



CRYPTOCURRENCY PERSPEKTIF ILMU EKONOMI

DR. SITI JAMILAH, S.E., M.Si.



DEFINISI

- *Cryptocurrency* adalah sebuah mata uang digital atau virtual yang dijamin oleh *cryptography*
- *cryptography* adalah sebuah metode yang digunakan untuk melindungi informasi dan saluran komunikasi melalui penggunaan kode.

ASSET KRIPTO

Aset kripto adalah komoditas tidak berwujud yang berbentuk **aset** digital yang menggunakan kriptografi, jaringan peer-to-peer, dan buku besar yang terdistribusi untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain.

- kriptografi adalah sebuah disiplin ilmu yang berkaitan erat dengan konsep kriptologi dan kriptanalisis.
- Kedua konsep ini mencakup teknik seperti *microdots*, yaitu teknik menggabungkan kata dengan gambar, dan cara-cara lain yang serupa untuk menyembunyikan informasi dalam *storage* pilihan atau transit.
- Namun, dalam dunia yang sudah serba digital, kriptografi kini sering dikaitkan dengan teknik *scrambling*, yaitu metode perubahan teks biasa menjadi teks sandi.
- Kedua proses ini lebih dikenal dengan istilah *encryption* dan *decryption*.
- Dengan adanya perubahan prioritas teknik yang digunakan untuk melindungi data, istilah kriptografi bergeser menjadi *modern cryptography*.

MODERN CRYPTOGRAPHY

Modern cryptography memiliki beberapa tujuan yang menjadi pedoman untuk para kriptografer.

Prosedur dan protokol yang memenuhi semua kriteria *cryptography* di disebut sistem kriptografi, yaitu :

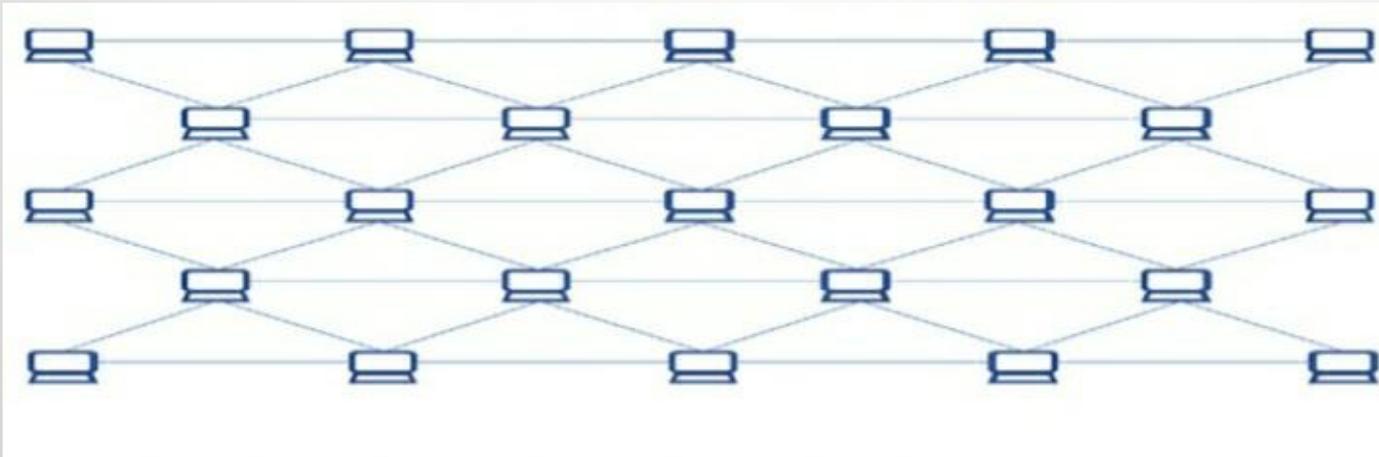
- *Confidentiality*: Informasi yang dilindungi tidak akan bisa diakses oleh siapa pun yang tak memiliki wewenang.
- *Integrity*: Data yang akan diterima dan dikirim tidak dapat diubah tanpa sepengetahuan kedua belah pihak.
- *Non-repudiation*: Pihak penerima atau pengirim tidak akan bisa menyangkal tujuannya menciptakan atau mengubah data.
- *Authentication*: Pihak penerima dan pengirim dapat mengetahui identitas masing-masing serta sumber data yang sedang mereka gunakan.

Blockchain



Blockchain adalah sistem pencatatan transaksi di banyak database yang tersebar luas di banyak komputer, yang masing-masing memuat catatan yang identikal. Sistem ini disebut juga dengan istilah distributed ledger. Dengan catatan transaksi yang terdesentralisasi ini, maka hampir tidak mungkin untuk di-hack atau dirubah secara sepihak, tanpa mengubah jumlah mayoritas dari semua database tersebut.

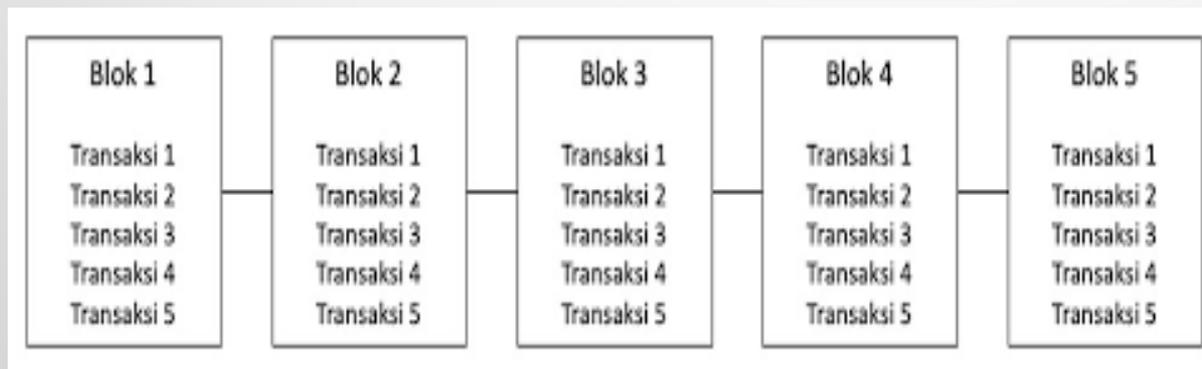
Gambar Blockchain :





Blockchain adalah sistem pencatatan transaksi dengan database tersebar (desentralisasi), catatan transaksi-transaksi ini dimuat dalam blok-blok yang saling tersambung. Jika satu blok sudah penuh, maka akan diciptakan blok berikutnya yang terkoneksi dengan blok sebelumnya. Catatan transaksi yang dimuat di blok yang sudah diciptakan, tidak akan bisa dirubah lagi sehingga blockchain sering disebut mempunyai sifat immutable (tidak dapat dirubah).

Rantainan block berisi catatan transaksi:



Perbandingan Sistem Tradisional Dengan Blockchain



Sistem Tradisional

Kepercayaan dengan pihak ketiga misalnya seseorang membeli secangkir kopi di cafe kesayangan di mall. Sewaktu orang itu membayar, orang itu menggesekkan kartu kredit di mesin kartu cafe. Di sini terjadi sebuah transfer uang dari account seseorang tersebut ke account cafe tadi. Akan tetapi cafe tersebut tahu darimana bahwa transfer ini benar-benar terjadi? Mengapa cafe tersebut bisa percaya bahwa uang orang tersebut telah ditransfer ke account mereka? Ini dikarenakan ada pihak ketiga yang dipercaya oleh seseorang tersebut dengan pihak cafe. Dalam hal ini, pihak ketiga itu adalah bank orang, atau jaringan kartu yang digunakan (Visa, MasterCard, atau American Express). Pihak cafe juga mempercayai pihak ketiga itu.

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

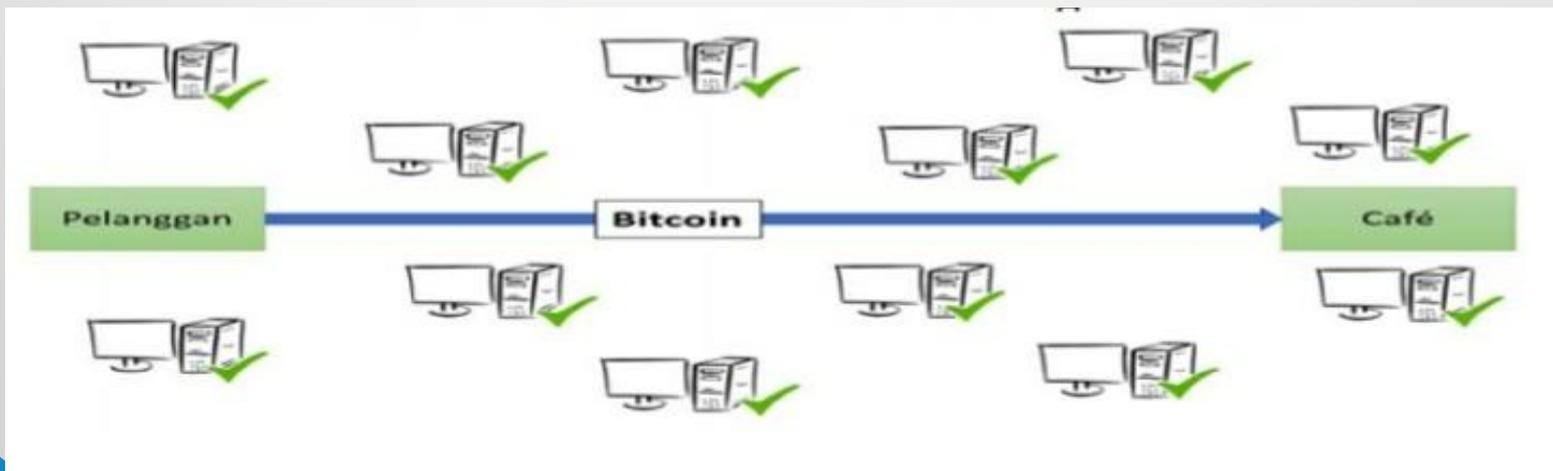


SISTEM BLOCKCHAIN

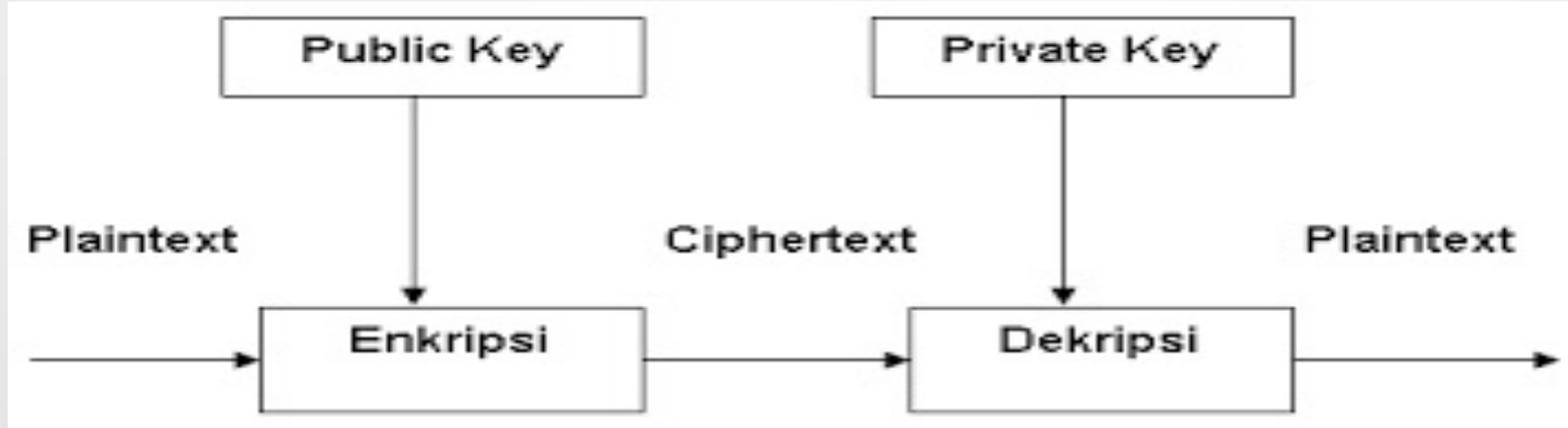


Blockchain adalah sistem yang tidak menggunakan pihak ketiga tersebut. Intinya, catatan transaksi-transaksi yang sudah terjadi, disimpan oleh banyak komputer yang tersebar di jaringan itu sendiri.

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 misalnya membayar kopi menggunakan Bitcoin, Ethereum, dan koin digital lainnya (salah satu crypto currency), misal penggunaan Bitcoin untuk pembayaran kopi tersebut ditransfer dari alamat Bitcoin anda ke alamat Bitcoin cafe secara peer-to-peer. Dan transaksi ini akan dicatat diseluruh komputer yang tersebar di jaringan Bitcoin.



SISTEM BLOCKCHAIN



1. Plaintext

Adalah pesan yang hendak dikirimkan dan berisi data berisi informasi yang asli.

2. Ciphertext

Adalah pesan tersandi yang merupakan hasil enkripsi dari plaintext.

3. Enkripsi

Adalah proses pengubahan informasi asli menjadi informasi yang tersandi.

4. Deskripsi

Merupakan kebalikan dari enkripsi dimana pengembalian data tersandi menjadi data asli yang dapat dimengerti.

5. Kunci/Key

Adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan deskripsi



Mata uang kripto tidak disimpan di bank atau *e-wallet*. Mata uang tersebut disimpan di sebuah sistem bernama blockchain

CARA KERJA CRYPTOCURRENCY

- Hal pertama ialah dengan meng-install wallet Bitcoin di komputer atau ponsel. Langkah ini secara otomatis akan membuat alamat Bitcoin pertama. Sama seperti email, kita bisa saling berbagi alamat Bitcoin kepada orang lain, sehingga mereka bisa membayar atau sebaliknya. Namun, alamat Bitcoin sebaiknya hanya digunakan sekali saja.
- Rantai-blok (blockchain) adalah sebuah catatan transaksi publik di mana jaringan Bitcoin bersandar. Semua transaksi yang telah dikonfirmasi tersimpan di dalam rantai-blok. Dengan demikian, wallet Bitcoin dapat menghitung sisa uang yang dapat dibelanjakan serta transaksi-transaksi baru dapat diverifikasi untuk memastikan bahwa memang dimiliki oleh pengguna itu.
- Private Keys, sebuah transaksi transfer nilai antar wallet Bitcoin yang dimasukkan ke dalam rantai-blok. Wallet Bitcoin menyimpan sebagian data rahasia yang disebut kunci pribadi atau seed, yang digunakan untuk menandatangani transaksi, memberikan bukti matematis bahwa memang benar berasal dari pemilik wallet.
- Pertambangan adalah sistem digunakan untuk mengonfirmasi antrian transaksi dengan memasukkannya ke dalam rantai-blok. Proses ini menegaskan urutan kronologis rantai-blok, melindungi netralitas jaringan, dan memungkinkan komputer lain untuk menyetujui keadaan sistem. Agar dapat dikonfirmasi, transaksi haruslah dirangkai dalam sebuah blok yang sesuai dengan aturan kriptografi ketat dan akan diverifikasi oleh jaringan. Pertambangan juga seperti sebuah lotre yang kompetitif dalam mencegah setiap individu menambahkan blok baru dengan mudah secara berturut-turut ke dalam rantai-blok.

Investasi Bitcoin

Banyak orang yang bilang jika investasi Bitcoin sama saja dengan investasi emas. Hal ini didasarkan pada beberapa karakteristik Bitcoin yang mirip dengan emas, seperti:

- Jumlahnya yang terbatas, hanya ada sekitar 21 juta saja di dunia.
- Nilai 1 Bitcoin sepadan dengan 100 juta, kita tidak harus membeli 1 Bitcoin, bisa juga membeli kurang dari 1 Bitcoin.
- Bitcoin tidak mengalami penurunan atau degradasi.
- Bitcoin bisa dipindahkan, tidak terpengaruh dengan jumlahnya yang terbatas.

Kemiripan-kemiripan ini yang lantas membuat Bitcoin disebut sebagai emas 2.0, apalagi cara investasi Bitcoin juga sama dengan investasi emas.

Cara Kerja Bitcoin

Mungkin beberapa orang sudah mengerti jika Bitcoin memiliki beberapa bagian yang juga menjadi cara kerjanya. Bagian-bagian tersebut, seperti:

- *Block Chain*. Di bagian ini, semua transaksi yang menggunakan Bitcoin dimuat. Transaksi dinyatakan telah selesai bila sudah masuk ke dalam bagian ini. *Block chain* berisi berbagai macam transaksi baru dan masing-masingnya terhubung dengan blok sebelumnya. Bahkan, transaksi yang ada bisa dirunut ke transaksi paling awal, yaitu ketika Satoshi Nakamoto menciptakan Bitcoin untuk pertama kalinya.

- *Miner*. Penambang Bitcoin bisa dibilang sebagai penjaga transaksi. Mereka memastikan agar transaksi-transaksi baru tercatat dan tidak ada yang mengganggu daftar transaksi lama. Disebut sebagai *miner* karena mereka yang menambang blok baru untuk memuat daftar transaksi baru. Sebagai kompensasinya, mereka akan mendapatkan beberapa Bitcoin. Peran mereka cukup penting, terutama untuk membuat sistem jaringan Bitcoin terus bekerja.

- *Wallet*. Seperti yang disebutkan di atas, Bitcoin yang kita miliki nantinya akan disimpan di *wallet*. Namun, sebenarnya yang disimpan hanyalah *private key* yang memberikan akses kepada pemilik Bitcoin untuk menambahkan transaksi ke *block chain*. Bitcoin sendiri tersimpan sebagai catatan transaksi yang ada di dalam *block chain* tersebut.

KARAKTERISTIK

1. **Digital:** *Cryptocurrency* adalah mata uang digital yang berarti hanya berlaku di komputer. *Cryptocurrency* tidak hadir dalam bentuk fisik yang dapat kita pegang sehari-hari.
2. **Peer-to-peer:** *Cryptocurrency* dapat digunakan untuk transaksi dari satu orang ke orang lainnya secara *online*.
3. **Global:** *Cryptocurrency* sama di setiap negara. Maka, transaksi dapat dilakukan secara bebas antarnegara tanpa terpengaruh oleh kurs.
4. **Terenkripsi:** Setiap pengguna memiliki kode tersendiri untuk bertransaksi dengan *cryptocurrency*. Setiap melakukan transaksi, pengguna tidak bisa melihat transaksi tersebut dilakukan oleh siapa. Tidak ada nama asli yang muncul dalam setiap transaksi *cryptocurrency*. Lebih dari itu, tidak ada aturan apa pun tentang siapa yang bisa menggunakan *cryptocurrency* dan digunakan untuk apa.
5. **Terdesentralisasi:** Transaksi uang pada umumnya selalu melibatkan pihak yang menengahi setiap transaksi, seperti bank. Namun di dunia *cryptocurrency*, tidak ada bank atau pihak tersebut. Setiap orang bertanggung jawab atas uang mereka sendiri.
6. **Truthless:** Dalam menggunakan *cryptocurrency*, kamu tidak perlu percaya kepada siapa pun dalam sistem.

FUNGSI

1. MEMBELI BARANG DAN JASA:

Saat ini, ada banyak toko yang mulai memberlakukan cryptocurrency sebagai alat pembayarannya, termasuk dua perusahaan ternama Overstock dan Newegg.

2. INVESTASI:

Investasi dengan cryptocurrency juga termasuk dalam kategori high risk. Prinsipnya kurang lebih sama dengan prinsip ekonomi, yaitu harga akan naik ketika ada banyak permintaan.

3. MINING :

Pada dasarnya, pengguna harus memecahkan teka-teki *cryptography* yang rumit untuk mengonfirmasi transaksi dan mencatatnya dalam *blockchain*.



CRYPTOCURRENCY DARI MASA KE MASA



Sumber:

Bright Finance, Money Crashers, Forbes, CNBC



Jenis-jenis Cryptocurrency

1. BITCOIN

- Jenis *cryptocurrency* ini pertama kali muncul pada 2009 oleh pihak yang bernama Satoshi Nakamoto. Tidak ada yang tahu apakah itu nama orang, kelompok, atau perusahaan dan dari mana mereka berasal.
- Pada November 2019, ada lebih dari 18 juta bitcoin yang diperdagangkan dengan total *market value* sekitar US\$146 miliar.
- Hingga kini, sekitar 68% *cryptocurrency* adalah bitcoin.



2. ETHEREUM

2. LITECOIN

- Jenis *cryptocurrency* ini hadir pada 2011 sebagai mata uang digital *peer-to-peer* (P2P) yang menghasilkan blok baru (yang membentuk *blockchain*) dengan kecepatan lebih cepat.
- Oleh karena itu, Litecoin memungkinkan pengguna melakukan transaksi dengan lebih cepat tanpa memerlukan sistem komputasi yang *powerful*.

3. DOGECOIN

- Dogecoin adalah turunan dari Litecoin yang muncul pada Desember 2013.
- Sesuai namanya, *dogecoin* adalah *cryptocurrency* yang menjadikan anjing Shiba Inu sebagai maskotnya.
- Jenis ini dikenal sebagai *cryptocurrency* yang paling bersahabat, sebab komunitasnya kerap melakukan donasi, amal, dan kegiatan-kegiatan positif lainnya.
- *Dogecoin* memiliki nilai yang jauh lebih rendah daripada *bitcoin*. Maka, tidak heran jika pengguna biasanya menggunakan jenis *cryptocurrency* ini untuk transaksi kecil, donasi, dan memberi tip.

4. BITCOINCASH

- BitcoinCash baru diluncurkan pada Agustus 2017, tetapi saat ini sudah menjadi lima *cryptocurrency* terbaik.
- Jenis ini diluncurkan karena adanya sekelompok pengguna Bitcoin tidak setuju dengan beberapa aturan yang berlaku.
- Mereka kemudian memisahkan diri dan membentuk mata uang digital sendiri yang bernama BitcoinCash. Kelompok tersebut juga melakukan beberapa improvisasi yang menurut mereka lebih baik dari *cryptocurrency* pertama tersebut.

5. FEATHERCOIN

- Feathercoin adalah jenis *cryptocurrency* yang bersifat *open source*. Jenis ini dibuat oleh Peter Bushnell, seorang IT *officer* di Brasenose College, Oxford Univesity pada April 2013.
- Feathercoin memiliki kemiripan dengan Litecoin dan berada di bawah lisensi MIT/X11.

HARGA CRYPTOCURRENCY

- BITCOIN => 1 Bitcoin = Rp. 471,673,126.40
- ETHEREUM => 1 Ethereum = Rp. 35,943,702.57
- LITECOIN => 1 Litecoin = Rp. 2,257,530.43
- DOGECOIN => 1 Dogecoin = Rp. **5,350.83**
- BITCOINCASH => 1 Bitcoincash = Rp. 8,296,490.59
- FEATHERCOIN => 1 Feathercoin = Rp. 367.51