BAB II

LANDASAN TEORI

2.1 Teknologi *Blockchain*

2.1.1 Definisi *Blockchain*

Blockchain adalah program atau protokol komputer yang memungkinkan banyak pengguna dari jaringan yang sama untuk merekam data berupa informasi transaksi pada satu buku besar terdistribusi, di mana setiap pengguna dapat melihat informasi dan data transaksi yang telah dimasukkan (Hamza, 2018).

Blockchain pada dasarnya adalah *ledger* atau buku besar yang menggunakan jaringan *Peer-to-Peer* (P2P) yang dapat diakses secara publik tanpa memerlukan otoritas pusat atau perantara pihak ketiga (Mohamed & Ali, 2018).

Blockchain merupakan hasil dari pengembangan teknologi berupa platform yang memungkinkan pengguna untuk dapat terus menerus mengakses jaringan *blockchain*, dan dilindungi dengan enkripsi sehingga tidak dapat diretas dengan mudah (Stein Smith, 2020).

Berdasarkan tiga definisi menurut para ahli di atas, dapat ditarik kesimpulan bahwa *blockchain* merupakan *database* terdistribusi yang merekam detail transaksi dalam blok-blok yang terlindungi oleh metode keamanan kriptografi dengan memanfaatkan protokol enkripsi.

2.1.2 Sejarah *Blockchain*

Konsep di balik teknologi *blockchain* sebenarnya sudah ada sejak akhir 1980-an dan awal 1990-an. Namun, upaya-upaya awal untuk mengembangkan konsep tersebut kurang berhasil dan tidak bertahan lama. Hingga pada tahun 2008, seseorang atau kelompok dengan nama samaran Satoshi Nakamoto menerbitkan *whitepaper* yang berjudul "*Bitcoin: A Peer-to-Peer Electronic Cash System"*. Kemudian pada tahun 2009 terbentuklah jaringan *blockchain* terdesentralisasi pertama untuk mata uang virtual *Bitcoin*.

2.1.3 Jenis *Blockchain*

Teknologi *blockchain* dapat dibagi menjadi dua jenis berdasarkan model perizinannya, yaitu *blockchain* publik dan *blockchain* privat.

1. *Blockchain* Publik

   Jaringan *blockchain* publik disebut juga sebagai *permissionless blockchain* karena semua pengguna dapat membuat blok baru tanpa memerlukan izin dari otoritas mana pun. Mayoritas *blockchain* jenis ini merupakan perangkat lunak *open-source*, yang tersedia secara bebas bagi siapa saja yang ingin mengunduh dan menggunakannya. Contoh *blockchain* jenis ini adalah *Bitcoin*.

2. *Blockchain* Privat

   Jaringan *blockchain* privat atau *permissioned blockchain* adalah jaringan di mana blok baru yang dibuat pengguna harus disahkan terlebih dahulu oleh beberapa otoritas, baik itu terpusat atau terdesentralisasi.

2.1.4 Komponen *Blockchain*

Seperti teknologi lain pada umumnya, *blockchain* juga memerlukan komponen-komponen agar dapat bekerja dengan baik, berikut akan diuraikan setiap komponen utama *blockchain*.

1. Fungsi *Hash* Kriptografi

   Teknologi *blockchain* menggunakan fungsi *hash* kriptografi untuk operasi yang dijalankan. Cara kerja komponen ini disebut dengan istilah *hashing*. *Hashing* adalah metode penerapan fungsi *hash* kriptografi pada *string* data, yang kemudian akan mengeluarkan *output* berupa huruf dan angka yang relatif unik, untuk hampir semua jenis dan ukuran *input* (contohnya, *file*, teks, atau gambar). Hal ini memungkinkan pengguna untuk memvalidasi kesamaan data secara mandiri dengan cara mengambil data *input*, lalu meng-*hash string* data tersebut, dan apabila *output* yang diperoleh memiliki nilai yang sama, maka dapat dipastikan bahwa tidak ada perubahan dalam data. Tabel di bawah menunjukkan perubahan *string* data sekecil apa pun akan menghasilkan nilai yang jauh berbeda.

Tabel II.1 *Hash* SHA-256

Input	**Nilai *Hash* SHA-256**
KTTA	0x1d08dfda11bf2165391f5b92660b5834420bc4522ce67ad4c61a122671b517f1
KTTa	0xb2161fe7523cb59575bb3fe35b0b79d67de120546a9f67f59ff562e31b8de06b
DATA	0xc97c29c7a71b392b437ee03fd17f09bb10b75e879466fc0eb757b2c4a78ac938
data	0x3a6eb0790f39ac87c94f3856b2dd2c5d110e6811602261a9a923d3bb23adc8b7

2. Transaksi

   Sebuah transaksi menunjukkan adanya interaksi antara para pengguna. Misalnya pada *cryptocurrency*, informasi bahwa pengguna A telah mengirimkan uang virtual sejumlah X ke pengguna B sekitar 1 menit yang lalu, dapat terlihat pada transaksi yang sudah terekam pada blok yang baru saja dibuat. Setiap blok dalam *blockchain* dapat berisi nol atau lebih transaksi, hal ini diimplementasikan agar keamanan jaringan *blockchain* tetap terjaga. Dengan adanya blok-blok baru yang terus menerus diterbitkan, dapat mencegah oknum yang berniat untuk membuat *blockchain* tiruan kemudian mengubahnya.

3. Kunci Asimetris Kriptografi

   Teknologi *Blockchain* menggunakan kunci asimetris kriptografi dalam operasinya. Kunci asimetris kriptografi merupakan sepasang kunci yang terdiri dari kunci publik dan kunci privat yang secara matematis saling terkait satu sama lain. Kunci asimetris kriptografi memiliki beberapa fungsi sebagai berikut :

   a. Kunci pribadi digunakan untuk menandatangani transaksi secara digital.
   b. Kunci publik digunakan untuk mendapatkan alamat pengguna.
   c. Kunci publik digunakan untuk memverifikasi tanda tangan yang dihasilkan dengan kunci pribadi.

d. Kunci asimetris kriptografi menyediakan kemampuan untuk memverifikasi bahwa pengguna yang mentransfer nilai ke pengguna lain memiliki kunci pribadi yang mampu menandatangani transaksi.

4. Alamat

   Jaringan *blockchain* pada umumnya menggunakan alamat, yang merupakan sebuah karakter alfanumerik pendek yang merupakan hasil dari penerapan fungsi *hash* kriptografi pada kunci publik pengguna, bersama dengan beberapa data tambahan. Sebagian besar implementasi komponen alamat pada jaringan *blockchain* adalah sebagai titik akhir "ke" dan "dari" dalam suatu transaksi. Alamat cenderung lebih pendek dari kunci publik dan tidak rahasia.

5. Buku Besar

   Seperti halnya buku besar tradisional, istilah buku besar pada *blockchain* juga memiliki makna yang sama, yakni kumpulan transaksi. Komponen buku besar ini disimpan secara digital, dan dapat diterapkan secara terpusat maupun terdesentralisasi.

6. Blok

   Ketika pengguna mengirimkan transaksi ke jaringan *blockchain,* melalui perangkat lunak pada *smartphone* ataupun komputer. Transaksi tersebut akan dikirim dulu ke sebuah *node* dalam jaringan *blockchain*. Sederhananya, *node* merupakan pengguna yang menjalankan perangkat lunak *blockchain*. Kemudian, transaksi yang dikirimkan akan disebarkan ke *node* lain di dalam jaringan *blockchain*, namun transaksi

ini belum terekam pada *blockchain*. Transaksi akan direkam ke *blockchain* ketika *node* yang terpilih menerbitkan blok. Sebuah blok berisi *header* blok dan data blok, *header* blok berisi *metadata* (nomor blok, informasi waktu, ukuran blok, dll.) untuk blok tersebut, sedangkan data blok berisi daftar transaksi yang telah divalidasi. Blok baru kemudian akan dirantai bersama blok yang berisi *hash* dari *header* blok sebelumnya, terus menerus sehingga membentuk *blockchain*.

2.1.5 Model Konsensus *Blockchain*

Salah satu aspek penting dalam proses operasi jaringan *blockchain* adalah menentukan *node* penerbit mana yang akan menerbitkan blok berikutnya. Pada jaringan *blockchain* publik, umumnya ada banyak *node* penerbit yang bersaing pada waktu yang sama, karena untuk setiap blok yang berhasil diterbitkan, akan diberikan *reward* yang umumnya berupa biaya transaksi. Proses ini diselesaikan melalui penerapan salah satu dari beberapa model konsensus sebagai berikut.

1. Model Konsensus *Proof of Work*

   Dalam model *Proof of Work* (PoW), hak menerbitkan blok baru akan diberikan kepada *node* yang pertama kali berhasil memecahkan algoritma berupa teka-teki komputasi. Solusi dari teka-teki kemudian menjadi "bukti" bahwa *node* yang bersangkutan telah memecahkan algoritma tersebut. Algoritma ini dirancang sedemikian rupa agar tidak mudah dipecahkan, sehingga model konsensus ini membutuhkan sebuah perangkat keras berspesifikasi tinggi untuk memecahkan algoritma. Model konsensus ini identik dengan sebutan *mining*.

2. Model Konsensus *Proof of Stake*

   Model *Proof of Stake* (PoS) atau *staking* didasari pada konsep bahwa semakin banyak jumlah *stake* yang diinvestasikan pengguna ke dalam sistem jaringan *blockchain*, maka semakin besar pula kemungkinan *node* mereka untuk terpilih. Dengan kata lain, *staking* berarti menginvestasikan sebagian besar aset berupa mata uang yang pengguna miliki, dengan harapan agar *node* mereka terpilih menjadi *node* penerbit selanjutnya, yang kemudian akan mendapatkan timbal balik berupa mata uang serupa sesuai dengan persentase yang telah disepakati pada awal program *staking*.

3. Model Konsensus *Proof of Elapsed Time*

   Pada model konsensus *Proof of Elapsed Time* (PoET), setiap *node* penerbitan akan meminta waktu tunggu dari masing-masing sistem komputer mereka, kemudian sistem akan menghasilkan waktu tunggu acak, masing-masing *node* penerbitan lalu mengambil waktu acak yang diberikan dan menjadi tidak aktif atau *idle* selama durasi tersebut. Setelah ada *node* penerbitan yang bangun dari keadaan *idle*, *node* tersebut akan membuat dan menerbitkan blok baru ke jaringan *blockchain*, kemudian setiap *node* penerbitan yang masih dalam keadaan *idle* akan aktif kembali, dan seluruh proses dimulai lagi dari awal.

4. Model Konsensus *Proof of Authority* atau *Proof of Identity*

Model konsensus ini akan memilih *node* penerbit yang telah diketahui identitasnya. Setiap *node* penerbit harus memiliki identitas yang terbukti dan dapat diverifikasi dalam jaringan *blockchain* (contoh, KTP yang telah diverifikasi dan disertakan pada jaringan *blockchain*). Tindakan yang dilakukan pengguna jaringan *blockchain* akan secara langsung memengaruhi reputasi *node* penerbit. *Node* penerbit dapat memperoleh reputasi dengan melakukan aktivitas sesuai ketentuan sistem mendapatkan dan disetujui oleh pengguna lain, sebaliknya *node* penerbit juga dapat kehilangan reputasi bila beraktivitas dengan cara tidak sesuai dan tidak disetujui oleh pengguna lain. Semakin rendah reputasinya, maka semakin kecil kemungkinan untuk mendapatkan hak menerbitkan blok. Oleh karena itu, semua pengguna berkewajiban untuk terus-menerus mempertahankan reputasinya.

2.2 Sistem Informasi Akuntansi

2.2.1 Definisi Sistem Informasi Akuntansi

Sistem ini merupakan sekumpulan dua atau lebih komponen yang terhubung dan berinteraksi untuk mencapai suatu tujuan (Romney & Steinbart, 2015). Di sisi lain, O'Brien dan Marakas (2008) menyatakan bahwa sistem berarti seperangkat komponen yang saling berhubungan dan memiliki batas-batas tertentu yang jelas. Dikatakan juga bahwa sistem dapat bekerja sama untuk mencapai tujuan dengan menerima *input* dan menghasilkan *output* dalam proses yang terorganisir.

Pengertian informasi menurut Kelly (2010) adalah data yang telah diolah menjadi berguna bagi penggunanya baik untuk sekarang atau di masa yang akan

datang. Sedangkan, menurut Carlos Coronel dan Stephen Morris (2016) informasi adalah hasil dari data mentah yang diolah untuk menghasilkan hasil.

Menurut Romney dan Steinbart (2015), pengertian Sistem Informasi Akuntansi adalah seperangkat sistem mulai dari pengumpulan data, pencatatan, penyimpanan, dan pemrosesan data hingga menjadi informasi yang bermanfaat bagi para pengguna membuat keputusan.

Dari beberapa pengertian para ahli di atas, dapat ditarik kesimpulan bahwa Sistem Informasi Akuntansi merupakan Sistem informasi akuntansi adalah kumpulan data yang saling berhubungan satu sama lain secara harmonis untuk memproses data transaksi yang berkaitan dengan masalah dalam informasi keuangan.

2.2.2 Manfaat Sistem Informasi Akuntansi

Romney dan Steinbart (2015) dalam bukunya berpendapat bahwa Sistem Informasi Akuntansi yang didesain dengan baik, dapat menambah nilai manfaat, seperti :

1. meningkatkan kualitas sekaligus mengurangi biaya produk atau jasa,
2. meningkatkan efisiensi,
3. berbagi pengetahuan,
4. meningkatkan efisiensi dan efektivitas rantai pasokannya,
5. meningkatkan struktur pengendalian internal,
6. meningkatkan pengambilan keputusan.