

BAB II

LANDASAN TEORI

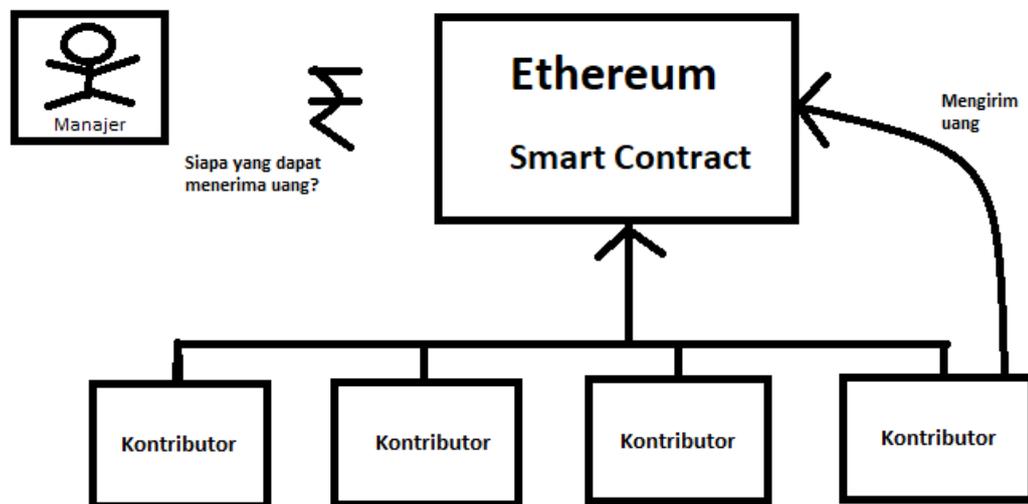
2.1 Blockchain

Sejarah awal *Bitcoin* (uang digital), yang ditemukan oleh seorang pria bernama Satoshi Nakamoto menjelang akhir tahun 2008, serta dalam makalah berjudul "*Bitcoin: A Peer-to-Peer Electronic Cash System.*" Temuan ini dikaitkan dengan Satoshi Nakamoto. Ia menuliskan pendapatnya tentang penerapan teknologi jaringan peer-to-peer dalam jurnal ini. *Peer-to-Peer*, umumnya dikenal sebagai P2P, adalah jaringan terdistribusi yang dapat berbagi file media dan juga bertukar data antara dua komputer (*peer*) atau jenis jaringan lain tanpa memerlukan perantara apa pun, sesuai dengan definisi yang diberikan oleh (Schollmeier, 2001). P2P adalah nama lain dari *peer-to-peer*. Penerapan konsep *Peer-to-Peer* tentunya dapat dikatakan tepat untuk memberikan solusi terkait metode transaksi menggunakan *Bitcoin* yang telah dibahas dalam makalah terkait konsep cara bertransaksi dengan uang digital (*Bitcoin*) online tanpa menggunakan pihak ketiga dan tanpa penyimpanan terpusat atau terdistribusi. Artikel ini mengkaji bagaimana mengelola transaksi elektronik yang terkait dengan pengertian pemanfaatan uang digital (*Bitcoin*) untuk melakukan transaksi online tanpa menggunakan pihak ketiga (Nakamoto, 2008).

Blockchain adalah semacam teknologi ledger terdistribusi dalam bentuk paling dasar di mana database transaksi saat ini disimpan dan dikelola di antara

beberapa *node* dalam jaringan *peer-to-peer*. Sebagai contoh, *blockchain* terpisah dari DLT pada umumnya dan memiliki kumpulan propertinya sendiri. Perbedaan ini dibuat karena *blockchain* sudah memiliki struktur database. Setiap bagian dari data transaksi akan ditambahkan ke rantai blok yang terhubung satu sama lain. Blok ini tidak dapat diubah karena hanya dapat ditambahkan. Untuk merekam setiap bagian dari data transaksi yang termasuk dalam *blockchain*, digunakan prosedur kriptografi dan konsensus seperti *Proof of Work*. Setelah itu, teknologi *blockchain* dikembangkan, dan mulai digunakan di sejumlah aplikasi, termasuk *Smart contract*. *Decentralized application* adalah aplikasi yang menggunakan teknologi *blockchain* dan menggabungkan *Smart contract*..

Gambar 2.1 Mekanisme Blockchain



Sumber : Penulis

Menurut definisi yang diberikan, *Blockchain* adalah database terdistribusi yang mencatat setiap transaksi atau pertukaran di setiap blok dan dilindungi oleh metode keamanan kriptografi, yang menjamin keamanan dan tidak dapat dengan mudah diubah nilainya (Angelis & Ribeiro da Silva, 2019). Namun ada juga yang

percaya bahwa teknologi *blockchain* dan mata uang digital seperti *Bitcoin* adalah hal yang sama. Karena alasan ini mengandung kekurangan, itu perlu diperbaiki. *Bitcoin* dan mata uang digital lainnya tidak dapat dibandingkan dengan *blockchain* dalam bentuknya yang paling dasar. Teknologi *Blockchain* berbeda dari mata uang digital pada tabel 2.1 berikut :

Tabel 2.1 Perbedaan *Blockchain* dan *Cryptocurrency*

	<i>Blockchain</i>	<i>Cryptocurrency</i>
1.	<i>Blockchain</i> adalah sejenis teknologi yang bekerja mirip dengan <i>ledger</i> atau database yang menyimpan semua data yang diperlukan untuk pertukaran data, dari uang digital hingga dokumentasi kepemilikan properti	<i>Cryptocurrency</i> adalah jenis mata uang digital yang juga menggunakan teknologi <i>Blockchain</i> . Ini karena proses transaksi tercatat di <i>Blockchain</i> .
2.	Tujuan teknologi <i>Blockchain</i> adalah untuk meminimalkan biaya yang terkait dengan pertukaran nilai sekaligus memungkinkan lingkungan yang aman untuk transaksi yang dapat dilakukan dengan siapa saja.	Tujuan <i>cryptocurrency</i> adalah untuk menghapus batasan apa pun yang dapat menghalangi atau memperumit transaksi keuangan sekaligus membuatnya lebih sederhana dan lebih cepat
3.	Topik percakapan <i>blockchain</i> mencakup berbagai topik dan akan terus berkembang	Pertukaran <i>cryptocurrency</i> hanya dapat dilakukan pada platform yang hanya berurusan dengan uang digital

Cryptocurrency adalah salah satu contoh hasil dari instalasi atau penyebaran teknologi *Blockchain*, dan mereka dapat beroperasi atau digunakan tanpa *cryptocurrency*. Diskusi singkat tentang perbedaan antara *Blockchain* dan *Cryptocurrency* mungkin mengarah pada kesimpulan ini. Dengan tidak adanya teknologi *Blockchain*, *cryptocurrency* akan menjadi usang.

Menurut kesimpulan penelitian yang dilakukan oleh Voshmgir Shermin, *Blockchain* dapat secara efektif, beragam, dan mencatat transaksi jangka panjang antara dua pihak. Namun terdapat sisi lain dari blockchain ini sendiri dimana system yang diterapkan cukup kompleks dan rumit sehingga apabila terjadi kerusakan dalam sistem tersebut membutuhkan proses yang rumit pula.

Jaringan *Blockchain* publik seperti Bitcoin dan *Ethereum* memungkinkan siapa saja untuk menyimpan dan mentransfer nilai dengan cara yang aman dan mandiri. Secara khusus, tidak diperlukan pembukuan pusat dan transaksi tidak dapat disensor atau dimodifikasi,. Transfer dasar masih terbatas pada aset protokol asli masing-masing *Blockchain* seperti BTC dalam kasus *Blockchain Bitcoin* dan ETH dalam kasus *Blockchain Ethereum*. Namun, ada cara untuk membuat representasi *on-chain* dari aset tambahan tersebut. Representasi seperti itu biasanya disebut sebagai token (*Blockchain*).

Menurut Abdulaziz Aborujilah, *Blockchain* memiliki pengaruh yang signifikan terhadap penyediaan peluang bisnis dan peluang terpenuhinya prinsip Good Governance seperti transparansi dan efisiensi dalam Administrasi pemerintahan. Dalam penelitian yang dilakukan Abdul, *Blockchain* memberikan keuntungan dalam manajemen pendaftaran tanah. Sebagai contoh, status kepemilikan dapat ditentukan dengan mudah. Departemen pencatatan tanah, departemen pendaftaran, dan entitas bank dapat terhubung melalui *blockchain* yang terpisah. Pengalihan kepemilikan membutuhkan waktu yang lebih singkat dan catatan atas tanah dapat dikelola dengan cara yang dapat dipercaya dengan upaya pemeliharaan yang lebih sedikit. Selain itu, teknologi *Blockchain* menawarkan

solusi yang dapat diterapkan untuk memigrasikan transaksi sistem informasi ke node *Blockchain* (Aborujilah et al., 2021).

2.1.1 Jenis-Jenis *Blockchain*

Berdasarkan jenis *Blockchain* terdapat tiga jenis yang umum diketahui beserta perbedaan dan tujuannya, yaitu:

1. *Public Blockchain*

Blockchain ini merupakan termasuk jaringan terdistribusi dalam skala besar karena memiliki sifat publik, memiliki makna terbuka kepada setiap orang yang berpartisipasi dan memiliki kode *open source*, sehingga para komunitas dapat melakukan kegiatan distribusi. Adapun tujuan dari jenis *blockchain* ini banyak digunakan untuk kegiatan transaksi mata uang digital atau *cryptocurrency*, di mana semua orang dapat melihat daftar transaksi yang pernah dilakukan dan memvalidasi transaksi.

2. *Private Blockchain*

Private Blockchain adalah implementasi *Blockchain* yang tidak dapat diakses oleh masyarakat umum dan hanya dimaksudkan untuk memungkinkan pertukaran data di antara para pesertanya. Secara alami, ini berarti bahwa mereka yang tidak berpartisipasi dalam *Blockchain* tidak dapat mengamati operasi yang terjadi di dalamnya. Izin dan kontrol akses ada di *blockchain* pribadi. Jika ada bisnis atau organisasi yang memanfaatkan teknologi *blockchain* pada umumnya. Jika, di sisi lain, seseorang merasa tidak nyaman dengan tingkat kontrol akses yang

disediakan oleh jaringan publik (*Blockchain publik*), *blockchain* pribadi dapat digunakan untuk mencapai tujuan yang sama.

3. *Semi-Private Blockchain*

Semi-private Blockchain atau sering disebut sebagai *consortium Blockchain*, merupakan jenis *Blockchain* yang menyembunyikan kode sumbernya dari publik tetapi memberikan akses kepada siapa saja yang telah diberi izin untuk menggunakannya. dengan cara yang sama seperti *blockchain* pribadi, data yang dikirim melalui *Blockchain* melalui transaksi akan tetap berada di jaringan *Blockchain* publik..

2.2 *Cryptocurrency*

Istilah "*cryptocurrency*" berasal dari bahasa Inggris dan terdiri dari dua kata: kriptografi (yang mengacu pada cara untuk memastikan kerahasiaan komunikasi) dan mata uang (*currency*). *Cryptocurrency* dapat didefinisikan sebagai media perdagangan dalam bentuk uang digital yang menggunakan prinsip-prinsip kriptografi. Hal ini dilakukan agar legitimasi dan keamanan uang digital yang diproduksi dan ditransaksikan dapat diverifikasi.

Cryptocurrency adalah mata uang digital *decentralized* yang memverifikasi dan mengenkripsi transaksi keuangan yang dilakukan melalui jaringan menggunakan prinsip kriptografi dan ilmu keamanan komunikasi. *Cryptocurrency*, sering dikenal sebagai uang digital adalah jenis aset digital yang dirancang untuk digunakan sebagai media perdagangan atau transaksi. *Cryptocurrency* khusus ini sudah mendapatkan popularitas di antara banyak orang di seluruh dunia, terutama di antara mereka yang tertarik menggunakan internet untuk menambah penghasilan

mereka. Uang digital ini tersedia dalam berbagai format, termasuk *Bitcoin*, *Dogecoin*, *Ethereum*, dan banyak mata uang kripto lainnya senilai ratusan dolar. Mata uang alternatif atau mata uang digital, adalah bagian dari kategori mata uang kripto yang lebih luas. *Bitcoin* adalah *cryptocurrency* pertama yang tidak dikendalikan oleh badan pusat ketika diluncurkan pada tahun 2009. Beberapa *cryptocurrency* baru telah diperkenalkan sejak saat itu. Dari sekitar 18.465 *cryptocurrency* yang telah dikembangkan pada tahun 2022, ada sekitar 10.363 *cryptocurrency* yang masih aktif diperdagangkan di pasar internet.

2.2.1 Nilai *Cryptocurrency*

Fondasi inti *cryptocurrency* adalah desentralisasi. Setiap orang dapat menghasilkan uang mereka sendiri sebagai hasil dari kualitas ini. Hal ini sangat kontras dengan sifat terpusat dari uang yang telah dipegang dan belanjakan, di mana pembuatan uang segar terbatas pada satu lembaga keuangan dan hanya dapat dilakukan oleh lembaga itu. Nilai *cryptocurrency* tidak dapat dikurangi oleh kekuatan inflasi karena mereka tidak dikendalikan oleh badan pusat mana pun.

2.2.2 Risiko *Cryptocurrency*

Terlepas dari semua keuntungan dan daya tarik *cryptocurrency*, pada akhirnya tetap harus berhati-hati saat berurusan dengan atau berinvestasi dalam *cryptocurrency* atau mata uang digital karena ada sejumlah kemungkinan bahaya. Salah satunya adalah bahwa ayunan *cryptocurrency* ini sangat tidak dapat diprediksi karena tidak diatur oleh otoritas mana pun. Ini karena tidak ada otoritas terpusat yang menanganinya. Kolektor, permintaan, dan penawaran, serta biaya

pembelian dan penjualan logam mulia, adalah satu-satunya faktor yang mempengaruhi nilainya. Nilainya semata-mata ditentukan oleh aspek tersebut.

Ada berbagai aspek yang perlu dipertimbangkan sebelum berinvestasi dalam *cryptocurrency*, termasuk yang berikut:

1. Durabilitas/daya tahan, beberapa ahli bisnis berpendapat bahwa *cryptocurrency* adalah suatu bentuk investasi yang sewaktu-waktu bisa terbongkar dan meledak atau dalam kata lain sebuah bentuk tipuan yang dapat mengakibatkan para Investor kehilangan seluruh aset dananya tanpa adanya balik modal ataupun ganti rugi.
2. Volatilitas yang lumayan besar, seperti ketika kita berinvestasi dengan *cryptocurrency* terdapat kemungkinan kita menghasilkan banyak uang, tetapi bisa juga kehilangan banyak uang dalam sekejap.
3. Aspek hukum, Saat ini belum ada undang-undang yang pasti terkait penggunaan *cryptocurrency* sebagai alat transaksi ini. Dan hal ini juga terjadi di beberapa negara yang tidak mengakui mata uang digital sebagai mata uang yang sah. Negara seperti China dan Korea Selatan melarang ICO (*Initial Coin Offering*). Negara Rusia melarang penuh penggunaan mata uang digital dikarenakan presiden Rusia menganggap bahwa mata uang digital bisa menimbulkan dampak negatif seperti pembiayaan terorisme.
4. Resiko Kehilangan. Terdapat kemungkinan hilangnya data dan akun dari pengguna *cryptocurrency* jika kata sandi maupun *privacy key* dari pengguna hilang atau diretas orang lain.

2.3 Teori Smart Contract

Ilmuwan komputer Nick Szabo merancang *Smart contract* dalam serangkaian makalah pada pertengahan 1990-an. Dia menggambarkan smart contract sebagai seperangkat janji yang ditentukan dalam bentuk digitalisasi, termasuk protokol di mana para pihak memenuhi janji-janji ini. *Smart contract* berusaha menangkap elemen kontrak yang bersifat algoritmik dan melindungi perjanjian dari gangguan melalui metode kriptografi. Banyak elemen operasional kontrak pada dasarnya mewakili klausa “jika-maka” bersyarat seperti pernyataan yang diposisikan untuk ekspresi dalam pemrograman bahasa komputer.

Beberapa pengamat memproyeksikan penggunaan *smart contract* dalam perjanjian berbasis kode yang lebih umum. Contohnya, definisi *smart contract* yang dikutip dari (Zheng et al., 2021) adalah memajukan konsepsi teknologi yang fleksibel. *Smart contract* adalah sebuah aplikasi dari *Blockchain* di mana sistem pelaksanaannya ditegakkan oleh sebuah protokol konsensus. *Smart contract* menggunakan teknik *proof of work* atau juga disebut bukti kerja, yang membuat proses transaksi dalam sistem ini lebih aman dan sulit untuk diretas atau dirusan oleh beberapa node dalam *blockchain* (Aborujilah et al., 2021).

Smart contract juga dijelaskan sebagai seperangkat aturan untuk memfasilitasi transfer mata uang atau aset digital antar pihak dalam kondisi tertentu secara digital. *Smart contract* adalah program komputer aman yang memiliki verifikasi diri, eksekusi mandiri, dan sifat tahan akan kerusakan. *Smart contract* digunakan untuk pertukaran nilai tanpa perlu pihak ketiga. *Smart contract* membantu kita menukar uang, properti, saham, atau apa pun yang berharga secara transparan, dan

menghindari layanan perantara. *Smart contract* berjalan di Mesin Virtual Ethereum (EVM) (Zheng et al., 2021).

2.4 Teori dan konsep umum *Non Fungible Token* (NFT)

Non-fungible token, juga dikenal sebagai NFT, adalah aset digital yang disimpan di *blockchain* yang dibedakan dari token lain dengan kode identifikasi dan kumpulan data (Ante, 2021). Token ini disebut sebagai *non-fungible* karena tidak memiliki kesepadanan yang merupakan karakteristik aset kripto secara umum. Kata "sepadan" mengacu pada fakta bahwa nilai aset kripto dapat diperdagangkan untuk item lain dengan unit yang setara dengan aset kripto. Orang B, misalnya, bisa meminjam Rp. 500.000 dalam bentuk lima Rp. 100.000 wesel dari orang A. Orang B dapat melunasi kewajiban di masa depan dengan membayar pinjaman dengan sepuluh lembar uang masing-masing Rp 50.000, bukan lima lembar senilai Rp 100.000. Akibatnya, menggunakan pendekatan Fungible untuk berdagang atau menukar NFT tidak dimungkinkan. *non-fungible token* (NFT) tidak dapat ditukar dengan apapun karena masing-masing unik dan tidak memiliki desain yang sama, sehingga tidak cocok untuk digunakan sebagai mekanisme pembayaran atau dalam transaksi komersial (Nurhadi, 2021).

2.4.1 Fungsi dan Manfaat NFT

Beberapa kegunaan dari *Non Fungible Token* (Nurhadi, 2021), antara lain :

- Dalam industri Seni, fungsi utama NFT adalah menyediakan keamanan bagi seniman atas karya yang dipublikasikan secara daring. Hal ini mencegah konten dapat tersebar secara bebas dan diklaim dengan mudah yang dapat menimbulkan kerugian bagi Seniman tersebut.

- Dalam bidang bisnis, segala bentuk transaksi bisnis menggunakan NFT ini seperti property, aset, lisensi, dan lain-lain akan tercatat dalam *blockchain* sehingga dapat meminimalisir adanya kehilangan, penipuan, maupun pencurian aset.
- Manfaat utama dari NFT ini adalah untuk mempermudah seniman mempromosikan dan menjual karya – karya digitalnya.

2.4.2 Risiko NFT

Selain beberapa manfaat yang ditawarkan, NFT juga memiliki kekurangan dan risiko. Risiko tersebut cenderung sama ketika kita bertransaksi menggunakan mata uang digital yaitu risiko kehilangan karya. Ketika terjadi peretasan akun, maka ada kemungkinan akan kehilangan segala akses termasuk akses *wallet* NFT (Nurhadi, 2021).

2.5 Teori dan konsep Ethereum

Vitalik Buterin pertama kali memperkenalkan *Ethereum* pada akhir tahun 2013. *Ethereum* ini memiliki tujuan untuk membangun aplikasi yang terdesentralisasi (Zheng et al., 2021). Pengembangan formal proyek perangkat lunak *ethereum* dimulai pada awal 2014 melalui Perusahaan Swiss. *Ethereum* adalah *blockchain* yang dapat diprogram yang bekerja menggunakan *Eth* sebagai *cryptocurrency* dasar untuk menggunakan sistem. *Ether* digunakan sebagai pembayaran biaya untuk informasi yang disimpan atau diproses. *Ethereum* digunakan sebagai basis untuk banyak aplikasi *blockchain*. *Ethereum* menawarkan penggunanya lingkungan yang komprehensif untuk membuat fungsionalitas mereka sendiri dengan bantuan aplikasi terdesentralisasi yang disebut sebagai *Decentralized application (Dapps)*.

Ethereum dibuat berdasarkan inovasi dari *Bitcoin*. Meskipun demikian terdapat perbedaan yang cukup signifikan diantara keduanya. Jika *Bitcoin* hanya sekedar mata uang digital biasa, *Ethereum* juga memiliki fungsi serupa dengan *Bitcoin* tetapi *Ethereum* memiliki platform atau *blockchain* tersendiri. Kemampuan program *Ethereum* memungkinkannya untuk digunakan sebagai platform untuk berbagai aset digital. ERC adalah singkatan dari *Ethereum Request for Comment* dan merupakan istilah yang diberikan untuk token yang dapat digunakan di *Ethereum*. Setiap token memiliki berbagai kegunaan dan hanya dapat digunakan dalam situasi tertentu, termasuk :

- **ERC-1155**

Token dapat digunakan untuk membuat token yang sepadan, yang memberikan nilai moneter di beberapa platform. Token dapat digunakan untuk membuat token ini. Protokol ERC-1155 lebih baik daripada protokol ERC-20 dan ERC-721.

- **ERC-20**

Token dapat dipertukarkan, atau dapat dipertukarkan, yang berarti semuanya sama dan dapat ditukar satu sama lain dengan mudah.

- **ERC-223**

Protokol ERC-223 adalah perpanjangan dari protokol ERC-20, yang dibuat untuk mengatasi beberapa kekurangan standar ERC-20.

- **ERC-721**

Non-fungible token (NFT) adalah token yang tidak dapat ditukar dengan token lain karena karakteristik unik yang membedakannya dari token yang sebanding.

- **ERC-777**

Token ini, seperti ERC-20, mempermudah partisipasi dalam operasi perdagangan yang canggih dan membantu menghilangkan kebingungan seputar desimal, pencetakan, dan pembakaran. ERC-777 menggunakan pengait (*hook*), yang merupakan fitur yang berguna dan menarik.

- **ERC-827**

Token ERC-20 ini memungkinkan pengguna *Ethereum* untuk mengirimkan uang tunai dan data, serta memungkinkan token disetujui untuk dibelanjakan oleh bisnis pihak ketiga yang berjalan di *blockchain* yang sama.

- **ERC-884**

Masing-masing token ini mewakili bagian yang berbeda di perusahaan Delaware, sesuai dengan persyaratan David Sag. Perusahaan ini dirancang untuk transaksi ekuitas, dan pemegang token harus masuk daftar putih menggunakan fitur *Smart contract*.

- **ERC-948**

Ini adalah protokol token *Ethereum* baru yang memungkinkan transaksi berbasis langganan dan dirancang untuk menghubungkan bisnis langganan dengan pelanggan.

2.5.1 Hubungan Hukum Transaksi *Ethereum* di Indonesia

Sebagai salah satu mata uang digital, *Ethereum* memiliki transaksi yang tidak seperti mata uang lainnya dan karenanya memiliki hubungan hukum yang berbeda. Sebagian besar mata uang memiliki jenis transaksi "segitiga" yang disebut sentralisasi atau terpusat dimana bank memainkan peran perantara keuangan antar pihak. Transfer pembayaran harus dilakukan melalui bank. Di sisi lain, transaksi *Ethereum* hanya membutuhkan dua pihak yang saling setuju untuk menukar barang atau mata uang tertentu dengan jumlah *Ether* tertentu. Transaksi ini disebut desentralisasi. Konsep transaksi ini tidak berbeda dengan konsep barter yang dilakukan untuk memenuhi kebutuhan mereka.

Gambar 2.1 Perbedaan antara transaksi terpusat dan transaksi terdesentralisasi



Sumber : Penulis