BAB II

LANDASAN TEORI

2.1.Cloud Mining

Cloud mining adalah penyedia jasa layanan perangkat mining untuk di sewakan ke pengguna bitcoin dengan share Ghs. Penyedia jasa biasanya menawarkan layanan *mining* melalui *website*nya untuk para *user* yang berminat untuk bergabung bersama- sama melakukan *mining* dengan sewa kontrak biasanya akan di beri *price list* (per ghs) dan berapa lama tenggang kontrak yang berlaku dan berapa presentase profit yang di dapat.

Untuk melakukan *mining* Bitcoin sendiri memang banyak hal yang harus di pertimbangkan selain pembelian komputer khusus *mining*, biaya listrik yang mahal lalu tata cara perawatan *hardware* beserta *software*nya, selain itu seorang *miner* juga harus di bekali pemahaman seluk beluk *hardware* dan *software* komputer.

Cloud mining atau cloud hashing memungkinkan pengguna untuk membeli kapasitas penambangan perangkat keras di pusat data. *Cloud mining* Bitcoin, kadang-kadang disebut juga cloud hashing, memungkinkan pengguna untuk membeli output daya penambangan Bitcoin dari perangkat keras penambangan Bitcoin yang ditempatkan di pusat data jarak jauh.

Penambangan Bitcoin dapat dikendalikan dari jarak jauh, hal ini memungkinkan pemilik untuk tidak berurusan dengan gangguan yang biasanya ditemui ketika menambang bitcoin seperti listrik, masalah hosting, panas, instalasi atau masalah perawatan.("Bitcoin Cloud Mining Contract Reviews". Bitcoin Mining. 28 Juni 2017 diakses pada 11 september 2018).

2.2.Cyber Crime

Kejahatan dunia maya atau disebut juga *cyber crime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit (*carding*), penipuan identitas, pornografi anak, dan lain sebagainya.

Kejahatan dunia maya (*cyber crime*) umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Perkembangannya *internet* ternyata membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin atau tidak terpikirkan akan terjadi. Sebuah teori

menyatakan, *crime is product of society its self*, yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan.

Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi *internet* ini sering disebut dengan *cyber crime* (Ari Juliano Gema, 2000). Dari pengertian ini tampak bahwa *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi *internet*. Definisi ini tidak menyebutkan secara spesifik dari karakteristik *cyber crime*. Definisi ini mencakup segala kejahatan yang dalam modus operandinya menggunakan fasilitas *internet*.

Menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital (Ade Maman Suherman, 2002: 168).

Berdasarkan definisi tersebut tidak dijelaskan apa maksud kata "jaringan komputer". Apabila dimaknai secara luas maka akan meliputi LAN (*Local Area Network*) dan *Internet*. LAN merupakan jaringan tertutup. Jenis kejahatan yang disebut termasuk dalam kategori *cyber crime* tidak dapat dilakukan dalam LAN ini, semisal dengan *spamming*,*cybersquatting*, dan lain sebagainya.

Cyber crime sering diidentikkan dengan *computer crime*. *The US Department of Justice* memberikan pengertian *computer crime* sebagai "*any illegal act requiring knowledge of computer for its perpetration, investigation, or*

prosecution". Artinya "setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki, dan menuntutnya" (Ari Juliano Gema, 2000).

Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu "*any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data*". Artinya "setiap perilaku ilegal, tidak pantas, tidak mempunyai kewenangan yang berhubungan dengan pengolahan data dan/atau pengiriman data" (Ari Juliano Gema, 2000).

Indra Safitri mengemukakan, kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan *internet* (Indra Safitri, 1999).

Laporan kongres PBB X/2000 dinyatakan *cyber crime* atau *computer related crime*, mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau bantuan peralatan komputer (Barda Nawawi Arief, 2003: 259).

2.3.Cryptocurrency

Cryptocurrency terdiri dari kata *Crypto* dan *currency*, bila ditinjau dari segi bahasa maka artinya adalah "Mata Uang Rahasia", karena *Crypto* artinya rahasia dan *currency* adalah mata uang. Arti ini sedikit mirip dengan pengertian dari segi istilahnya, yaitu "Mata uang yang bersifat digital dan rahasia".

Cryptocurrency adalah mata uang yang berbentuk digital(digital/*virtual currency*) dan juga bersifat rahasia, tentu saja karena berbentuk digital maka tidak ada bentuk fisiknya, kecuali membuat sendiri dari emas atau logam lain dengan nilai sama. Mata uang ini tetap mempunyai nilai, seperti membeli Laptop atau *Smartphone* dari *Apple* menggunakan Bitcoin. *Cryptocurrency* pertama yang dibuat adalah Bitcoin, oleh karena itu Bitcoin yang paling terkenal. Bitcoin dibuat oleh seorang "*Anonymous*" bernama Satoshi Nakamoto, setelah Bitcoin muncul, akhirnya muncul juga coin-coin lain yang disebut Altcoin(*Alternative Coin*), seperti Litecoin dan Dogecoin.

Gambar 2.1: contoh contoh coin *Cryptocurrency*

Sifat yang membedakan *Cryptocurrency* dengan uang biasa adalah sifatnya terdesentralisasi dan rahasia. Terdesentralisasi artinya mata uang ini tidak diatur oleh orang/organisasi tertentu, termasuk pembuatnya sendiri. Jadi harganya bisa naik turun, bisa jadi mahal lalu terjun bebas jadi sangat murah. *Cryptocurrency* juga bersifat rahasia, karena namanya juga "*Crypto*". *Cryptocurrency* menggunakan metode kriptografi untuk mengamankan dan merahasiakan transaksi. Perlu diketahui bahwa banyak penjahat di *Deepweb* yang bertransaksi menggunakan *Cryptocurrency* karena memang FBI pun tidak akan tahu seseorang mengirim dengan nominal berapa ke orang lain untuk membayar sesuatu. Cara alami mendapatkan Cryptocurrency yaitu menambang dengan komputer, tapi arti menambangnya bukan berarti menggali sesuatu. Cara komputer menambang yaitu dengan menyelesaikan transaksi dari pengguna lain, jadi seperti mengurus transaksi orang lain kemudian dibayar.(“Apa Yang Dimaksud Dengan Cryptocurrency”.finansialku.com.23 Januari 2018. Diakses pada 11 september 2018).

2.4.BitCoin

Bitcoin adalah sebuah uang elektronik yang di buat pada tahun 2009 oleh Satoshi Nakamoto. Nama tersebut juga dikaitkan dengan perangkat lunak sumber terbuka yang dia rancang, dan juga menggunakan jaringan *peer-to-peer* tanpa penyimpanan terpusat atau *administrator* tunggal di mana Departemen Keuangan Amerika Serikat menyebut bitcoin sebuah mata uang yang terdesentralisasi.

Bitcoin tidak tergantung dengan mempercayai penerbit utama. Bitcoin menggunakan sebuah database yang didistribusikan dan menyebar ke node-node dari sebuah jaringan P2P ke jurnal transaksi, dan menggunakan kriptografi untuk menyediakan fungsi-fungsi keamanan dasar, seperti memastikan bahwa bitcoin-bitcoin hanya dapat dihabiskan oleh orang memilikinya, dan tidak pernah boleh dilakukan lebih dari satu kali.

Desain dari Bitcoin memperbolehkan untuk kepemilikan tanpa identitas (*anonymous*) dan pemindahan kekayaan. Bitcoin - bitcoin dapat disimpan di komputer pribadi dalam sebuah format *file wallet* atau di simpan oleh sebuah servis *wallet* pihak ketiga, terlepas dari semua itu Bitcoin - bitcoin dapat di kirim lewat internet kepada siapapun yang mempunyai sebuah alamat Bitcoin. Topologi *peer-to-peer* bitcoin dan kurangnya administrasi tunggal membuatnya tidak mungkin untuk otoritas, pemerintahan apapun, untuk memanipulasi nilai dari bitcoin - bitcoin atau menyebabkan inflasi dengan memproduksi lebih banyak bitcoin.

Bitcoin adalah salah satu dari implementasi pertama dari yang disebut *cryptocurrency*, pertama kali di deskripsikan oleh Wei Dai pada tahun 1998 dalam milis cypherpunks.(“Bitcoin”.wikipedia.diakses pada 11 september 2018).

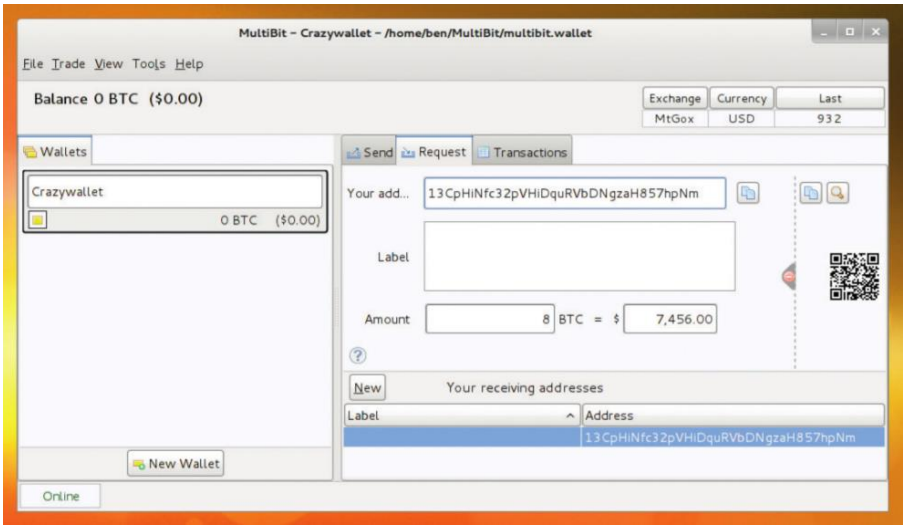
2.5.Block Chain

Block chain adalah daftar tiap transaksi Bitcoin yang pernah terjadi. Sebelum transaksi masuk ke *block chain*, maka transaksi itu belum selsai. Sesuai namanya, *block chain* merupakan rangkaian/rentetan sebuah blok. Blok tersebut

berisi sekumpulan transaksi baru dan terhubung dengan blok sebelumnya. Semua orang dapat memvalidasi *block chain* dengan mengikuti seluruh catatan yang merekam setiap transaksi sampai dengan transaksi pertama saat Satoshi Nakamoto membuat Bitcoin, tidak ada satu organisasi atau perseorangan pun yang memegang salinan block chain sendiri. Bitcoin dibuat agar terdistribusi dengan baik, sehingga tidak ada titik kesalahan yang dapat merusak *block chain* baik secara sengaja maupun tidak disengaja. *Block chain* dipegang oleh setiap komputer yang menambang Bitcoin.

Block chain merupakan catatan tiap transaksi yang dapat diverfikasi secara publik. Setiap detail transaksi akan disebarluaskan ke semua *miner* yang ada di jaringan bitcoin dengan permintaan agar dimasukkan ke blok berikutnya.

Seorang *miner* dapat dibayar atas pekerjaannya menambah sebuah blok, ada dua hal yang harus terjadi, harus memastikan hash-nya valid dan blok tersebut tercatat di *block chain*. Syarat pertama murni tantangan yang bersifat teknis, sedangkan syarat yang kedua akan memaksa mereka untuk memeriksa semua kemungkinan. *Block chain* yang mengandung transaksi yang tidak valid (misal, seseorang melakukan transaksi dengan coin yang tidak mereka miliki), maka *miner* berikutnya yang mendapatkan kiriman dari *miner* tersebut akan menolak sehingga ia tidak mendapat bayaran. *Miner* akan memeriksa setiap transaksi untuk memastikan kevalidannya sebelum ditambahkan ke dalam sebuah blok.



Gambar 2.2: contoh wallet chain block

Seorang miner menerima sebuah blok dari miner lainnya, akan mendapatkan insentif saat menemukan kesalahan karena dua hal. Pertama, jika menolak sebuah blok, itu artinya masih memiliki kesempatan untuk menambangnya untuk sendiri. Kedua, jika menerima blok yang oleh miner lain ditolak karena tidak valid, maka penambangan yang di lakukan akan sia-sia karena blok ini tidak akan masuk ke *block chain*, pada waktu yang sama mereka akan mendapatkan insentif saat menerima blok yang valid, karena jika menolak sebuah blok yang diterima oleh *miner* lain, maka blok selanjutnya yang mereka tambang akan ditolak oleh *miner-miner* lain.

Masalah yang mungkin terjadi yaitu dua miner dapat membuat *block* yang sama pada waktu yang bersamaan dan mengirimkannya ke *miner* lain, saat hal ini terjadi akan ada sebuah perpecahan di *block chain*. *Miner* dapat bekerja di salah satu blok, dan *miner* yang lain di blok satunya. Aturan Bitcoin menyatakan bahwa

block chain valid yang lebih panjang yang akan dipakai. Salah satu dari perpecahan dua perpecahan tadi salah satunya akan masuk ke blok berikutnya lebih dulu, sehingga *miner* akan melewatkan *chain* yang lebih pendek agar mendapat bayaran untuk menambang *chain* yang lebih panjang.

Aturan ini memastikan bahwa sebuah jaringan *miner* yang ingin memaksimalkan keuntungan pribadi tetap menjaga integritas mata uang ini. Sekelompok *miner* yang ingin mengakali sistem akan membutuhkan *computing power* yang lebih besar dari kombinasi semua *miner* yang benar (agar mereka dapat menambang blok dengan *rate* yang lebih cepat dan memiliki *block chain* lebih panjang). *Hashcash* selanjutnya mengamankan jaringan Bitcoin melalui raw *computing power*.

Penambangan Bitcoin harus tetap untung. Jaringan Bitcoin memiliki performa sebesar 15 peta hash per detik dan terus naik, untuk membeli *computing power* yang lebih besar untuk mengalahkan angka di atas akan membutuhkan sekitar 150 juta poundsterling dan akan terus bertambah. Harga ini belum termasuk listrik, ruang penyimpanan, pendinginan, gaji orang yang menjalankannya,dan lain lain.(“Memahami Cara Kerja Bitcoin”.codepolitan.11 juli 2017.diakses pada 11 september 2018).

2.6.HashCash

Hashcash adalah sistem yang digunakan oleh *miner* untuk memverifikasi bahwa mereka telah menambah sebuah blok sebelum blok tersebut dimasukkan ke

block chain. Fungsi dasarnya adalah membuat *block chain* menjadi tidak memungkinkan untuk diubah.

Proses ini bergantung pada proses *hashing*, terutama fungsi *hash* SHA256. Fungsi ini menerima sebuah input dan mengeluarkan output sebuah angka 256-bit. Angka yang dimasukkan ke fungsi *hash* adalah *header block* (didalamnya terdapat sebuah *counter*) dan semua *hash* dari transaksi lain. Tugas *miner* adalah mencari nilai untuk *counter* dimana *output* dari fungsi *hash* berada di bawah nilai tertentu. Batas nilai ini akan menyesuaikan dengan pengaturan kesulitan saat ini, yang normalnya berubah tiap 2016 blok.

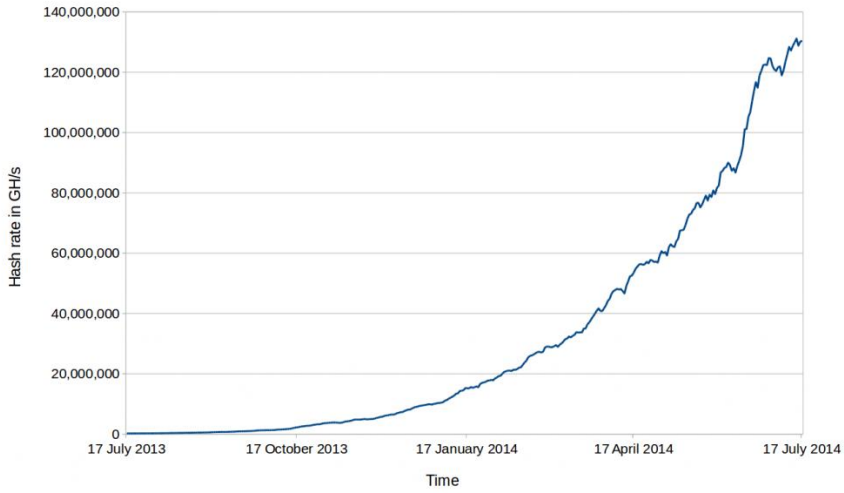
Satu-satunya cara untuk mendapatkan nilai *hash* yang dibutuhkan adalah dengan *computing power* yang besar, dengan makin banyaknya nilai *hash* yang didapatkan dalam waktu yang lebih cepat akan memperbesar kemungkinan mendapatkan nilai yang memenuhi. Saat nilai *hash* ditemukan, itu artinya kita sudah menambah blok tersebut dan dapat mengirimkannya ke *miner* lain di jaringan.

Kecepatan sebuah jaringan atau sebuah komputer penambang Bitcoin dilihat dari berapa banyak *hash* yang dapat dicoba dalam satuan waktu (biasanya dihitung dalam juta hash perdetik atau GHs).

Miner tidak perlu khawatir pekerjaan mereka diambil orang karena didalamnya ada *hash* dari semua transaksi dan salah satu transaksi itu adalah

bayaran untuk *miner* itu sendiri karena menambang blok. Hasil ini tidak bisa diambil orang tanpa mengubah nilai *hash*-nya.

Algoritma *hashcash* yang digunakan oleh Bitcoin sedikit berbeda dengan algoritma yang digunakan untuk mendeteksi pesan *spam*, meskipun cara kerja keduanya hampir mirip.



Gambar 2.3: grafik *hashcash* dari 17 jul 2013 sampai 17 juli 2014

2.7. Wallet

Wallet Bitcoin adalah tempat (dompet) penyimpanan Bitcoin, seseorang tidak akan bisa memiliki Bitcoin tanpa mempunyai tempat penyimpanan Bitcoin (Dompet Bitcoin / Wallet Bitcoin). Fungsi wallet Bitcoin ini adalah untuk menyimpan beberapa keypair kriptografi, atau lebih biasa dikenal dengan sebutan "*Bitcoin Address*" (alamat Bitcoin).

Sifat Wallet Bitcoin berbeda dengan dompet konvensional yang biasa kita kenal, yang fungsinya mampu menyimpan sejumlah uang. Wallet Bitcoin memiliki fungsi yang berbeda, karena dompet Bitcoin akan mengorganisasikan sejumlah alamat Bitcoin (*Bitcoin address*) yang dimiliki oleh si pengguna. Jumlah dana yang dimiliki pengguna dapat diakses dengan melakukan permintaan data jumlah dana yang terdapat pada alamat-alamat Bitcoin yang dimiliki dan menjumlahkannya.

Pengguna Bitcoin bisa memiliki banyak alamat bitcoin, dengan alamat bitcoin (*Bitcoin Address*) inilah pengguna Bitcoin bisa saling bertransaksi, baik mengirim maupun menerima Bitcoin dari pengguna lainnya, untuk bisa membelanjakan Bitcoin pemilik membutuhkan baris kode khusus bernama "private key". Baris kode ini disimpan di dalam "wallet" atau dompet digital, ketika akan dipakai barulah pemilik mengakses kode tersebut dan menggunakannya untuk transaksi. Hal yang perlu diketahui ada 2, yakni tentang *Private Key*, dan *Public Key* dalam *wallet Bitcoin*.

Private Keys

Private Key (kunci rahasia), hanya diketahui oleh pemilik alamat Bitcoin, sifatnya private key berfungsi layaknya sebagai nomor PIN dalam sebuah rekening Bank. Secara garis besar *Private Key* inilah sebagai kunci pengaman pengguna bitcoin. *Private key* bisa disimpan di komputer maupun dicetak dengan printer, jika

Private Key ini diketahui orang lain maka besar kemungkinan akan bisa dicuri oleh orang lain.

Contoh Private Key:
5KJvsngHeMpm884wtkJNzQGaCErckhHJBGFsvd3VyK5qMZXj3hS

Public Keys

Public Key, lebih tercermin pada alamat bitcoin (Bitcoin Address). Public Key didalam Bitcoin, memiliki fungsi untuk mengidentifikasi alamat pengirim dan penerima Bitcoin. Sehingga bitcoin akan bisa didistribusikan kepada orang lain.

Contoh Alamat Bitcoin:
1rYK1YzEGa59pI314159KUF2Za4jAYYTd