

BAB II

LANDASAN TEORI

2.1. Teknologi *Blockchain*

Blockchain merupakan *data base* (basis data) yang terdistribusi dan dibagikan di setiap *node* (sistem) yang terhubung di dalam jaringan komputer. *Blockchain* sebagai *data base*, menyimpan informasi secara elektronik dalam format digital. *Blockchain* ini di kenal banyak orang karena kegunaan mereka dalam sistem *cryptocurrency*, seperti Bitcoin, yang digunakan untuk menjaga catatan transaksi yang aman dan terdesentralisasi. Inovasi yang sebenarnya ada di dalam *blockchain* adalah menjamin keterpercayaan dan keamanan catatan data, tanpa perlu adanya pihak ketiga untuk memverifikasi data tersebut.

Perbedaan utama antara *data base* biasa dan *blockchain* berada pada struktur data tersebut. *Blockchain* mengumpulkan informasi bersama dalam kelompok, yang dikenal sebagai *block*, lalu *block* menyimpan kumpulan informasi tersebut kedalamnya. *Block* memiliki kapasitas penyimpanan tertentu, dan ketika informasi diisi kedalam *block*, *block* akan menyimpan,

lalu menutup kemudian menautkannya ke *block* yang diisi sebelumnya, hal ini akhirnya membentuk rantai data yang kita kenal sebagai *blockchain*.

Sedangkan di dalam *data base* biasa, data disusun kedalam bentuk tabel, sedangkan *blockchain*, menyusun datanya ke dalam potongan-potongan (*block*), lalu dikaitkan satu sama lain. Struktur data pada *blockchain* ini secara terstruktur membuat garis waktu data yang tidak dapat diubah ketika diimplementasikan pada sistem yang terdesentralisasi

2.2. Gambaran Umum Sistem *Blockchain*

2.2.1. Perkembangan *Blockchain*

Perkembangan teknologi *blockchain* mengalami perkembangan yang sangat cepat, seperti yang kita lihat saat ini begitu banyak perusahaan besar di dunia berlomba-lomba untuk mengimplementasikan teknologi ini ke kehidupan kita sehari-hari. Hal ini dapat kita lihat pada perusahaan Facebook dengan produknya Bernama Metaverse.

Tahap perkembangan *blockchain* terbagi atas tiga tahapan (Swan, 2015), namun pada tahun 2017 awal, Bashir, pada bukunya yang berjudul *Mastering Blockchain* menambahkan satu lagi tahapan perkembangan Blockchain untuk menyempurnakan penelitian dari peneliti sebelumnya. Berikut tahapan perkembangan *blockchain*:

1) *Blockchain* 1.0

Blockchain generasi pertama diperkenalkan pertama kali bersamaan dengan penggunaan *cryptocurrency*. Pada tahapan ini

blockchain digunakan sebagai inti dari aplikasi dalam hal transaksi atau mata uang.

2) *Blockchain 2.0*

Pada generasi kedua ini *blockchain* masih digunakan dalam sektor finansial, pembedanya dari generasi pertama yaitu, diperkenalkannya *smart contract* ke dalam ekosistem *blockchain*. *Smart contract* dianggap dapat menangani berbagai macam produk keuangan seperti surat utang dan lain sebagainya.

3) *Blockchain 3.0*

Blockchain generasi ketiga ini tidak terbatas lagi pada sektor finansial, *blockchain* dapat diimplementasikan pada sektor-sektor lain selain jasa keuangan, seperti pemerintahan, dokumen kepemilikan, kesehatan, peradilan, lelang dan lain-lain.

4) *Blockchain X.0*

Blockchain generasi X merupakan tahapan terakhir dari *blockchain*. Di mana suatu hari nanti kita akan memiliki layanan *blockchain* publik yang tersedia dan dapat digunakan siapa saja seperti halnya mesin pencari Google. Generasi ini telah menggunakan *artificial intelligence* (kecerdasan buatan) dan telah di terapkan pada seluruh sektor kehidupan masyarakat.

2.2.2. Perbedaan *Blockchain* dengan *Cryptocurrency*

Blockchain dan *cryptocurrency* pada dasarnya adalah dua hal yang berbeda, berikut beberapa penjelasan mengenai *blockchain* dan *cryptocurrency* ini:

Table 1 Perbedaan Blockchain dan dan Cryptocurrency

Perbedaan	<i>Blockchain</i>	<i>Cryptocurrency</i>
Pengertian	<i>Blockchain</i> adalah teknologi basis data yang menyimpan segala informasi pertukaran data, seperti mata uang digital, pengarsipan, hingga sertifikat kepemilikan (tanah, nft dan sebagainya)	<i>Cryptocurrency</i> adalah sejenis mata uang yang digunakan didalam ekosistem <i>blockchain</i> , sehingga dapat disimpulkan bahwa <i>cryptocurrency</i> merupakan salah satu implementasi dari <i>blockchain</i> .
Tujuan	Mengurangi biaya yang dikeluarkan oleh organisasi dengan mengurangi kehadiran perantara. Hal ini menciptakan efisiensi	<i>Cryptocurrency</i> menyederhanakan dan meningkatkan kecepatan transaksi keuangan tanpa ada batasan dari pihak tertentu.

	dalam pemrosesan transaksi dan juga mengurangi tugas manual seperti pengumpulan dan pengeditan data, serta menyederhanakan proses audit dan pelaporan.	
Perkembangan	Perkembangan dari <i>blockchain</i> sangat luas hampir semua sektor dapat menggunakan teknologi ini.	<i>Cryptocurrency</i> terbatas pada transaksi mata uang digital saja

Pada penjelasan perbedaan pada tabel (2), dapat diambil kesimpulan bahwa *cryptocurrency* seperti Bitcoin, merupakan salah satu contoh hasil implementasi dari teknologi *blockchain*, dan dapat dikatakan bahwa *blockchain* bisa saja digunakan tanpa menggunakan *cryptocurrency*. Sedangkan, *cryptocurrency* tidak akan dapat digunakan tanpa adanya teknologi *blockchain*.

2.2.3. Jenis-Jenis *Blockchain*

Berdasarkan perkembangan *blockchain* pada tahun terakhir, *blockchain* dapat dibagi menjadi beberapa tipe dengan karakteristik yang berbeda, yaitu:

1) *Public Blockchain*

Blockchain ini merupakan jaringan terdistribusi secara umum karena sifatnya yang bersifat publik, artinya terbuka untuk semua orang yang berpartisipasi di dalamnya dan bersifat *open source* sehingga komunitas dapat mendistribusikannya. Tujuan dari *blockchain* jenis ini banyak digunakan untuk melakukan transaksi dalam *cryptocurrency*, di mana siapa pun dapat melihat daftar transaksi yang telah dilakukan dan memvalidasi transaksi tersebut.

2) *Private Blockchain*

Private blockchain merupakan jenis *blockchain* yang bersifat tertutup dan biasanya hanya digunakan untuk pertukaran informasi internal saja. Hal ini dapat mencegah pihak yang tidak berkepentingan untuk melihat apa yang sedang dilakukan di dalam *blockchain*. Menurut Mukhopadhyay (2018), ada pembatasan akses atau izin khusus untuk *private blockchain*. Biasanya perusahaan atau organisasi menggunakan jenis *blockchain* ini untuk menghindari kontrol akses yang terlalu luas seperti yang disediakan *public blockchain*, sehingga *private blockchain* menjadi solusinya.

3) *Semi-Private Blockchain*

Semi-Private Blockchain, umumnya dikenal sebagai *consortium blockchain*, jenis *blockchain* ini memberikan akses kepada siapa saja yang memiliki hak untuk menggunakannya dan memiliki *source code* yang tertutup. Jenis ini hampir sama dengan *private blockchain*. Namun, untuk penyimpanan data yang dikirim melalui transaksi, akan selalu disimpan di jaringan *public blockchain*.

2.2.4. Struktur Pembangun Sistem *Blockchain*

Menurut Laurance (2017), struktur pembangun dari sistem *blockchain* terdiri dari 3 bagian utama yaitu:

1) *Block (Block)*

Blockchain terdiri dari banyak *block* yang mewakili daftar transaksi yang valid dan tersimpan. Setiap *block* memiliki *hash* kriptografi *sebagai* penunjuk atau identitas setiap *block*, sehingga *block* dapat terhubung satu sama lain. Menurut Antonopoulos et al., (2017), struktur *block* terdiri dari *header*, diikuti oleh metadata dan daftar transaksi yang disimpan. Di bawah ini adalah penjelasan dari komponen yang ada di setiap *block* jaringan *blockchain*:

- a. *Block Size* adalah bagian pertama dari struktur *block* yang menyimpan informasi mengenai ukuran *block* dalam *byte*.
- b. *Block Header* adalah bagian dari *block* yang berukuran 80 *bytes* dan menyimpan gabungan metadata, seperti:

- *Version*: Menyimpan informasi versi untuk satu *block* dan berukuran 4 *bytes*.
 - *Previous Block Hash*: Metadata yang menyimpan *hash* dari *block* sebelumnya juga bertindak sebagai "rantai" yang menghubungkan *block* ke *block* sebelumnya dan berukuran 32 *bytes*.
 - *Merkle Root*: Merupakan kompilasi informasi dari semua transaksi yang di-*hash* pada *block* dengan ukuran 32 *bytes* dan tujuannya adalah untuk memberikan kesimpulan tentang semua transaksi yang dilakukan oleh *block*.
 - *Timestamp*: Menyimpan informasi mengenai *timestamp* atau kapan *block* tersebut dibuat dan memiliki ukuran sebesar 4 *bytes*.
 - *Difficulty Target*: Menyimpan informasi tentang kesulitan algoritma PoW (Proof of Work) yang digunakan dan berukuran sebesar 4 *bytes*.
 - *Nonce*: Merupakan nomor acak yang disimpan dengan ukuran 4 *bytes* dan digunakan saat menambang *block* baru.
- c. *Record* adalah bagian dari *block* yang menghitung berapa banyak transaksi yang telah dilakukan dan biasanya berukuran 1-9 *bytes*.
- d. Daftar Transaksi Merupakan bagian yang menyimpan sekumpulan data dari transaksi yang dilakukan di *block* dengan ukuran data yang berbeda-beda.

2) Rantai (*Chain*)

Supaya setiap *block* pada *blockchain* saling terhubung, diperlukanlah “rantai” dalam bentuk *hash* yang menghubungkan antara satu *block* dengan *block* lainnya. Mekanisme *hash* adalah salah satu konsep matematis kompleks yang diterapkan ke *blockchain*. Meskipun *blockchain* dianggap sebagai inovasi teknologi terbaru. Tapi tidak dengan *hash*. Konsep *hash* sudah ada selama kurang lebih 30 tahun dan digunakan dalam konsep *blockchain*, karena *hash* hanya dapat membuat fungsi satu arah yang tidak dapat di *crack* (di deskripsi). Fungsi *hash* menciptakan algoritme matematika yang memetakan data dari semua ukuran ke dalam bit karakter, biasanya memiliki panjang sekitar 32 karakter, di mana panjang ukuran bit mewakili data yang sedang diproses atau di-*hash*. *Secure Hash Algorithm* (SHA) adalah salah satu fungsi *hash* yang digunakan pada *blockchain*, sedangkan algoritma yang umum digunakan untuk *hashing blockchain* menggunakan algoritma SHA256, yang mengubah panjang data dari berbagai ukuran menjadi karakter *hash* 256-bit. (32 bytes), jadi dalam *hash blockchain* dapat dianggap sebagai sidik jari data yang unik dalam satu *block* untuk mengunci *block* agar tetap berurutan di *Blockchain*.

3) Jaringan (*Network*)

Istilah jaringan atau *network* dalam *blockchain* merupakan representasi dari jumlah *node* atau komputer yang saling terhubung

dan menjalankan suatu algoritma untuk mengamankan jaringan tersebut. Setiap *node* memiliki catatan semua transaksi yang tercatat di *Blockchain*. *Node* ini berlokasi di seluruh dunia dan dikelola oleh semua orang yang merupakan bagian dari jaringan *blockchain*. Hal ini sangat jelas terkait dengan topologi jaringan yang digunakan *blockchain* yaitu *Peer-to-Peer*, dimana semua *node* dapat berkomunikasi antara satu *node* dengan *node* lainnya untuk menerima dan mengirim pesan.

2.2.5. Partisipan Pada Sistem *Blockchain* Beserta Perannya

Gupta (2018), pada bukunya yang berjudul *Blockchain for Dummies* menyatakan bahwa ada tujuh partisipan yang diwajibkan ada untuk mengoperasikan sistem *blockchain*. Partisipan tersebut yaitu sebagai berikut:

1) *Blockchain User*

Merupakan partisipan yang memiliki akses atau izin untuk bergabung dan melakukan aktivitas di dalam jaringan *blockchain*.

2) *Regulator*

Merupakan *Blockchain user* yang memiliki izin khusus untuk mengelola *blockchain user* biasa, tugasnya seperti memberikan/melarang izin tertentu dalam aktivitas jaringan *blockchain*.

3) *Blockchain Developer*

Merupakan programmer yang membuat aplikasi yang memuat jaringan *blockchain*. Partisipan ini dapat juga disebut sebagai perantara antara *blockchain user* dengan aplikasi.

4) *Blockchain Network Operator*

Merupakan seorang yang dipercaya untuk mengatur dan memonitor jaringan *blockchain*.

5) *Traditional Processing Platforms*

Merupakan sistem komputer digunakan oleh *blockchain* untuk meningkatkan pemrosesan. Sistem ini juga memerlukan izin untuk masuk kedalam jaringan *blockchain*.

6) *Traditional Data Sources*

Merupakan sistem data yang menyediakan data untuk memproses *smart contract* dan membantu menentukan bagaimana komunikasi dan transfer data akan terjadi antara aplikasi/data tradisional dan *blockchain*.

7) *Certificate Authority*

Merupakan partisipan yang menerbitkan dan mengelola berbagai jenis sertifikat yang diperlukan untuk menjalankan *blockchain* yang membutuhkan izin untuk mengoperasikannya.

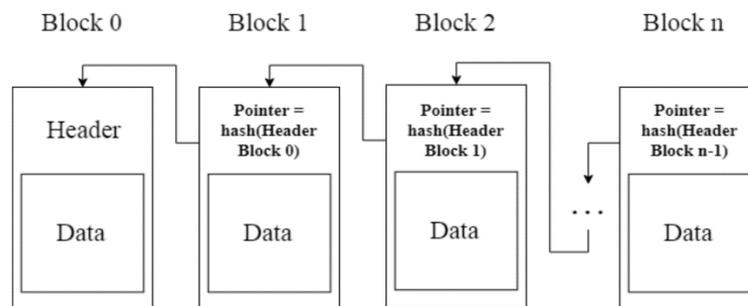
2.2.6. Cara Kerja Sistem *Blockchain*

Setiap *block* pada *blockchain* berisi beberapa data atau informasi. Data yang disimpan di dalam *block* bergantung pada jenis *blockchain* yang digunakan. Pada *blockchain* Bitcoin misalnya menyimpan detail tentang transaksi, seperti pengirim, penerima, dan jumlah koin.

Sebuah *block* juga memiliki *hash*, *hash* disini memiliki kegunaan yang hampir sama dengan sidik jari. *Hash* mengidentifikasi *block* dan semua isinya dan itu selalu unik, seperti sidik jari. Ketika *block* ditambahkan jaringan, maka *hash* nya akan langsung dihitung/dibuat. Mengubah sesuatu di dalam *block* akan menyebabkan *hash* berubah. Jadi dengan kata lain *hash* sangat berguna ketika Anda ingin mendeteksi perubahan pada *block*. Jika sidik jari suatu *block* berubah, maka *block* tersebut tidak lagi sama.

Elemen berikutnya pada *block* adalah *hash* dari *block* sebelumnya. Ini akan secara langsung membuat rantai dari *block* dan mekanisme inilah yang membuat *blockchain* aman. Sebagai contoh pada gambar (1), disini kita memiliki rantai 3 *block*. Seperti kita tau, setiap *block* memiliki *hash* dan *hash* dari *block* sebelumnya. Jadi *block* nomor 3 merujuk pada *block* nomor 2 dan *block* nomor 2 merujuk ke *block* nomor 1.

Gambar 1 Skema *hash* pada Blockchain



Block pertama pada *blockchain* memiliki keunikan, dikarenakan tidak bisa merujuk *hash* ke *block* sebelumnya. *Block* ini disebut dengan

block genesis. Jika kita mengutak-atik *block* kedua, ini akan menyebabkan *hash block* juga berubah. Hal ini secara beruntun akan membuat *block* 3 dan semua *block* selanjutnya tidak valid, karena mereka tidak lagi menyimpan *hash* yang valid dari *block* sebelumnya. Jadi mengubah satu *block* akan membuat semua *block* berikutnya tidak valid. Tetapi menggunakan *hash* belumlah cukup untuk mencegah gangguan atau peretasan. Komputer pada masa sekarang sangat cepat dan dapat menghitung ratusan ribu *hash* per detik.

Penggunaan computer canggih dapat secara langsung mengutak-atik *block* dan menghitung ulang semua *hash* dari *block* dan membuat sistem *blockchain* valid lagi. Jadi untuk mengatasi ini, *blockchain* memiliki sesuatu yang dikenal dengan *proof-of-work*. *Proof-of-work* adalah mekanisme yang memperlambat pembuatan *block* baru. Sebagai contoh pada Bitcoin, dibutuhkan sekitar 10 menit untuk menghitung *proof-of-work* yang diperlukan dan menambahkan *block* baru ke dalam *blockchain*. Mekanisme ini membuat proses peretasan sangat sulit untuk dilakukan, karena jika kita mengutak-atik 1 *block*, maka kita harus menghitung ulang *proof-of-work* untuk seluruh *block*.

Selain menggunakan mekanisme *proof-of-work* dan *hash*, ada satu cara lagi untuk mengamankan sistem *blockchain* yaitu dengan cara mendistribusikan seluruh data pada komputer yang terhubung. Mekanisme ini disebut dengan jaringan *peer-to-peer* dan siapa pun yang diberikan izin dapat bergabung. Ketika seseorang bergabung dengan

jaringan tersebut, ia mendapatkan salinan lengkap dari *blockchain*. *Node* menggunakan ini untuk memverifikasi bahwa semuanya masih valid. Sebagai contoh ketika seseorang membuat *block* baru, *block* tersebut akan dikirim ke semua orang di jaringan dan setiap *node* kemudian memverifikasi *block* itu untuk memastikan bahwa itu tidak dirusak atau masih valid. Semua *node* dalam jaringan ini memiliki konsensus. Mereka dapat setuju atau tidak tentang *block* mana yang valid dan mana yang tidak.

Jadi untuk berhasil meretas sistem *blockchain*, maka kita harus mengutak-atik semua *block* di rantai, mengulang bukti kerja/*hash* untuk setiap *block* dan mengendalikan lebih dari 50% jaringan *peer-to-peer*. Dengan hal tersebut dapat kita simpulkan bahwa sistem keamanan *blockchain* ini sangat ketat dan hampir mustahil untuk diretas.

2.3. Gambaran Umum Sertifikat Tanah Digital

Sertipikat tanah digital merupakan sebuah inovasi yang dikeluarkan oleh Kementerian Agraria dan Tata Ruang mengenai pengamanan kepemilikan tanah. Hal tersebut diatur dalam Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Republik Indonesia Nomor 1 Tahun 2021 tentang sertipikat elektronik. Penggunaan sertipikat ini dimaksudkan untuk mewujudkan modernisasi pelayanan pertanahan guna meningkatkan indikator kemudahan berusaha dan pelayanan publik kepada masyarakat, perlu mengoptimalkan pemanfaatan teknologi informasi dan komunikasi dengan menerapkan pelayanan pertanahan berbasis elektronik.

Berikut perbedaan sertipikat tanah elektronik dengan sertipikat tanah konvensional:

- 1) Sertipikat elektronik berbentuk dokumen elektronik yang berisi informasi mengenai tanah. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
- 2) Sertipikat elektronik menggunakan kode *hash* yang dihasilkan oleh sistem. Kode *hash* pada sertipikat tanah elektronik ini sendiri hampir sama penggunaannya dengan yang ada pada sistem blockchain.
- 3) Sertipikat tanah elektronik menggunakan tanda tangan digital yang dianggap dapat menjamin keamanan data. Tanda tangan digital sendiri memiliki pengertian yaitu tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
- 4) Sertipikat tanah elektronik memiliki pangkalan data/*data base*, yang digunakan sebagai media penyimpanan data-data tanah

2.4. Gambaran Umum Penatausahaan Barang Milik Negara

2.4.1. Penjelasan mengenai penatausahaan Barang Milik Negara

Penatausahaan Barang Milik Negara (BMN) merupakan rangkaian kegiatan yang meliputi pembukuan, inventarisasi dan pelaporan BMN yang diatur di dalam Peraturan Menteri Keuangan Republik Indonesia Nomor 181/PMK.06/2016 Tentang Penatausahaan Barang Milik Negara.

Ruang lingkup kegiatan penatausahaan BMN meliputi:

- 1) Pembukuan, yang terdiri atas kegiatan pendaftaran BMN ke dalam Daftar Barang.
- 2) Inventarisasi, yang terdiri atas kegiatan pendataan, pencatatan dan pelaporan hasil pendataan BMN.
- 3) Pelaporan, yang terdiri atas kegiatan penyusunan dan penyampaian data dan informasi BMN secara semesteran dan tahunan.

Objek Penatausahaan BMN meliputi:

- 1) Semua barang yang dibeli atau diperoleh atas beban Anggaran Pendapatan dan Belanja Negara.
- 2) Semua barang yang berasal dari perolehan lainnya yang sah, meliputi:
 - a. Barang yang diperoleh dari hibah/ sumbangan atau yang sejenisnya.
 - b. Barang yang diperoleh sebagai pelaksanaan perjanjian/kontrak.
 - c. Barang yang diperoleh sesuai dengan ketentuan Peraturan Perundang-undangan.
 - d. Barang yang diperoleh berdasarkan putusan pengadilan yang telah memperoleh kekuatan hukum tetap.

Pengklasifikasian objek penatausahaan BMN meliputi:

- 1) Aset lancar berupa barang persediaan.
- 2) Aset tetap, meliputi:
 - a. tanah.
 - b. peralatan dan mesin.
 - c. gedung dan bangunan.
 - d. jalan, irigasi, dan jaringan.
 - e. aset tetap lainnya.
 - f. konstruksi dalam pengerjaan.
- 3) Aset lainnya, meliputi:
 - a. Aset kemitraan dengan pihak ketiga.
 - b. Aset tak berwujud.
 - c. Aset tetap yang dihentikan dari penggunaan.

Pelaksana penatausahaan BMN meliputi:

- 1) Penatausahaan BMN pada Pengguna Barang dilakukan oleh Pelaksana Penatausahaan yang terdiri atas:
 - a. UAKPB
 - b. UAPPB-W
 - c. UAPPB-EI
 - d. UAPB
- 2) Penatausahaan BMN pada Pengelola Barang dilakukan oleh Pelaksana Penatausahaan yang terdiri atas:
 - a. KPKNL selaku Pengelola Barang kantor daerah

- b. Kanwil DJKN selaku Pengelola Barang kantor wilayah
- c. Kantor Pusat DJKN selaku Pengelola Barang