Apa itu Blockchain dan Cryptocurrency?

Blockchain adalah sistem pencatatan atau database yang tersebar luas di jaringan, atau disebut juga dengan istilah distributed ledger. Tapi apakah maksudnya?

Perbandingan Sistem Tradisional Dengan Blockchain

Saya yakin anda sudah bisa banyak menemukan definisi dari blockchain di internet, jadi saya akan coba jelaskan artinya dengan cara saya sendiri. Mari kita bandingkan sistem tradisional dengan sistem blockchain.

1) Sistem Tradisional: Kepercayaan Dengan Pihak Ketiga

Misalnya anda membeli secangkir kopi di café kesayangan anda di Mall. Sewaktu anda membayar, anda menggesekkan kartu kredit anda di mesin kartu café. Di sini terjadi sebuah transfer uang dari account anda ke account café tadi. Tapi anda tahu darimana bahwa transfer ini benar-benar terjadi? Mengapa café anda bisa percaya bahwa uang anda telah ditransfer ke account mereka? Ini dikarenakan ada pihak ketiga yang dipercaya oleh anda dan café anda. Dalam hal ini, pihak ketiga itu adalah bank anda, atau jaringan kartu yang anda gunakan (Visa, MasterCard, atau Amreican Express). Café anda mempercayai pihak ketiga itu.

Tapi apa yang akan terjadi jika sistem bank anda, atau pihak jaringan kartu kredit anda mengalami gangguan teknis atau misalnya di hack?

2) Sistem Blockchain

Blockchain adalah sistem yang tidak menggunakan pihak ketiga tersebut. Intinya, catatan transaksi-transaksi yang sudah terjadi, disimpan oleh banyak komputer yang tersebar di jaringan itu sendiri. Jadi akan lebih susah untuk men-hack sistem ratusan atau ribuan komputer, dan kemungkinannya kecil untuk semua komputer itu mengalami gangguan di waktu yang sama.

Jadi, jika anda misalnya membayar kopi anda menggunakan Bitcoin (salah satu cryptocurrency), Bitcoin untuk pembayaran kopi tersebut ditransfer dari alamat Bitcoin anda ke alamat Bitcoin cafe anda secara peer-to-peer. Dan transaksi ini akan dicatat di seluruh komputer yang tersebar di jaringan Bitcoin.

Analogi Sederhana Untuk Menjelaskan Cara Kerja Blockchain

1) Contoh Non-Blockchain: Sebuah RT Yang Mempercayai Pihak Ketiga

Di sebuah RT yang mempunyai 15 rumah, Pak RT mempercayai pencatatan transaksi finansial kepada Pak Budi. Pak Budi bertugas untuk mencatat siapa saja yang belum membayar iuran bulanan RT, dan juga rumah mana yang berhutang ke rumah lain jika mereka mengadakan acara makan bersama. Di sini, Pak Budi adalah pihak yang dipercayakan sebagai akuntan. Ke-15 rumah di RT tersebut, mempercayai Pak Budi untuk melakukan pencatatan yang akurat. Tentunya ada beberapa resiko di sini:

Bagaimana jika buku catatan finansial Pak Budi dicuri oleh pihak yang tidak bertanggung jawab?

Bagaimana jika Pak Budi mencoba mencuri uang kas RT?

Bagaimana jika sahabat-sahabat Pak Budi mencoba memanipulasi Pak Budi untuk menghapus hutang mereka dari catatan Pak Budi?

2) Jika RT Ini Menggunakan Sistem Blockchain

Jika kita ingin mengubah RT di atas untuk menggunakan sistem blockchain, maka Pak RT memulai dengan menanyakan ke para penghuni: siapa saja dari mereka yang tertarik untuk menjadi akuntan RT. Semisal ada 9 penghuni yang tertarik, maka 9 orang ini akan mencatat semua transaksi yang terjadi di RT itu, dan catatan mereka semua pun akan identik / sama. Dengan cara ini, akan lebih sulit untuk mencuri 9 buah buku catatan, atau pun untuk memanipulasi 9 orang yang berbeda.

Apakah keuntungan yang bisa didapat untuk menjadi akuntan di RT ini?

Cryptocurrency

Sebut saja di RT ini, semua penghuninya menyukai coklat, jadi kita akan gunakan coklat sebagai currency / uang yang dipakai di sini. 9 penghuni ini akan bekerja menjadi akuntan di RT itu, dan mereka akan bersaing untuk mendapatkan coklat imbalan dari pekerjaan akuntan mereka. Di dalam dunia blockchain dan cryptocurrency, 9 penghuni ini disebut juga sebagai miner (penambang) karena mereka bekerja untuk menambang coklat.

Jika ada sebuah kalkulasi transaksi yang kompleks, misalnya ke-15 rumah di RT ini semua mengadakan acara makan siang di restoran, dan semua orang memesan makanan yang berbeda sehingga pembayarannya pun berbeda, ke-9 akuntan RT ini akan bersaing untuk mengkalkulasikan transaksi paling cepat. Siapapun yang menyelesaikan kalkulasi paling awal, dan bisa dikonfirmasi oleh 8 akuntan lainnya bahwa perhitungannya benar, maka dia akan diberikan hadiah coklat. Inilah mengapa para penambang idealnya mempunyai sistem komputer yang kuat dan cepat.

Namun, selain dari 9 orang akuntan ini, para penghuni lain di RT ini juga bisa memperjual-belikan coklat itu sendiri, karena coklat ini mempunyai nilai (ada penawaran dan permintaan). Dan jika RT ini memiliki penduduk baru, permintaan coklat akan bertambah banyak, sehingga harga coklat akan naik karena permintaan yang lebih tinggi sedangkan jumlah penawaran (atau supply coklat) jumlahnya tetap.

Di dalam dunia cryptocurrency, coklat di atas adalah perumpamaan dari Bitcoin, Ether (currency yang digunakan oleh blockchain Ethereum), atau cryptocurrency lainnya.

Sifat-Sifat Blockchain Yang Penting Untuk Dimengerti Oleh Investor Cryptocurrency

Jika anda telah membaca dan mengerti konsep blockchain secara umum di atas, berikut ini adalah penjelasan lebih lanjut tentang blockchain dari sisi investor cryptocurrency.

1. Open-source dan Transparan

Cukup penting untuk dimengerti bahwa kode blockchain itu sifatnya transparan. Jika anda adalah seorang developer yang bisa membaca kode blockchain, anda bisa memverifikasi sendiri kode apa yang tertulis, misalnya pada Bitcoin:

Ada berapa banyak supply Bitcoin di saat permulaan (blok Genesis)

Berapa tingkat inflasi Bitcoin (untuk mengerti permintaan dan penawaran)

Jika anda bandingkan dengan mata uang umum sebuah negara (misalnya Dollar AS), yang biasanya dikontrol oleh bank sentral (Federal Reserve di Amerika Serikat), orang biasa seperti kita tidak akan pernah tahu seberapa banyak uang baru yang akan dicetak di masa depan, misalnya 10 tahun yang akan datang; Atau berapa suku bunga bank di tahun depan. Dengan cryptocurrency, semua ini bisa diverifikasi di dalam kode yang tertulis.

2. Ter-desentralisasi / Tidak Terpusat

Cryptocurrency adalah sistem yang tersebar, dimana tidak ada satu orang atau satu perusahaan yang mengontrolnya. Kode blockchain tidak terletak di sebuah server pusat yang dioperasikan oleh sebuah perusahaan, tetapi tersebar di ribuan komputer di jaringan blockchain tersebut. Anda pun bisa mempunyai node sendiri, dimana komputer / mesin anda berisikan blok-blok dan catatan transaksi blockchain tersebut.

3. Supply dan Tingkat Inflasi-nya Jelas (Datanya Tersedia)

Karena blockchain itu sifatnya transparan, kita bisa tahu secara tepat ada berapa banyak supply cryptocurrency tersebut dan ada berapa banyak yang akan dicetak di masa depan.

Mengapa Supply itu Penting?

Semua hal di dunia ini yang bisa dijual dan dibeli, mempunyai harga. Dan harga semua hal selalu bergantung dari supply dan demand (permintaan dan penawaran).

Bayangkan bila semua orang di dunia mempunyai pohon apel yang bisa memproduksi jumlah apel yang tidak terbatas, dengan kualitas yang sama. Maka harga apel akan menjadi sangat murah dan bahkan mungkin mendekati 0, karena percuma saja anda membeli sesuatu yang bisa anda produksi sendiri kapan pun anda mau.

Sebuah analogi lain: Bayangkan jika perusahaan mobil Ferrari hanya memproduksi 10 Ferrari special edition di dunia. Anda memutuskan untuk membeli satu buah mobil tersebut dengan harga mahal, karena sangat eksklusif. Akan tetapi di 5 tahun mendatang, ternyata Ferrari memutuskan untuk memproduksi mobil tersebut sebanyak 10 ribu unit. Bagaimana perasaan anda? Dan menurut anda, apa yang akan terjadi dengan harga mobil special edition tersebut?

Konsepnya sama dengan saham. Untuk mengerti harga atau nilai sebuah perusahaan, kita perlu mengerti berapa market capitalization perusahaan tersebut, yang bisa didapat dari jumlah saham dikalikan harga saham. Pendapatan di masa depan dan profit margin juga penting, namun ini adalah topik tersendiri.

Jumlah Supply dan Tingkat Inflasi Bitcoin

Mari kita lihat jumlah supply dan tingkat inflasi Bitcoin sebagai contoh. Grafik di bawah ini dibuat berdasarkan kode Bitcoin, dan bisa menggambarkan secar

a tepat berapa jumlah supply Bitcoin yang akan beredar di masa depan.

Jumlah Supply dan Tingkat Inflasi Bitcoin - Cointelegraph.com

4. Immutable (Tak Bisa Dibatalkan)

Apapun yang sudah terjadi dan dikonfirmasi di blockchain, tidak bisa dibatalkan. Jadi jika anda telah membuat kesalahan dalam mentransfer dana anda ke alamat yang salah, berarti dana anda hilang - kecuali jika pemilik dari account penerima tersebut berbaik hati untuk mengembalikan dana anda. Tapi harus diingat, hampir tidak mungkin kita bisa mengetahui siapa pemilik sebuah alamat cryptocurrency.

Tentu saja ada kasus-kasus pengecualian di blockchain dimana sesuatu bisa dibatalkan. Contohnya terjadi pada Ethereum. Pada waktu itu, seorang (atau sekelompok) hacker mencuri dana Ether yang sangat besar dari project The DAO (15% dari semua Ether yang beredar). Para penemu dan developer Ethereum tidak membiarkan hal ini terjadi dan membatalkan transaksi tersebut dengan sebuah hard fork yang membuahkan Ethereum versi baru. Tetapi versi lama Ethereum masih tetap di-maintain oleh beberapa pihak miner. Versi lama ini dikenal dengan nama Ethereum Classic.

5. Hampir Tidak Mungkin Untuk di-Hack

Project blockchain yang bagus tentunya akan didukung oleh banyak miner / penambang yang ikut membantu mengamankan jaringan blockchain tersebut dengan kekuatan mesin / komputer mereka. Penambangan cryptocurrency adalah bisnis tersendiri yang sangat besar. Para penambang diberi imbalan dengan cryptocurrency yang mereka tambang.

Pada intinya, para penambang bersaing untuk menyelesaikan sebuah perhitungan matematika. Siapapun yang berhasil memecahkan perhitungan tersebut dengan akurat dan menciptakan blok baru untuk blockchain tersebut, akan diberikan imbalan. Maka dari itu para penambang ini berani untuk berinvestasi besar untuk membeli perangkat komputer yang kuat dan juga membayar biaya listrik yang mahal untuk aktifitas mereka.

Sebuah catatan: Sistem penambangan di atas adalah untuk sistem blockchain proof-of-work, seperti Bitcoin. Beberapa tipe blockchain (seperti Ethereum di masa yang akan datang), menggunakan sistem proof-of-stake - atau virtual mining / penambangan virtual. Ini adalah topik tersendiri.

Untuk bisa meng-hack sebuah blockchain, anda harus mengontrol lebih dari setengah (>50%) kekuatan komputer yang ikut mengamankan jaringan blockchain tersebut (dikenal dengan nama penyerangan 51%).

Anda mungkin pernah mendengar bahwa sebuah blockchain pernah di-hack sebelumnya. Hack-hack ini umumnya terjadi pada sebuah exchange (seperti Mt.Gox), dan smart contract yang memiliki kelemahan security (seperti The DAO); dan bukan pada blockchain itu sendiri.

Untuk menggambarkan seberapa sulit dan mahal untuk mengontrol kekuatan 51% pada sebuah jaringan blockchain, di bawah ini adalah contoh aktifitas penambangan yang dilakukan oleh perusahaan dan perorangan:

Penambangan Bitcoin.com - Bitcoin.com - yang hanya mengkontribusikan sebesar 1.7% kekuatan hash rate pada saat tulisan ini dibuat.

Penambang Litecoin Perseorangan - Reckoner.com.au