya adalah untuk mendapatkan Bitcoin yang telah diterbitkan oleh *miner*.

Jadi sebenarnya istilah *mining* itu mungkin kurang tepat. Oleh sebab tugas mereka yang sebenarnya adalah untuk memproses dan meluluskan transaksi, mungkin istilah 'pakar memproses dan meluluskan transaksi (PMMT)' lebih tepat kut!

Grafik 18.1: Komputer Ant*miner* S9 yang digunakan khusus untuk *mining* Bitcoin

“Mengapakah *miner* melakukan semua kerja ini?” Anda mungkin bertanya.

Jawapannya, apabila mereka berjaya menyelesaikan masalah tersebut (iaitu memproseskan dan meluluskan transaksi), mereka menerima ganjaran 12.5 Bitcoin sebagai upah mereka. (Ganjaran itu ialah 50 Bitcoin per blok pada permulaannya dulu. Ianya dibahagi dua menjadi 25 Bitcoin pada bulan November 2012 dan kemudian dibahagi dua sekali lagi menjadi 12.5 Bitcoin pada bulan Julai 2016. Pembahagian dua dalam Bitcoin ini memang sudah ditetapkan oleh penciptanya, Satoshi Nakamoto. Beliau menetapkan ganjaran setiap blok dibahagi dua setiap 210,000 blok diterbitkan. Jadi pembahagian dua yang berikutnya dijangka berlaku pada bulan Mei 2020.)

Para *miner* juga mendapat sedikit ganjaran dalam bentuk fi yang dikenakan untuk memproseskan setiap transaksi dalam blok. Buat masa ini, fi adalah rendah. Tetapi fi ini dijangkakan akan naik sikit apabila semua Bitcoin telah diterbitkan pada 2140. Malah fi itulah yang akan menjadi satu-satunya ganjaran buat *miner* kerana waktu itu Bitcoin baru tidak akan diterbitkan lagi. Tetapi oleh sebab 2140 adalah lebih 120 tahun di hadapan, anda tidak perlu pening kepala memikirkan tentang poin ini lagi!

Kerja *mining* ini berlaku lebih kurang setiap 10 minit. Dalam tempoh tersebut, koleksi komputer *mining* mengumpulkan beberapa ratus transaksi urus niaga Bitcoin yang belum diproseskan ke dalam satu blok dan menukarkannya kepada masalah matematik. *Miner* yang berjaya menyelesaikan masalah matematik tersebut akan mengumumkan kejayaan tersebut kepada *miner-miner* lain yang berada di dalam *network*. Kumpulan *miner* ini akan memeriksa sama ada penjual Bitcoin memang benar memiliki Bitcoin dan berhak untuk menjual Bitcoin tersebut, dan juga memeriksa jawapan yang diberikan kepada masalah matematik tersebut adalah betul. Jika kesemua jawapannya adalah betul, mereka akan memberikan kelulusan untuk blok tersebut ditambah kepada lejar yang dinamakan *blockchain*. Kumpulan *miner* itu kemudiannya akan memulakan usaha untuk menyelesaikan masalah matematik di blok yang berikutnya. Jadi blok itu bersambung-sambung. Itulah sebabnya blok-blok itu diistilahkan sebagai *blockchain*.

Seperti yang saya tulis di atas, *miner* yang berjaya menyelesaikan masalah matematik tadi diberikan ganjaran 12.5 Bitcoin. Tetapi apa yang menariknya, walaupun mereka menerima ganjaran ini sebaik sahaja mereka berjaya menyelesaikan masalah matematiknya, mereka hanya dapat membelanjakan Bitcoin tersebut hanya selepas 99 blok lagi ditambah kepada lejar! Ini memberikan insentif kepada para *miner* untuk terus-menerus berusaha mengesahkan transaksi Bitcoin.

Sistem ini juga menambahkan tahap sekuriti Bitcoin. Untuk para *hacker* melakukan *double-spend* Bitcoin (membelanjakan Bitcoin yang sama dua kali), mereka perlu berpatah balik dan mengubahkan blok yang telah diluluskan. Dan untuk bertindak demikian, mereka perlu menguasai lebih 51 peratus kapasiti kuasa daya komputer kumpulan-kumpulan *miner*. Dan ini adalah satu kemungkinan yang amat tipis kerana kumpulan-kumpulan *miner* mempunyai antara komputer yang paling berkuasa di seluruh dunia! Kuasa komputer-komputer mereka adalah 13,000 kali lebih berkuasa berbanding dengan kuasa 500 *super*-komputer di dunia!

Ada orang yang berpendapat istilah *mining* itu digunakan kerana ia menyerupai aktiviti perlombongan komoditi lain seperti emas. *Mining* memerlukan usaha serta menambahkan jumlah mata wang baru dengan perlahan yang memang menyerupai aktiviti perlombongan emas.

Forging

Dalam sistem POS dan DPOS, istilah '*mining*' dan '*miner*' (dalam sistem POW) digantikan dengan istilah '*forging*' dan '*forger*'.

Proses mencipta blok – memeriksa, meluluskan serta merekodkan transaksi – itu masih kekal. Apa yang berbeza dalam *forging* ialah cara pemilihan dan ganjaran.

Dalam kebanyakan sistem POS, *coin* dicipta sebelum ICO (dipanggil '*pre-mined'*) dan jumlahnya sudah ditetapkan. Jadi ini bermakna semua *coin* dalam sesuatu sistem itu diterbitkan pada mulanya. Para *forger* kemudiannya menerima *coin* tersebut sebagai ganjaran untuk memproses transaksi dan menempa blok.

Untuk membolehkan dirinya menempa blok di sesuatu *blockchain*, seorang *forger* perlulah memiliki *coin* berkenaan dan kemudiannya mencagarkan sebahagian daripada *coin* tersebut. Jika beliau meluluskan transaksi yang tidak betul dalam blok, maka *coin* yang telah dicagarkan itu akan dirampas. Beliau juga tidak dibenarkan untuk memproseskan blok lagi pada masa depan. Jadi cagaran ini merupakan insentif untuk para *forger* membuat kerja dengan betul!

Sistem ini tidak menyediakan cara untuk mengendalikan pengedaran *coin* pada fasa permulaan, jadi *coin* yang menggunakan sistem ini sama ada di *pre-mined* sebelum ICO, atau mereka bermula dengan sistem POW dulu dan beralih ke sistem POS kemudian.

Dalam POS, para *forger* tidak berlawan sesama mereka seperti dalam sistem POW tetapi dipilih. Dan pilihan itu menggunakan beberapa kaedah yang berbeza. Dua kaedah yang popular adalah 'Pemilihan Rawak-Rawak' dan 'Pemilihan Berasaskan Usia *Coin*'.

Dalam pemilihan kaedah Pemilihan Rawak-Rawak, formula digunakan untuk mencari *forger* berikutnya berdasarkan gabungan nilai *hash* terendah dan saiz pegangan *coin*. Dan oleh kerana saiz pegangan *coin* merupakan info umum, setiap *node* biasanya dapat meramalkan *forger* yang mana akan dipilih untuk menempa blok seterusnya.

BlackCoin (BLK) dan Nxt (NXT) adalah dua contoh *coin* yang menggunakan kaedah Pemilihan Rawak-Rawak.

Seperti namanya, sistem berasaskan usia *coin* memilih *forger* seterusnya berdasarkan usia *coin* yang telah dicagarkan oleh si *forger*. Usia *coin* dikira dengan mendarabkan jumlah hari *coin* yang dicagarkan dengan bilangan *coin* yang dicagarkan. Dan *coin* tersebut mestilah berusia sekurang-kurangnya 30 hari sebelum mereka boleh dikira untuk menempa blok. *Forger* yang telah mencagarkan jumlah *coin* yang lebih banyak dan usia *coin* yang lebih tua mempunyai peluang yang lebih besar dipilih untuk menempa blok seterusnya.

Sebaik sahaja *forger* mencipta blok, usia *coin* mereka ditetapkan semula kepada sifar dan mereka mesti menunggu sekurang-kurangnya 30 hari lagi sebelum mereka boleh menempa blok lain. Dan oleh sebab peluang kejayaan *forger* meningkat apabila mereka gagal menempa blok, sistem ini bermakna yang *forger* berpeluang besar untuk menempa blok – dan mendapat ganjaran – dengan lebih kerap. Dalam masa yang sama, sistem ini menggalakkan komuniti *decentralized* yang maju dan sihat.

Contoh *coin* yang menggunakan kaedah Pemilihan Berasaskan Usia *Coin* ialah Peercoin (PPC).

Rumusannya, sistem POS adalah lebih efisien dan mesra alam kerana kos elektrik dan peralatan jauh lebih rendah daripada kos yang berkaitan dalam sistem POW. Jumlah orang yang terlibat menjalankan *node* juga lebih ramai kerana prosesnya mudah dan kosnya lebih berpatutan. Ini seterusnya menjadikan *coin* ini lebih *decentralized*.

Semua ini menerangkan mengapa lebih 90 peratus daripada *coin* yang wujud sekarang ini menggunakan sistem POS dan bukan POW lagi.

19. APAKAH ITU STABLECOIN?

Stablecoin adalah kelas baru *cryptocurrency* yang cuba menawarkan kestabilan nilai dan disokong oleh aset rizab.

Stablecoin nampak menarik kerana mereka menawarkan yang terbaik dari kedua-dua dunia – pemprosesan segera, tahap sekuriti dan tahap privasi *cryptocurrency* berserta kestabilan mata wang fiat.

Sepertimana kita semua tahu, Bitcoin ialah *cryptocurrency* yang pertama diterbitkan, malahan ianya merupakan *cryptocurrency* yang paling popular sehingga kini. Tetapi Bitcoin mempunyai satu masalah besar – nilainya boleh meruap dengan ketara. Sebagai contoh, ia meningkat dari paras $1,000 pada bulan Januari tahun 2017 kepada $19,000+ pada bulan Disember dalam tahun yang sama, dan kemudian menjunam di bawah tahap $4,000 pada bulan Februari 2019. Malah perubahan harga *intraday* Bitcoin dan sesetengah *cryptocurrency* lain boleh menjadi amat liar; nilainya boleh naik atau turun melebihi 10% dalam tempoh beberapa jam sahaja! Situasi ini sudah cukup untuk membuatkan kita diserang sakit jantung!

Keterlaluan naik turun nilai jangka pendek ini membuatkan Bitcoin dan banyak *cryptocurrency* lain kurang sesuai untuk digunakan sebagai mata wang (buat masa ini). Pada dasarnya, mata wang harus bertindak sebagai medium pertukaran dan instrumen simpanan nilai. Dan nilai tersebut haruslah stabil secara relatif untuk sesuatu jangka masa; ia tidak sepatutnya naik turun dengan mendadak dari satu hari ke hari yang lain.

Dan berita baiknya ialah Stablecoin menyediakan penyelesaian untuk menangani masalah kemeruapan nilai ini.

Sebab utama mengapa nilai mata wang fiat stabil ialah kewujudan autoriti (contohnya Bank Negara) yang menerbitkan dan menyokong mata wang tersebut. Dan kehadiran autoriti ini memberikan kepercayaan kepada semua yang nilai mata wang tersebut akan dijaga dan dikawal rapi.

Sebagai contoh akan kawalan tersebut, ketika berlakunya kes-kes tertentu apabila nilai mata wang fiat bergerak dengan drastik, pihak autoriti melompat masuk ke dalam pasaran dan menguruskan permintaan dan penawaran mata wang untuk mengekalkan kestabilan nilai. (Ini tidak berlaku setiap kali, tetapi inilah teorinya!)

Sebahagian besar *cryptocurrency* termasuklah Bitcoin tidak mempunyai kuasa pusat atau autoriti untuk mengawal nilai apabila diperlukan dan tidak juga mempunyai rizab atau aset yang boleh menyokong penilaian mereka.

Jadi Stablecoin cuba merapatkan jurang antara mata wang fiat dan *cryptocurrency*.

Terdapat tiga kategori Stablecoin:

Kategori Stablecoin yang pertama mengekalkan mata wang fiat (contohnya Dolar Amerika) sebagai rizab dan cagaran untuk mengeluarkan sebilangan *coin*. Ada juga Stablecoin yang menyimpan cagaran dalam bentuk logam berharga seperti emas atau perak atau komoditi seperti minyak. Walau bagaimanapun, kebanyakan Stablecoin menggunakan Dolar Amerika sebagai rizab.

Contoh Stablecoin begini ialah Basecoin yang mana protokolnya memang untuk menstabilkan nilainya. Nilai Basecoin disandarkan kepada Dolar sejak pelancaran.

Kategori Stablecoin yang kedua disokong oleh *cryptocurrency* dan/atau aset lain. Oleh kerana *cryptocurrency* dan aset rizab itu juga mungkin terdedah kepada keruapan nilai, Stablecoin sebegini di‘*over-collateralized’*. Maksudnya di sini ialah jumlah *cryptocurrency* rizab itu mengatasi jumlah Stablecoin yang diterbitkan.

Sebagai contoh, ether yang bernilai $2,000 disimpan sebagai rizab untuk menerbitkan Stablecoin yang bernilai $1,000.

Contoh Stablecoin begini ialah DAI yang disokong oleh sekumpulan aset yang berbeza. Malah DAI mendakwa yang ianya adalah Stablecoin yang pertama dilancarkan di *blockchain* Ethereum.

Kategori Stablecoin yang ketiga dikenali sebagai *Non-Collateralized* Stablecoin. Ianya adalah unik kerana ianya tidak menggunakan sebarang simpanan atau rizab. Sebaliknya, Stablecoin sebegini menggunakan mekanisma konsensus untuk meningkatkan atau mengurangkan bekalan token berdasarkan keperluan. Tindakan ini adalah serupa dengan percetakan wang kertas yang dilakukan oleh bank pusat dalam usaha untuk mengekalkan nilai mata wang fiat.

Stablecoin ini bergantung kepada kontrak pintar untuk menjual token jika harga jatuh di bawah pasak atau untuk membekalkan token ke pasaran jika nilai meningkat. Dengan cara ini, nilai token itu kekal stabil.

Contoh Stablecoin begini ialah CarbonCoin (Carbon).

20. APAKAH ITU *MASTERNODE*?

Salah satu topik utama tentang *cryptocurrency* yang dibincangkan oleh ramai orang ialah cara-cara untuk menjana wang daripadanya. Cara yang paling ketara adalah dengan menjual beli *cryptocurrency* dengan menjadi seorang *trader*. Cara yang kedua adalah dengan menjadi seorang *miner*. Dua cara ini bukanlah rahsia dan malah diketahui oleh umum.

Sebenarnya, terdapat satu lagi cara untuk menjana wang daripada *cryptocurrency* – menjadi *masternode*.

"Apakah itu *masternode*?" Anda sudah tentu bertanya.

Sebelum menceritakan tentang *masternode*, saya terangkan apakah itu *node* dulu.

Definisi sebenar *node* ialah sebarang peranti elektronik yang aktif, termasuk komputer, telefon atau pencetak, yang mempunyai akses internet dan mempunyai alamat IP. Walau bagaimanapun, *node* dalam konteks perbincangan kita ini ialah komputer yang mempunyai akses internet.

Peranan *node* adalah untuk menyokong rangkaian dengan mengekalkan salinan *blockchain* dan dalam beberapa kes, memproses transaksi. Setiap *cryptocurrency* mempunyai *node* mereka sendiri untuk memproses transaksi dan mengekalkan rekod-rekod transaksi tersebut.

Pembaca yang bijak – andalah tu! – akan sedar yang *node* ialah istilah alternatif kepada '*miner*' dan '*forger*'.

Masternode pula ialah komputer yang menyimpan salinan penuh *blockchain* sesuatu *cryptocurrency* secara *real-time* dan ianya berfungsi 24/7.

Mereka berbeza daripada *node* biasa kerana mereka melakukan beberapa fungsi lain selain menyimpan salinan penuh *blockchain* dan memproses transaksi. Fungsi-fungsi ini termasuklah:

- Meningkatkan tahap privasi transaksi.
- Memproses transaksi secara segera.
- Mengambil bahagian dalam urus pentadbiran.
- Mengundi.

Masternode juga sentiasa berkomunikasi dengan *node* lain untuk mengekalkan rangkaian.

Dan sebagai balasan untuk melakukan semua usaha ini, *masternode* mendapat ganjaran dalam bentuk *coin* yang mereka sertai itu. Ganjarannya diterima seminggu sekali atau sebulan sekali, bergantung kepada *coin* yang disertai. Jadi ganjaran ini merupakan sejenis pendapatan pasif – jenis pendapatan yang saya amat sukai!

"Berapa banyakkah ganjaran yang boleh saya terima menjadi *masternode*?" Ini mungkin merupakan soalan anda yang kedua.

Jawapannya ialah ganjarannya berbeza di antara *coin* yang berbeza. Ia bergantung di antara lain kepada:

- *Coin* yang anda melabur.
- Protokol ganjaran bagi setiap *masternode.*
- Peningkatan nilai *coin* tersebut pada masa depan.

Sebagai contoh, Dash membayar 45% daripada ganjaran blok terkini kepada *masternode*, 45% kepada *miner* dan 10% kepada bajet. Ganjaran blok ialah 3.34 Dash, jadi *masternode* yang dipilih menerima 1.67 Dash per pembayaran atau kira-kira 6 Dash sebulan. Semasa saya menulis buku ini, satu Dash bernilai $88.15. Jadi anda akan mendapat ganjaran bernilai $528.90 setiap bulan yang bersamaan lebih kurang RM2,208 – kira cukuplah untuk beli kopi putih dan telur setengah masak tiap-tiap pagi!

Sebelum anda naik syeikh dan melompat nak jadi *masternode*, saya perlu terangkan yang anda perlu memilik 1,000 Dash untuk dijadikan cagaran sebelum boleh menjadi *masternode* Dash. Ini bermakna anda perlulah mengeluarkan modal berjumlah RM368,170 dulu untuk menyertai mereka. (Ya, ini mainan orang kaya sahaja, ya?)

Saya perlu tambah juga yang ganjaran blok menurun sebanyak 7.14% setahun jadi pendapatan tahunan untuk pemilik *masternode* adalah kira-kira 7% daripada jumlah cagaran, dan akan berkurangan dengan peredaran masa.

Sehingga bulan November 2018, rangkaian Dash mempunyai lebih daripada 5,400 *masternode*s di lebih 45 buah negara dan dihoskan di lebih 140 ISP.

21. APAKAH ITU ERC-20?

Saya bermula dengan cerita sejarah pendek Ethereum.

Apabila Ethereum dilancarkan pada tahun 2015, ia telah memberi peluang kepada para *developer* untuk melancarkan *Decentralized Application* (dApps) mereka sendiri dengan cepat dan mudah. *Developer* tidak perlu mencipta dApps dari mula; mereka boleh mempercepatkan prosesnya dengan ketara dengan menggunakan *blockchain* Ethereum. Peluang ini disambut dengan rakus oleh *developer* dan ratusan dApps baru telah dilancarkan! Malah, banyak ICO telah dilancarkan waktu ini untuk mengutip dana untuk melancarkan dApps-dApps baru ini. Dana yang kutip pula, bukan sikit, tuan-tuan dan puan-puan; jumlahnya masuk berbilion-bilion Dolar!

Bagaimanapun, kebanyakan dApps tersebut menggunakan token mereka sendiri: token itu hanya boleh digunakan dalam dApps yang tertentu sahaja. Dan untuk menambahkan komplikasinya, token-token tersebut tidak serasi satu sama lain. Token A tidak serasi dengan token B dan token C, dan sebaliknya. Situasi ini lebih kurang seperti mereka bertutur bahasa yang berlainan. Ini menimbulkan masalah kepada semua pihak terutamanya pengguna jika mereka mempunyai 10 atau 20 token yang berbeza! Situasi ini sudah tentu memeningkan kepala dan menimbulkan masalah.

Untuk mengatasi masalah ini, komuniti Ethereum pun mencipta satu standard – senarai peraturan-peraturan – yang perlu diikut oleh semua *developer*. Standard ini dinamakan ERC-20: singkatan nama ***E**thereum **R**equest for **C**omments* (bukan *Election Committee*, ya?) sementara 20 adalah nombor yang dipilih di angin lalu!

Token ERC-20 ini sangatlah penting kerana ia menyenaraikan peraturan-peraturan yang perlu dipatuhi oleh semua token di *blockchain* Ethereum. Dan oleh sebab kebanyakan *developer* mengikut peraturan-peraturan tersebut, ini memudahkan dan memudahkan semua pihak kerana sekarang semua token yang berbeza boleh digunakan – dikongsi, ditukar dan dipindahkan kepada *wallet*. Dalam kata lain, semua token tersebut sekarang bercakap bahasa yang sama.

ERC-20 amat berjaya sehinggakan pada bulan April 2019, lebih 181,000 token wujud di *blockchain* Ethereum. Malah, nilai token yang menggunakan standard ERC-20 telah melebihi 90% daripada nilai pasaran *cryptocurrency* pada satu ketika!

Tetapi ERC-20 juga tidak sempurna, dan mempunyai beberapa masalahnya sendiri (terlalu panjang dan terlalu teknikal untuk diterangkan di sini jadi anda terima sahajalah poin ini!). Jadi komuniti Ethereum pun dalam proses untuk memperbaiki dan menaikkan tahap standard yang baru dan yang lebih canggih.

Satu hari nanti, ERC-20 akan diganti oleh standard yang baru tetapi apa yang pasti ialah ERC-20 memainkan peranan yang penting dalam kejayaaan token.

22. APAKAH ITU *SMART CONTRACT*?

Definisi teknikal '*smart contract*' atau 'kontrak pintar' ialah protokol komputer yang bertujuan untuk memudahkan, mengesahkan, atau menguatkuasakan poin yang tertera dalam sesuatu kontrak. Istilah sesuatu kontrak itu ditulis dalam bentuk kod komputer dan kemudiannya dimuat naik kepada sesuatu *blockchain*, selalunya Ethereum. Transaksi yang berlaku dalam *smart contract* diproses oleh *blockchain* apabila syarat-syarat tertentu dipenuhi dan berlaku secara automatik tanpa campur tangan pihak ketiga. Dan oleh sebab *smart contract* wujud di *blockchain*, ini bermakna ianya dapat dilihat oleh semua orang dan sama pentingnya, tidak dapat diubah suai atau ditukar ganti.

Okay, sekarang anda ulang balik semua ayat-ayat di atas dan terangkan maksudnya kepada saya!

Anda masih pening? Tak usah bimbang kerana saya berikan satu contoh untuk menerangkan bagaimana *smart contract* berfungsi.

Katakan anda menyewa apartmen saya di KL (jangan lupa yang saya juga seorang pemilik hartanah yang terkenal, ehem, ehem!). Kita berdua bersetuju dengan syarat dan istilahnya, dan juga bersetuju untuk menggunakan *smart contract* di *blockchain* Ethereum untuk menguatkuasakan poin yang tertera dalam perjanjian sewa.

Apabila anda membuat bayaran deposit yang secukupnya (dengan menggunakan ETH), anda akan menerima kunci masuk digital dan juga resit pembayaran pada tarikh yang telah kita tetapkan.

Dan sekiranya kunci tidak tiba tepat pada waktunya, *blockchain* akan mengisukan bayaran balik (*refund*) kepada anda. Jadi anda tidak menanggung risiko tidak mendapat produk/servis yang telah dipersetujui.

Saya pula tahu yang saya memang akan mendapat semua bayaran pada tarikh-tarikh yang telah dipersetujui.

Dokumen itu pula dibatalkan secara automatik selepas tempohnya, dan kod tersebut tidak boleh diubah suai oleh mana-mana pihak tanpa pengetahuan pihak lain kerana semua peserta dimaklumkan serentak.

Jadi semuanya berlaku secara automatik apabila syarat-syarat tertentu dipenuhi contohnya apabila sesuatu transaksi berlaku atau masa berlalu – tanpa campur tangan pihak ketiga. Poin yang sama pentingnya ialah kita berdua rasa selesa dan selamat melakukan semua transaksi ini kerana kita tidak menanggung risiko serta tidak ada penipuan atau kes pecah amanah yang berlaku!

Saya rasa inilah sebabnya kontrak itu disebut pintar!

Itu contoh yang mudah. Berita yang lebih baiknya ialah *smart contract* tidak dihadkan kepada perjanjian sewa sahaja, malah ianya boleh digunakan untuk banyak situasi yang lain: daripada derivatif kewangan kepada premium insurans, undang-undang hartanah, penguatkuasaan kredit, khidmat kewangan, pemindahan data, proses undang-undang, ICO dan malah undian dalam pilihan raya! Dan saya pasti terdapat 1,001 situasi lagi yang akan mengguna pakai *smart contract* ini pada masa depan.

23. APAKAH ITU *SHARDING*?

Sharding adalah kaedah memisahkan data secara mendatar dalam pangkalan data. Pangkalan data ini dipecahkan menjadi bahagian yang lebih kecil yang dipanggil '*shards*', dan kemudiannya disusun kembali untuk membentuk pangkalan data asal. *Sharding* menyebarkan beban dan membuat pangkalan data lebih efisien.

Oleh sebab salah satu masalah besar dalam teknologi *blockchain* adalah *scalability*, konsep *sharding* ini pun dipinjam dan diaplikasikan untuk menangani masalah tersebut.

Apabila *sharding* diaplikasikan dalam *blockchain*, setiap *node* menyimpan hanya sebahagian data dalam *blockchain* tersebut, dan tidak keseluruhan data sepertimana *node* yang wujud dalam *blockchain* yang biasa. (Walaupun *node* dalam *shard* tertentu mengekalkan hanya data di dalam *shard* tersebut, data tersebut masih tetap dikongsikan. Perkongsian data ini bermakna *decentralization* tetap wujud dalam *shard* tersebut.) Dan oleh kerana setiap *node* tidak memuatkan semua data di dalam *shard* itu pada keseluruhan *blockchain*, ini mempercepatkan transaksi yang seterusnya membantu *scalability*.

Walau bagaimanapun, *sharding* hanya boleh diaplikasikan dalam sistem POS dan bukan POW. Hal ini kerana, sepertimana yang anda tahu, *node* dalam POW merekodkan semua data dalam *blockchain*, yang tidak berlaku dalam *sharding*.

Jadi rumusannya, *sharding* mempercepatkan transaksi yang seterusnya membantu *scalability*. Inilah salah satu sebab mengapa Ethereum mahu berhijrah ke sistem POS.

24. APAKAH ITU ICO?

Initial Coin Offering yang lebih terkenal dengan akronimnya ICO merupakan usaha untuk mengutip dana bagi melancarkan *cryptocurrency* yang baru. Konsep dan nama ICO lebih kurang serupa dengan *Initial Public Offering* (IPO) tetapi ianya berbeza kerana ICO tidak menerbitkan saham dan juga tidak memerlukan kelulusan daripada mana-mana institusi atau autoriti kewangan.

Apabila sesuatu firma *cryptocurrency* ingin mengumpul dana melalui ICO, ia biasanya membuat kertas putih yang menyatakan tujuan projek, jumlah wang diperlukan, ganjaran untuk perintis projek, jenis wang yang diterima dan tempoh kempen ICO. Firma tersebut membentangkan kertas putih ini dan memberikan peluang kepada mereka yang berminat untuk melabur dalam projek mereka.

Pelabur awal biasanya membeli *cryptocurrency* baru itu dengan harapan projek ICO itu berjaya selepas ia dilancarkan. Jika ianya berjaya, maka nilai *cryptocurrency* baru itu akan naik lebih tinggi daripada harga belian mereka.

Satu contoh projek ICO yang berjaya menguntungkan pelabur awal ialah platform *blockchain* Ethereum. ICO projek Ethereum telah berjaya mengumpul dana berjumlah $18 juta Bitcoin (atau $0.40 per Ether) semasa ianya diumumkan pada tahun 2014. Projek ini dilancarkan pada tahun 2015 dan nilai Ether pada hujung bulan April 2020 melebihi $207!

Tetapi konsep semi-liar ICO yang tidak dikawal selia dan tidak memerlukan kelulusan mana-mana autoriti kewangan menarik perhatian para jin dan jembalang berkaki dua! Mereka pun turut serta melancarkan ICO sendiri dan berjaya mengutip dana yang masuk beratus-ratus juta Dolar! Malangnya, beberapa projek ICO telah gagal, malah ada yang penipuan semata.

Satu contoh ICO yang gagal ialah Enigma di mana penggodam telah melarikan Ether berjumlah $500,000. Apa yang lebih mengejutkan dan menggemparkan tentang kes ini ialah Enigma ialah *coin* yang mengutamakan keselamatan!

Contoh yang kedua ialah kehilangan wang berjumlah $10 juta daripada dana yang dikutip oleh ICO Coindash. Insiden itu amat mencurigakan sehinggakan ramai pengguna menuduh kehilangan itu adalah hasil kerja ‘orang dalam’!

Kes scam yang nyata ialah OneCoin yang beroperasi pada tahun 2015 hingga tahun 2017. Walaupun banyak bendera merah yang berkibar tentang OneCoin – termasuklah ejaan yang salah di laman webnya, beberapa ahli pasukannya terlibat dengan *scam* lain sebelumnya, pengasasnya Ruja Ignatova mungkin telah memalsukan kelayakannya serta

amaran daripada banyak kerajaan (!) – mereka telah berjaya mengutip $4 bilion daripada pelabur di serata dunia. (Walaupun kita rasa kasihan terhadap pelabur-pelabur tersebut, dalam masa yang sama, kita juga tak begitu terkejut akan kehilangan wang itu. Ini adalah kerana mereka masih sanggup melabur walaupun begitu banyak amaran yang telah diberikan oleh pelbagai pihak. Mereka ini macam memang sahaja hendak cari penyakit!)

Oleh itu, tidaklah menghairankan sangat apabila Bank Pusat China membuat kenyataan pada 4 September 2017 untuk melarang semua ICO di negara itu. Menurut laporan itu juga, semua penjualan token dilarang di dalam negara itu sementara organisasi yang telah melancarkan ICO diarahkan untuk mengembalikan semua dana pelabur.

Akibat larangan ini, harga Bitcoin jatuh 5%, sementara harga Ethereum merudum 11%!

Sebagai maklumat tambahan, Malaysia telah menklasifikasikan ICO dan *exchange cryptocurrency* sebagai sekuriti dan oleh itu, perlu mendapat kebenaran untuk beroperasi daripada Suruhanjaya Sekuriti pada awal tahun 2019. Sesiapa yang melanggar perintah The Capital Markets and Services (Digital Currency and Digital Token) Order 2019 ini boleh dipenjarakan tidak melebihi 10 tahun dan denda tidak melebihi RM10 juta!

Berat tu!

Berita baiknya ialah sesiapa yang dipenjarakan mungkin mendapat peluang untuk berkenalan dengan bekas-bekas menteri di dalam penjara!

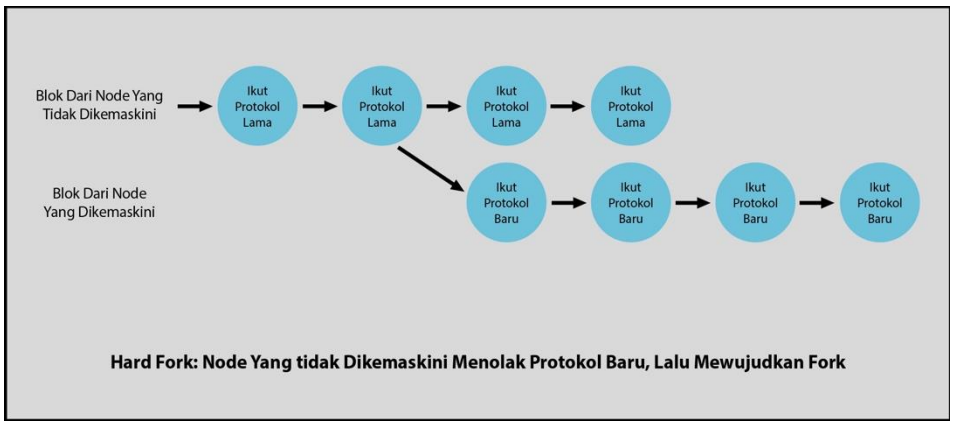
25. APAKAH ITU *FORK*?

Istilah *fork* (garpu) digunakan dalam bahasa Inggeris untuk menerangkan tempat di mana jalan atau sungai berpecah dua.

Istilah ini sekarang dipinjamkan dalam dunia *cryptocurrency*. *Fork* berlaku apabila perubahan radikal dilaksanakan pada protokol rangkaian yang membuat blok dan transaksi yang sah sebelum ini menjadi tidak sah, atau sebaliknya. Langkah ini menyebabkan *blockchain* itu berpecah dua: versi original yang kekal di sepanjang laluan lama dan versi terkini yang mengikuti blok baru yang dinaik taraf.

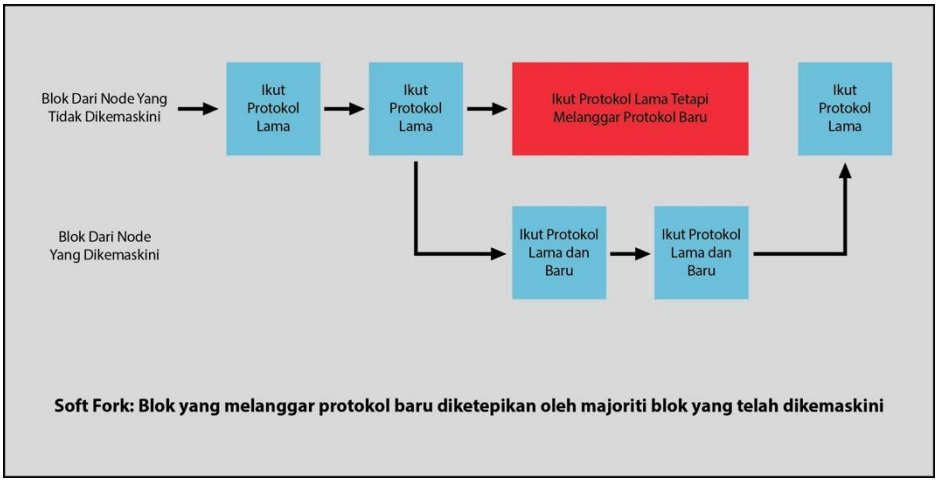
Fork terbahagi kepada dua jenis: *hard fork* dan *soft fork*.

Hard fork memerlukan semua *node* atau pengguna untuk menaik taraf ke versi terkini protokol perisian.



Grafik 25.1: *Hard Fork*

Soft fork pula ialah perubahan kepada protokol perisian di mana blok/transaksi yang sah sebelum ini menjadi tidak sah. Oleh sebab *node* lama akan mengiktiraf blok baru di *blockchain* sebagai sah, *soft fork* adalah *backward-compatible*. *Soft fork* tidak memerlukan mana-mana *node* untuk menaik taraf untuk mengekalkan konsensus kerana semua blok baru masih diterima oleh *node* lama. Jadi ianya tidaklah begitu serius jika dibandingkan dengan *hard fork*.



Grafik 25.2: *Soft Fork*

"Apakah tujuan *fork* ini?" Soalan ini sudah tentu bermain dalam kepala anda.

Berikut adalah jawapannya:

Terdapat beberapa sebab mengapa pemaju melaksanakan *hard fork*. Antara sebab-sebabnya adalah untuk membetulkan risiko keselamatan yang wujud dalam versi lama perisian atau untuk menambah fungsi baru atau untuk mengalihkan urus niaga seperti yang berlaku di *blockchain* Ethereum pada tahun 2016.

Seperti yang saya ceritakan dalam Bab 13, seorang *hacker* telah berjaya menggodam dan mencuri Ether bernilai $50 juta dari platform Ethereum pada tahun 2016.

Pihak *developer* dan ramai pengguna Ethereum bersetuju untuk melakukan *hard fork* supaya semua *coin* yang dicuri itu boleh dikembalikan kepada pemilik-pemilik asalnya. Dalam masa yang sama, sekumpulan pengguna lain pula berpendapat yang usaha ini melanggar erti asas *decentralization*. Kumpulan yang kedua ini percaya bahawa satu-satunya cara untuk mempunyai *cryptocurrency* yang benar-benar *decentralized* adalah untuk tidak terlibat dan membiarkan *coin* itu mengikut aliran.

Bincang sana, bincang sini tetapi kata sepakat gagal ditemui!

Jadi pada akhirnya, *developer* Ethereum meneruskan keputusan mereka untuk melaksanakan *hard fork* tersebut.

Akibat pertikaian ini, rangkaian Ethereum berpecah dua: Ethereum (ETH) diteruskan pada blok yang telah di-*forked*, manakala Ethereum Classic (ETC) diteruskan pada blok asal.

Ethereum melaksanakan *hard fork* sekali lagi pada bulan Januari 2018: Ether Zero. Tetapi oleh sebab Ether Zero bertujuan untuk meningkatkan kelajuan kadar transaksi rangkaian, *fork* ini tidaklah terlalu ekstrim seperti kes Ethereum Classic.

Metropolis ialah *fork* Ethereum yang terkini (dijangkakan berlaku pada bulan October 2020). *Fork* ini adalah sebahagian daripada rencana untuk menjadikan rangkaian Ethereum lebih cepat, lebih murah dan lebih efisien. Dua rencana utama Metropolis ialah kenaikan status privasi dan penghijrahan Ethereum daripada POW ke POS.

Jadi itulah sejarah pendek Ethereum dan *fork*nya.

Poin seterusnya ialah *fork* boleh berlaku di mana-mana platform *cryptocurrency* dan bukan hanya Ethereum.

Malah Bitcoin juga telah melalui proses *fork* ini berkali-kali!

Hard fork Bitcoin yang pertamanya berlaku pada 1 Ogos 2017. Selepas tarikh tersebut, terdapat dua versi Bitcoin yang berasingan: Bitcoin original yang dilabelkan BTC dan Bitcoin Cash yang dilabelkan BCC (ada juga mereka yang melabelkannya sebagai BCH).

Situasi ini berlaku dan mempunyai asalnya kerana setiap blok dalam rangkaian Bitcoin dihadkan saiznya. Had ini memang ditetapkan dari mula untuk melindungi Bitcoin daripada serangan *hacker*. Malangnya, had ini juga memperlahankan proses meluluskan transaksi setiap blok. Masalah ini menjadi kronik kerana jumlah transaksi Bitcoin semakin bertambah kebelakangan ini.

Para *miner* dan komuniti Bitcoin semuanya bersetuju yang proses baru diperlukan untuk mempercepatkan transaksi Bitcoin. Malangnya, mereka tidak dapat bersetuju dengan cara untuk melakukannya! Walaupun kumpulan besar bersetuju untuk membesarkan saiz blok dengan menggunakan teknologi SegWit, malangnya, sekumpulan *miner* yang lain berkeras yang teknologi tersebut masih kurang efektif dan mahu lebih banyak yang dilakukan. Walaupun banyak perbincangan yang dilakukan, kedua-dua kumpulan ini masih tidak mendapat kata sepakat.

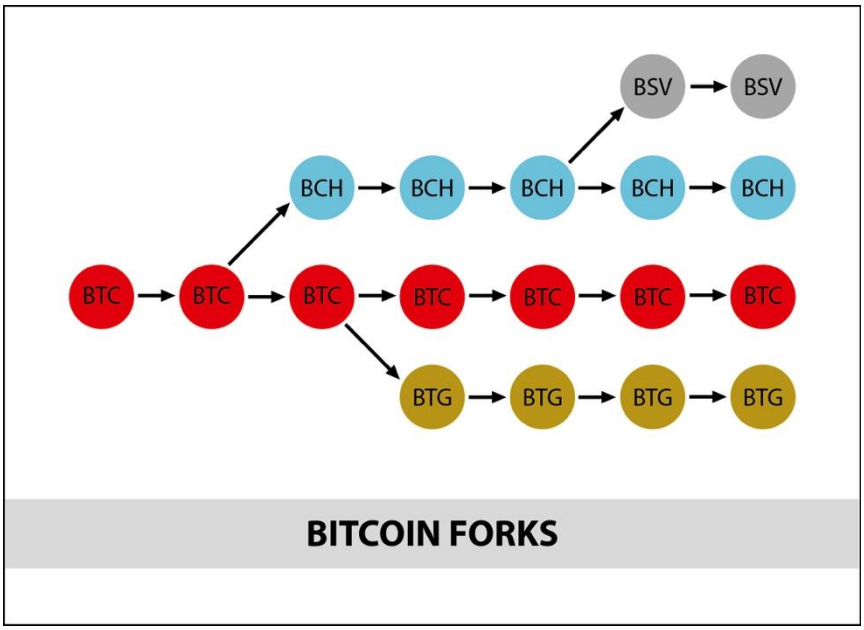
Jadi Bitcoin pun melalui proses *hard fork* pada tarikh di atas.

Mereka yang memegang Bitcoin sebelum tarikh tersebut kini mempunyai kedua-dua BTC dan juga BCC selepas 1 Ogos – satu BCC untuk setiap BTC yang dimiliki. Jadi mereka mempunyai aset digital serta-merta (kira dapat durian runtuhlah)!

Nilai pada hari pertama BCC diterbitkan ialah $400 sementara nilai BTC ialah $2,700. Dan ianya tidak menghairankan yang nilai kedua-duanya naik turun seperti monyet mabuk dalam hari-hari yang berikutnya!

Bitcoin melalui proses *hard fork* yang kedua pada bulan October 2017 (BTC) dengan kemunculan Bitcoin Gold (BTG). Sama seperti peristiwa *hard fork* yang pertama, pemilik Bitcoin menerima satu BTG untuk setiap BTC yang dimiliki.

Dan mungkin kerana Bitcoin Cash (BCH) tidak mahu ketinggalan (!), ia turut melalui proses *hard fork* pada bulan November 2018 dan menjanakan Bitcoin SV (BSV). Lagi sekali, pemilik menerima satu *coin* BSV untuk setiap BCH yang dimiliki.



Grafik 25.3: Sejarah *Hard Fork* Bitcoin

"Ini amat bagus!" Anda mungkin berkata. "Setiap kali ada *hard fork*, semua pemilik *coin* mendapat *coin* baru secara percuma."

Kata-kata anda itu tepat sekali! Saya rasa, dan walaupun tidak diceritakan sangat, tujuan utama *hard fork* ini adalah untuk menjanakan *coin* percuma kepada pemilik! (Sama ada konsep itu adalah betul atau tidak, tidak ramai orang yang bising kerana semua orang dapat *coin* percuma!)

Tetapi sudah tentunya kerana ini dunia *cryptocurrency*, kesejahteraan komuniti adalah amat penting dan dihargai. Tidak semua dilakukan kerana wang ringgit semata.

Pada masa saya menulis buku ini, rangkaian Steem di dalam proses untuk melakukan *hard fork* untuk melarikan diri daripada cubaan *takeover* oleh pengasas Tron, Justin Sun.

Majoriti pemegang Steem memandang serong akan cubaan Justin lalu mereka berganding bahu untuk menahan *takeover* itu daripada berlaku.

Sama ada *fork* itu berlaku atau tidak, masa akan menentukannya.

26. APAKAH ITU *PUMP AND DUMP*?

Pump and dump adalah istilah yang digunakan untuk menerangkan fenomena di mana sesuatu pihak (selalunya mereka yang mempunyai kepentingan dalam *coin* tersebut seperti pihak pengurusan atau pasukan *developer*) menggunakan beberapa strategi untuk memanipulasikan harga sesuatu *coin*. Ini mungkin termasuk membuka cerita yang *coin* itu akan diterima oleh syarikat-syarikat besar atau *coin* itu akan memperkenalkan teknologi baru yang canggih. Berita-berita sebegini selalunya menarik perhatian para spekulator dan pelabur yang meluru untuk melabur dalam *coin* tersebut. Malah ada juga orang yang akan begitu teruja sehinggakan mereka sanggup menjadi *miner coin* tersebut di samping melabur di dalamnya. Tindakan mereka menyebabkan harga *coin* tersebut naik. Kenaikan awal harga *coin* itu menarik perhatian lebih banyak pelabur yang kemudiannya turut sama melabur yang seterusnya menyebabkan harga *coin* tersebut naik lagi. Dan lagi dan lagi.

Anda perlu ingat yang bagi setiap pembeli, mesti ada penjualnya.

Dan selalunya si penjual dalam kes-kes *pump and dump* adalah mereka yang mempunyai kepentingan di dalam *coin* tersebut, seperti yang diterangkan sebelum ini adalah pihak pengurusan atau pasukan *developer coin* itu sendiri. Ataupun orang yang menerbitkan berita-berita tadi!

Saya rasa tidak perlu diterangkan yang mereka ini menjual secara senyap-senyap. Maklumlah mereka melompat dan menjerit *coin* merekalah yang terbaik di dunia apabila di depan pelabur. Jadi semua usaha jualan itu perlulah dibuat secara tersembunyi atau di belakang tabir.

Anda perlu ingat juga yang ribuan Altcoin (atau istilah yang lebih tepatnya Scamcoin (!)) telah direka semata-mata untuk membuat keuntungan bagi pencipta mereka!

Biasanya, Scamcoin begini akan diumumkan secara mengejut (tiba-tiba sahaja muncul) di forum-forum *cryptocurrency* yang popular. Dan sering kalinya Scamcoin begini telah di*pre-mined* oleh pencipta mereka, yang bermaksud bahawa pencipta memiliki jumlah *coin* yang amat banyak.

Pencipta Scamcoin kemudiannya mengaplikasikan strategi '*pump and dump*' ini untuk mendapatkan sokongan pelabur *crypto*. Mereka mula menyebarkan cerita yang *coin* mereka itu akan mengubah dunialah, teknologi *coin* mereka teramat canggihlah, dan itu dan ini. Mereka juga akan menggalakkan pelabur untuk menjadi *miner coin* tersebut. Dan jika mereka berjaya mencari orang untuk memulakan dagangan *coin* mereka, mereka akan terus-menerus menyebarkan cerita-cerita yang indah sensasi tentang *coin* mereka

untuk memacu nilainya. Jumlah pelabur naik, nilai *coin* pun naik. Sementara itu di belakang tirai, pencipta menjual semua *coin* mereka, mengambil wangnya dan keluar dari pasaran (dan mungkin pergi belayar di *yacht* masing-masing). *Coin* tersebut ditinggalkan begitu sahaja, terkontang-kanting tanpa sokongan teknikal.

Waktu inilah berita akan terbit membongkarkan yang semua cerita-cerita indah sensasi itu adalah khabar angin sahaja. Malah, ianya adalah pembohongan semata.

Sudah tentu harga *coin* tersebut pun jatuh merudum setelah situasi sebenarnya terbongkar. Para spekulator dan pelabur pun menanggung kerugian yang masuk beratus-ratus juta Dolar sementara pihak pengurusan tersenyum lebar dan mengaut keuntungan besar. Mengapa tidak? Mereka mendapat wang kertas sebenar sementara *miner*, spekulator dan pelabur memegang *coin* yang tidak begitu bernilai atau tidak bernilai langsung!

Satu contoh ketara ialah Foin.

Foin dilancarkan pada bulan Julai 2018 dengan harga lebih kurang $400. Harganya naik secara perlahan-lahan tetapi tiba-tiba sahaja melompat daripada $1,492 pada 1 November 2019 kepada $2,574 pada 15 Disember 2019! Foin membuat kenyataan pada tarikh tersebut yang ia telah membeli AliExchange (sebuah *exchange* yang berpangkalan di Estonia) dengan harga 1 juta Foin dan melarang para pelabur daripada mengeluarkan wang dari akaun mereka.

Apa yang lebih peliknya ialah harga Foin melompat lagi hingga ke $3,640 pada 23 Disember!

Sudah tentu parti liar begitu tidak akan bertahan lama. Berita sebenarnya pun terbongkar yang Foin ialah *scam* semata.

Semuanya jatuh berkecai selepas itu: harga Foin merudum lebih 99% di bawah $1 semasa buku ini diterbitkan! Malah pemilik-pemilik *coin* tersebut tidak dapat menjual *coin* kerana tidak ada siapa yang nak beli!

Cerita sampingan: seorang kenalan saya telah ‘melabur’ dalam Foin. Semasa harga Foin sedang naik, dia menceritakan kepada semua orang yang pelaburannya bernilai lebih RM200 juta! Ya, tuan-tuan dan puan-puan, angka itu betul! Bukan RM2 juta, bukan RM20 juta tetapi RM200 juta! (Jika beliau menjual semua Foin yang dimilikinya ketika nilainya di puncak, beliau akan menjadi salah seorang individu yang paling kaya di Malaysia!)

Sekarang saya dengar dia tidak mahu bercakap lagi tentang *crypto*!

Untuk pengetahuan anda dan untuk bagi sedap hati kepada semua, kes *pump and dump* ini bukan berlaku dalam dunia *crypto* sahaja tetapi dalam pelaburan lain termasuklah saham.

27. APAKAH ITU DEFI?

DeFi ialah nama singkatan Siti Dafinaz, anak Pak Husin yang duduk di hujung kampung saya!

DeFi dalam *cryptocurrency* pula adalah singkatan kepada *Decentralized Finance*. Ianya merangkumi aset digital, protokol, kontrak pintar, dan dApps yang dibina di atas *blockchain*.

Fikirkan DeFi sebagai ekosistem kewangan terbuka di mana anda boleh membina pelbagai produk dan perkhidmatan kewangan kecil yang *decentralized*. Dan oleh sebab semua ini adalah apps yang dibina di atas *blockchain*, mereka boleh digabung, diubah suai, dan diintegrasikan mengikut keperluan. Jadi ianya adalah lebih kurang seperti set lego!

Walaupun aplikasi DeFi boleh dibina di dalam berbagai platform, pilihan utama, seperti yang anda boleh agak, adalah platform Ethereum.

Tarikan utama DeFi ialah ia membolehkan anda mengawal aset anda sendiri.

Walaupun beberapa bank dan firma fintech berjanji untuk memberikan lebih banyak kuasa dan kawalan kepada pengguna, kita sebenarnya masih bergantung kepada mereka untuk menguruskan dana kita. Jadi semua itu sebenarnya hanya kata-kata manis dan merupakan janji kosong belaka!

Objektif DeFi adalah untuk memberi anda kuasa dan kawalan penuh terhadap aset anda. Dan situasi ini boleh diwujudkan melalui *decentralization* dan teknologi *blockchain*.

Hakikat bahawa semua protokol DeFi adalah *open-source* membolehkan sesiapa sahaja (yang mempunyai kepakaran) untuk membina produk kewangan yang baru di atasnya.

Para *developer* di seluruh dunia boleh bekerjasama antara satu sama lain untuk menghasilkan produk baru yang membawa kepada inovasi yang lebih pantas dan rangkaian yang selamat.

Berita yang lebih menariknya ialah sesiapa sahaja boleh menyimpan, berdagang, dan melabur aset mereka di *blockchain* dengan selamat serta memperoleh pulangan yang jauh lebih tinggi daripada sistem kewangan tradisional. Sebagai contoh, token NEXO memberikan pulangan 8% setahun berbanding kurang daripada 1% dari bank-bank tradisional.

Dan oleh sebab tiada pengantara yang mengendalikan aset anda, anda mempunyai kawalan penuh terhadap pelaburan anda.

Salah satu contoh syarikat yang menawarkan produk DeFi ialah Credissimo dan token NEXO yang dinyatakan tadi. Malah Credissimo juga merupakan *market leader* di dunia dalam pinjaman *crypto*.

Contoh kedua ialah *lending platform* MakerDao yang menjadi terkenal hasil perkembangan pesat dan populariti Stablecoinnya Dai.

Pasaran DeFi adalah masih kecil ($1 bilion pada hujung tahun 2019) berbanding dengan sistem kewangan tradisional tetapi ia meningkat dengan pesat sejak dua tahun kebelakangan. Apa yang pasti ialah jumlah projek dan dApps kewangan akan meningkat pada hari-hari yang akan datang.

Satu hari nanti, saya rasa banyak institusi kewangan tradisional akan merasa bahang yang teramat panas kerana pasaran mereka sudah dibolos! Dan jika mereka hanya duduk mendiamkan diri, besar kemungkinan mereka akan menjadi nota sejarah!

28. ISU-ISU SEKURITI

Saya ingin menekan ~~sikit~~ banyak (!) tentang sekuriti di sini.

Pertama, anda perlu ingat yang Altcoin wujud di internet. Dan walaupun banyak kebaikan yang muncul dan wujud kerana internet, dalam masa yang sama, banyak benda yang kurang baik juga wujud di internet. Dan salah satu daripada kekurangannya ialah ramai penjahat beroperasi di internet! Untuk menambahkan masalahnya, penjahat-penjahat ini begitu licik. Mereka mungkin berada di seberang lautan dan jauh beribu-ribu kilometer tetapi mereka masih boleh mencuri semua Altcoin anda!

Oleh sebab situasinya begini, anda perlulah menambahkan ilmu tentang Altcoin sebelum melangkah masuk ke dalam dunia ini. Ini termasuklah membaca buku (seperti yang anda sedang lakukan sekarang) dan menyertai seminar yang dikelolakan oleh pakar yang betul-betul pakar (bukan pakar yang membeli PhDnya!). Langkah ini adalah kritikal kerana ilmu ini akan menolong anda untuk membuat pilihan yang lebih baik serta lebih bijak dan dalam masa yang sama, mengelak daripada terjerlus dalam ribuan *scam* yang wujud dalam dunia *cryptocurrency* ini. Tanpa ilmu ini, peluang untuk anda ditipu adalah amat tinggi.

Satu contoh penipuan ialah kewujudan beberapa syarikat *scam* yang mengatakan mereka menyediakan servis *wallet*. Apabila pengguna memindahkan Altcoin ke dalam *wallet* tersebut, syarikat itu pun menutup operasi dan mencuri semua Altcoin tersebut.

Lagi satu contoh penipuan ialah syarikat yang mengatakan mereka menjual komputer *mining*. Mereka menipu kerana tidak menghantar produk yang dipesan oleh pembeli walaupun mereka memang menerima wang daripada pembeli.

Bagaimanapun contoh penipuan yang ketara berlaku dalam industri *cloud mining*. Walaupun ada segelintir syarikat yang menawarkan servis *cloud mining* ini adalah tulin, dianggarkan lebih 80 peratus daripada ‘syarikat’ tersebut adalah *scam*, menipu atau membohong! Ambil perhatian kerana syarikat tersebut mempunyai gudang *mining* mereka sendiri tidak bermakna mereka tidak menipu pelabur-pelabur mereka. Salah satu contoh ketara di sini ialah Bitclub Network yang telah didedahkan sebagai *scam* pada bulan Januari 2020. Sebelum berkubur, Bitclub Network yang beroperasi selama lebih lima tahun telah mengutip wang melebihi $722 juta Dolar! Apa yang lebih malangnya ialah beratus-ratus rakyat Malaysia telah menjadi mangsa *scam* Bitclub Network ini!

Grafik 28.1: *Banner* Mega *Scammer* Bitclub Network

Anda juga perlu tahu yang kebanyakan laman web si penjahat ini amat menarik dan canggih. Malah ada yang lebih canggih daripada laman web yang menawarkan servis yang betul! Jadi sekali lagi, anda perlu sentiasa berwaspada dengan setiap tawaran yang muncul tentang Altcoin.

Anda juga perlu ingat, oleh sebab Altcoin wujud di internet, ianya amat terdedah kepada serangan penjahat-penjahat ini. Mereka ini memang dan sentiasa mencari peluang dan lubang untuk mencuri Altcoin anda.

Walaupun banyak langkah yang diambil oleh pihak *exchange* untuk mempertingkatkan tahap sekuriti mereka, selagi mana *exchange* itu wujud di internet (dan ianya memang *online* 24/7!), ianya tetap terdedah kepada serangan *hacker*.

Anda juga perlu menggunakan akal fikiran kerana ramai juga orang kehilangan *coin* kerana mereka cuai.

Sebagai contoh, saya mendengar banyak cerita menarik tentang bagaimana pemilik kehilangan Bitcoin mereka kerana cuai, dan bukan kerana dicuri *hacker*. Sebagai contoh, seeorang pembeli kehilangan telefon bimbit, dan turut kehilangan Bitcoinnya kerana terlupa maklumat *login*nya. Seorang lagi pengguna kehilangan Bitcoinnya apabila *hard drive*nya terbakar. Dia buat *backup*. Tetapi malangnya *backup drive* itu berada di sebelah *hard drive*nya. Jadi kedua-dua *hard drive* dan *backup drive* itu terbakar sekali! Oleh sebab itu, dia juga kehilangan Bitcoinnya sebab semua data tentang akaun Bitcoin beliau hangus (*literally* hangus dalam kes ini!).

Satu cerita yang menarik tetapi tragik ialah kes seorang lelaki Australia bernama Campbell Simpson membuangkan *hard drive* komputer bimbitnya yang mempunyai 1,400 Bitcoin pada tahun 2010. Masa itu Bitcoin itu bernilai hanya $25. Hari ini, nilai Bitcoin yang sama ialah $11.5 juta!

Kes yang lebih tragik telah berlaku kepada James Howell, seorang lelaki di South Wales. Anda mungkin pernah membaca cerita beliau membuangkan *hard drive* lamanya di tong sampah pada tahun 2013. Tidak berapa lama kemudian, dia baru teringat yang maklumat tentang Bitcoinnya berada di dalam *hard drive* yang dibuangnya itu. Dia bergegas ke tempat buang sampah tetapi malangnya *hard drive*nya itu sudah tidak ada di sana. Dia kehilangan 7,500 Bitcoin yang kini bernilai $62 juta (mak datuk!)!

Walaupun semua kes ini melibatkan Bitcoin, cerita-cerita yang lebih kurang serupa juga berlaku kepada pemilik-pemilik Altcoin. Berpuluh-puluh ribu pemilik Altcoin telah menanggung kerugian yang masuk beratus-ratus juta Dolar kerana kecuaian atau sikap tidak apa mereka.

Anda tentu masih ingat cerita dalam Bab 13 tentang seorang pelabur di China yang telah kehilangan Bitcoin (BTC) dan Bitcoin Cash (BCH) yang bernilai $42 juta? Anda tentu ingat yang kes penggodaman itu berlaku melalui proses *sim swap* telefon. Si pelabur ini memang mencari penyakit kerana menyimpan data *cryptocurrency* yang bernilai $42 juta itu di dalam telefon beliau!

Jadi poinnya di sini ialah anda perlu mengambil banyak langkah untuk mengawasi Altcoin anda setiap masa. Ini termasuklah menggunakan pembekal perkhidmatan (*exchange*, broker dan sebagainya) yang mempunyai tahap sekuriti yang tinggi dan canggih.

Berikut adalah beberapa langkah yang anda perlu ambil:

- Gunakan *password* yang unik, panjang dan rumit.
- Tukar *password* itu dari semasa ke semasa.
- *Backup* semua *password* dan *passphrase*.
- *Backup* juga semua *password* dan *passphrase* dengan menulisnya di atas kertas.
- Simpan kertas itu di tempat yang selamat.
- Gunakan *public address* yang berbeza setiap kali anda ingin menerima Altcoin.
- Pindahkan majoriti Altcoin anda ke *hardware wallet*.
- Minimumkan masa *online* anda semasa membuat pembelian dan jualan.
- *Backup* data dalam telefon bimbit anda jika data Altcoin anda berada di dalamnya.
- *Backup* data itu *offline* juga.
- Simpan semua *offine backup* itu di tempat yang selamat (mungkin dalam peti deposit keselamatan) dan jauh dari *hard drive* anda.

Semua langkah-langkah di atas ini akan menambahkan kerja anda. Tetapi anda perlu melakukannya dan tidak boleh leka. Sebab satu kelekaan boleh bermakna kehilangan Altcoin anda! Dan apabila nilai satu Altcoin anda naik menjadi $5,000 atau $10,000, anda pasti akan menangis sampai keluar air mata darah!

Dan sebelum saya akhiri bab ini, saya ingin berpesan juga yang jembalang berkaki dua di dalam dunia *cryptocurrency* bukan sahaja *scammer* dan mereka yang tidak kenali tetapi termasuk juga para *developer* dan pengasas Altcoin tertentu. Saya tak nak sebut nama mereka tetapi adalah dua tiga individu yang merupakan pengasas Altcoin-Altcoin yang agak popular. Malangnya, kadangkala tindak tanduk mereka begitu mencurigakan. Mereka mencanangkan keluhuran tetapi bertindak sebagai penipu. Mereka menjerit ‘kita semua’ tetapi tindakan mereka mengutamakan diri mereka. Jadi mereka ini umpama musang berjanggut!

Saya perlu menambah yang saya tak akan melabur dalam mana-mana Altcoin yang ada sangkut paut dengan geng musang berjanggut ini, tidak kira bagaimana popular pun *coin* tersebut. Saya bertindak begini kerana saya tahu yang satu hari mereka ini akan membelit saya, dan saya tak mempunyai impian untuk menjadi mangsa jembalang, musang atau ular sawa!

Jadi anda pun perlu berhati-hati dengan mereka ini, ya?

29. KESELAMATAN ALTCOIN ANDA TERLETAK DI TANGAN ANDA 100%!

Saya perlu mengingatkan yang tanggungjawab untuk menjaga dan menyelamatkan Altcoin anda adalah 100%-nya di tangan anda. Ianya bukan di tangan *exchange*, bank, bank negara, majlis tertinggi Altcoin (kerana ianya tidak wujud) atau menteri kewangan. Anda yang memikul tanggung jawab itu seorang diri.

Oleh sebab itu, ambillah langkah berjaga-jaga setiap kali anda berinteraksi dengannya: cipta pelbagai kata laluan, gunakan *public address wallet* yang berbeza setiap kali anda ingin menerima/menghantar Altcoin, minimumkan masa di atas talian, buat *backup* (*online* dan fizikal) dan simpan kebanyakan Altcoin anda dalam *hardware wallet*.

Akhirnya, anda perlu ingat bahawa Altcoin ialah produk yang unik dan berbeza daripada kebanyakan produk-produk lain. Sebagai contoh, apabila anda sudah klik '*send*' ketika melakukan transaksi, Altcoin itu akan pergi buat selama-lamanya. Anda tidak boleh membatalkannya, tukar fikiran, minta balik atau minta *refund*. Tidak ada orang untuk anda telefon, tidak ada pejabat dan malah tidak ada autoriti di mana anda boleh pergi mengadu dan meluahkan rasa ketidakpuasan hati anda. Jadi tidak ada jalan kembali dalam Altcoin!

Oleh sebab itu, anda perlu berhati-hati setiap kali anda berinteraksi dengannya. Berikut adalah beberapa langkah yang anda perlu ambil:

- Periksa dan periksa lagi mengenai pihak yang anda ingin berurusan dalam melakukan transaksi Altcoin. Jika pihak itu nampak lain macam atau mempunyai banyak cerita negatif tentang mereka, jangan berinteraksi dengan mereka.
- Sebelum menghantar Altcoin, anda periksa dan periksa lagi jumlah Altcoin dan pastikan alamatnya betul.
- Simpan kebanyakan Altcoin anda dalam *hardware wallet* (saya tahu yang saya dah sebut tentang ini tetapi sebab ianya kritikal, saya ulang jugalah!).

Dan yang paling penting, gunakan otak anda.

TENTANG PENULIS

Azizi Ali merupakan penulis, penceramah dan mentor kewangan #1 di Malaysia.

Buku pertama beliau, *Jutawan Dari Planet Jupiter* telah mengubah senario percetakan di Malaysia. Ianya telah terjual melebihi 300,000 naskhah dan menjadi penggerak kepada seminar dan buku kewangan di Malaysia. Sejak itu, Azizi telah menulis lebih daripada 35 buah buku berkenaan kewangan dan penciptaan kekayaan. Tajuk-tajuk buku beliau yang laris di pasaran ialah *Bagaimana Hendak Menjadi Jutawan Hartanah, Lahirnya Seorang Jutawan, Pesara Jutawan, Masa Untuk Emas, Maharaja Wang* dan *Rahsia Bitcoin*. Buku beliau turut diterbitkan di Indonesia dan juga Brazil. Buku-buku beliau juga dijual dalam bentuk eBook di Amazon.com.

Beliau telah memberi ceramah di hadapan lebih 500,000 peserta seminar dan kerap muncul di media massa. Antara organisasi yang telah menjemput beliau ialah Jabatan Perdana Menteri, Kementerian Kewangan, Suruhanjaya Sekuriti, LHDN, KWSP, CIMB, Eco-World, Tabung Haji dan Petronas.

Azizi merupakan pemegang Chartered Financial Consultant (ChFC), Islamic Financial Planner (IFP) dan juga memegang Ijazah Sarjana (MBA) dari University of Bath, UK.

Untuk mengetahui lebih lanjut tentang Bitcoin,
sila log masuk ke laman web:

www.RahsiaBitcoin.my

Untuk mengetahui lebih lanjut tentang pelaburan emas,
sila log masuk ke laman web:

www.RahsiaEmas.com

Untuk mengetahui lebih lanjut tentang bisnes emas,
sila log masuk ke laman web:

www.RahsiaSuratPajak.com

Dapatkan petunjuk dan bimbingan secara
peribadi daripada Mentor Jutawan #1 Malaysia.
Sertai program Inner Circle sekarang!

www.InnerCircle.my

Sila layari www.BookPlanet.com.my untuk senarai penuh
buku-buku yang dapat membantu anda mencapai impian anda

www.BookPlanet.com.my