BAB II
LANDASAN TEORI

Pada bagian bab kedua terkait dengan landasan teori sebagai pedoman dalam melakukan penelitian. Lalu dalam bab ini terdapat pembahasan teori-teori mengenai verifikasi laporan investigasi forensik digital, teknologi *Blockchain*¸ jaringan Ethereum, dan metodologi pengembangan sistem.

2.1 Sistem Verifikasi Dokumen Investigasi Forensik Digital

Menurut dokumen Standardisasi Nasional Indonesia ISO 9000:2005 (2008) mengenai sistem manajemen mutu pada poin 3.8.4, definisi verifikasi adalah konfirmasi, melalui penyediaan bukti objektif, bahwa persyaratan yang ditentukan telah dipenuhi. Kemudian untuk pengertian dari sistem verifikasi dokumen hasil investigasi forensik digital merupakan sistem yang mengelola laporan terkait dengan dokumen investigasi forensik digital yang telah dibuat dan dikirimkan oleh pihak penyidik kepada pemeriksa atau ahli forensik digital dalam membantu proses verifikasi laporan

Selama proses pelaporan dan verifikasi tersebut, sistem ini juga dirancang dengan menggunakan teknologi *Blockchain.* Hal tersebut dilakukan supaya laporan yang sudah diperiksa oleh pemeriksa atau ahli forensik digital, selanjutnya akan dilakukan proses verifikasi dengan mengunggah dokumen melalui sistem dan juga menyimpan data pendukung integritasnya pada jaringan *Blockchain*, yang juga akan menghasilkan sebuah bukti transaksi unik (*transaction hash*) yang digunakan untuk membuktikan apakah dokumen yang digunakan telah terverifikasi pada sistem atau belum. Adapun tujuan perancangan sistem verifikasi ini dijelaskan pada poin-poin berikut:

a. Memudahkan penyidik untuk melakukan verifikasi laporan dokumen hasil investigasi forensik digital sebagai cara pengesahan sebuah laporan.
b. Menyediakan informasi laporan dokumen hasil investigasi forensik digital kepada pihak verifikator untuk dilakukan penilaian dan verifikasi yang dikirimkan oleh penyidik.
c. Menghasilkan laporan yang telah terverifikasi dengan baik untuk dapat digunakan sebagaimana semestinya.
d. Menjaga kevalidan data laporan dokumen investigasi forensik digital menggunakan *Blockchain*.

Sedangkan terkait dengan dokumen laporan yang ditulis dan dikirimkan juga bersifat resmi dan mengikuti pedoman penulisan yang disesuaikan untuk umum supaya dapat dimengerti serta mengandung penulisan dengan bahasa hukum untuk menjelaskan pembuktian. Menurut Kelley (2012), terdapat panduan atau struktur laporan dokumen hasil investigasi forensik digital yang baik dan juga harus memuat beberapa hal seperti:

a. Halaman judul laporan
b. Daftar isi
c. Ringkasan investigasi
d. Tujuan investigasi
e. Analisis barang bukti
f. Metodologi atau tahapan investigasi
g. Temuan-temuan yang berkaitan dengan kasus yang diselidiki
h. Kronologis atau alur investigasi
i. Kesimpulan
j. Bagian tanda tangan
k. Lampiran

2.2 Teknologi *Blockchain*

Blockchain sebagai bagian dari usulan yang penulis telah sampaikan pada pembahasan sebelumnya. Jelas diketahui bahwa *Blockchain* memiliki peran khusus dalam pembangunan sistem verifikasi dokumen laporan investigasi forensik digital. Sebelum memasuki tahapan implementasi atau penerapan *Blockchain* terhadap sistem yang dirancang, pada bagian subbab ini membahas penjelasan teori yang berkaitan dengan teknologi *Blockchain* seperti definisi, sejarah singkat *Blockchain*, struktur, cara kerja *Blockchain*, dan lain sebagainya.

2.2.1 Definisi *Blockchain*

Sejarah awal mula penemuan Bitcoin (uang digital) pada akhir tahun 2008, yang ditemukan oleh seorang yang bernama Satoshi Nakamato, serta dalam *paper* yang berjudul "Bitcoin: A Peer-to-PeerElectronic Cash System". Di mana dirinya menuliskan gagasan terkait pemanfaatan teknologi jaringan *Peer-to-Peer*. Menurut Schollmeier (2001) definisi *Peer-to-Peer* atau yang dikenal dengan P2P adalah jaringan terdistribusi yang dapat berbagi berkas media dan juga bertukar data antara dua komputer (*peer*) atau jenis jaringan tanpa adanya perantara. Untuk menangani transaksi elektronik yang telah dibahas dalam *paper* tersebut terkait konsep cara bertransaksi dengan uang digital (Bitcoin) secara daring tanpa

menggunakan pihak ketiga dan tanpa penyimpanan secara terpusat atau terdistribusi, penerapan konsep *Peer-to-Peer* tentu dapat dikatakan sudah sesuai untuk memberikan solusi terkait metode transaksi dengan menggunakan Bitcoin (Nakamoto, 2008).

Melalui temuan cara bertransaksi Bitcoin tersebut, secara bersamaan konsep *Blockchain* pun pada awalnya yang hanya digunakan untuk mengamankan transaksi uang digital tersebut, hingga sekarang telah mengalami perkembangan pesat yang dapat diterapkan dalam berbagai hal, terutama pada bidang digital yang mengutamakan kepercayaan, keamanan, dan kevaliditasan sebuah transaksi data. Menurut Yaga et al. (2018), *Blockchain* merupakan *ledger* atau buku besar digital yang terdistribusi dari transaksi yang ditandatangani secara kriptografis dan dikelompokkan ke dalam blok. Setiap blok dihubungkan secara kriptografis dengan *hash* blok sebelumnya setelah dilakukan validasi dan menjalani keputusan konsensus. Ketika blok baru berhasil dibuat dari proses *mining*, data pada blok sebelumnya akan hampir mustahil untuk diubah atau dimanipulasi.

Berkaitan dengan definisi *Blockchain* yang telah dijelaskan menurut Yaga et al. (2018), dapat ditarik kesimpulan mengenai definisi *Blockchain* secara umum, bahwa *Blockchain* merupakan *database* terdistribusi yang mencatat setiap terjadinya transaksi atau pertukaran dalam setiap blok dan dilindungi dengan metode keamanan kriptografi, sehingga aman dan tidak dapat mudah diubah nilainya. Namun, pada kenyataannya masih ditemukan pemikiran terkait definisi *Blockchain* dan *cryptocurrency* seperti Bitcoin merupakan hal yang sama pada masyarakat awam. Sebenarnya pemikiran tersebut tentu saja merupakan sebuah kekeliruan yang harus diluruskan. Pada dasarnya *Blockchain* tentu saja tidak sama dengan *cryptocurrency* seperti Bitcoin atau mata uang digital lainnya. Berikut terdapat uraian perbedaan antara *Blockchain* dan *cryptocurrency* pada Tabel 2.1:

Tabel 2.1 Perbedaan *Blockchain* dengan *Cryptocurrency*

Blockchain	**Cryptocurrency**
Blockchain merupakan teknologi seperti *ledger* atau basis data karena menyimpan segala informasi pertukaran data, seperti mata uang digital hingga surat sertifikat kepemilikan tanah.	*Cryptocurrency* adalah mata uang digital yang juga merupakan salah satu implementasi teknologi *Blockchain*, karena proses transaksinya disimpan pada *Blockchain*.

Tujuan dari teknologi *Blockchain* adalah untuk membuat biaya pertukaran nilai menjadi rendah dan memiliki lingkungan yang aman dalam transaksi *peer-to-peer* dengan siapa-pun.	Tujuan dari adanya *cryptocurrency* adalah untuk menyederhanakan dan meningkatkan kecepatan transaksi keuangan tanpa adanya batasan dari pihak tertentu.
Ranah pembahasan *Blockchain* sangat luas dan akan terus berkembang.	*Cryptocurrency* hanya terbatas pada pertukaran mata uang digital saja.

Pada penjelasan singkat perbedaan pada Tabel 2.1, dapat diambil kesimpulan bahwa sebenarnya *cryptocurrency* seperti Bitcoin, Ether, Litecoin dan berbagai jenis *cryptocurenncy* lainnya merupakan salah satu contoh hasil penerapan atau implementasi dari teknologi *Blockchain*, dan dapat dikatakan bahwa *Blockcain* tentu saja dapat berfungsi atau digunakan tanpa menggunakan *cryptocurrency*. Namun, *cryptocurrency* tentu tidak akan dapat digunakan tanpa teknologi *Blockchain*.

2.2.2 Jenis-Jenis *Blockchain*

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

a. *Public Blockchain*

Seperti namanya, *Blockchain* ini merupakan jaringan terdistribusi yang besar karena memiliki sifat publik yang berarti terbuka kepada semua orang yang berpartisipasi dan memiliki kode yang bersifat *open-source*, sehingga para komunitas dapat berdistribusi. Tujuan dari jenis *Blockchain* ini banyak digunakan untuk melakukan transaksi mata uang digital atau *cryptocurenncy*, di mana semua orang dapat melihat daftar transaksi yang pernah dilakukan dan memvalidasi transaksi.

b. *Private Blockchain*

Private Blockchain adalah salah satu jenis *Blockchain* yang bersifat tertutup dan bertujuan untuk melakukan pertukaran informasi secara internal saja. Tentu hal tersebut dapat membuat pihak-pihak yang tidak bergabung, tidak dapat melihat proses-proses apa saja yang dilakukan pada *Blockchain* tersebut. Menurut Mukhopadhyay (2018), terdapat batasan akses pada *private Blockchain*. Apabila terdapat organisasi atau perusahaan yang menerapkan teknologi *Blockchain* secara umum. Namun, tidak terlalu nyaman dengan akses kontrol yang

diberikan oleh jaringan publik (*public Blockchain*), tentu saja tujuan tersebut dapat dicapai dengan memanfaatkan *Blockchain* yang bersifat *private* ini.

c. *Semi-Private Blockchain*

Semi-private Blockchain atau sering disebut sebagai *consortium Blockchain*, merupakan jenis *Blockchain* yang memberikan hak akses kepada siapa saja yang berhak menggunakannya dan memiliki *source code* yang tertutup. Mirip seperti dengan *private Blockchain.* Namun, untuk penyimpanan data yang dikirimkan melalui transaksi tetap akan tersimpan pada jaringan *Blockchain* publik.

2.2.3 Perkembangan *Blockchain*

Menurut perkembangannya *Blockchain* hingga saat ini terbagi menjadi tiga era sejak pertama kali diperkenalkan dengan penemuan Bitcoin pada sekitar akhir tahun 2008 (Bashir, 2017), tiga era perkembangan *Blockchain* yaitu:

a. *Blockchain* 1.0

Generasi pertama dari *Blockchain* yang diawali dengan kemunculan istilah *Bitcoin* dan secara dasar digunakan untuk *cryptocurrency* atau mata uang digital, juga termasuk teknik kriptografi keuangan dalam mengamankan proses transaksi dan aplikasi secara publik.

b. *Blockchain* 2.0

Implementasi *Blockchain* untuk layanan keuangan dan kontrak cerdas (*smart contract*) diperkenalkan secara khusus pada generasi *Blockchain* 2.0 melalui *platform* jaringan yang bernama Ethereum. Selain itu juga berbagai macam pelayanan lainnya seperti perusahaan pasar juga mulai menggunakan layanan *Blockchain*. Pada generasi ini juga *Blockchain* lebih fleksibel terhadap kebutuhan penggunanya.

c. *Blockchain* 3.0

Pada generasi ketiga, *Blockchain* sudah digunakan untuk diimplementasikan pada aplikasi di luar industri jasa keuangan dan digunakan di industri yang lebih bersifat umum seperti pemerintahan, kesehatan, kepemilikkan karya seni, proses peradilan, dan lain sebagainya.

2.2.4 Kelebihan Teknologi *Blockchain*

Beberapa contoh kelebihan dari teknologi *Blockchain* yang telah diketahui dari definisi penjelasan sebelumnya yaitu:

a. Transparansi atau keterbukaan, dalam *Blockchain* menerapkan sistem yang transparan supaya proses yang ada di dalamnya dapat dilihat dan dibagikan kepada semua orang.

b. Kekal atau tetap, karena hanya terjadi sekali penulisan data pada *Blockchain* dan apabila data tersebut diubah, akan sangat susah sekali dan hampir tidak mungkin untuk mengubah semua data yang telah tersimpan pada *Blockchain*. Sebab data yang akan diubah akan mempengaruhi catatan transaksi setelahnya, sehingga dengan mengubah sebuah data, diperlukan upaya untuk mengubah hampir seluruh rekaman data yang telah ada.
c. Memiliki sistem keamanan yang kuat dengan menerapkan kriptografi seperti fungsi *hash* untuk memverifikasi dan menjaga integritas data pada setiap *block* sehingga valid serta mencegah dari adanya perubahan data.
d. Memiliki kemudahan dalam melacak setiap data transaksi pada jaringan *Blockchain*, karena data transaksi yang disimpan pada jaringan *Blockchain* tentu akan merujuk pada transaksi sebelumnya, sehingga hal ini dapat mempermudah dalam proses verifikasi dan pencarian data transaksi.
e. Bersifat *anonymous*, meskipun data yang disimpan pada jaringan publik *Blockchain* bersifat transaparan atau dapat dilihat oleh orang lain. Namun, terkait dengan identitas setiap pengguna yang mengirimkan maupun menerima transaksi dalam jaringan *Blockchain* menggunakan suatu alamat tertentu atau yang disbeut dengan *public key*, dan dalam hal ini, identitas sebenarnya dari setiap pengguna tidak ditampilkan pada interaksi transaksi tersebut

2.2.5 Struktur *Blockchain*

Di balik bagaimana cara proses *Blockchain* bekerja, tentunya terdapat bagian-bagian penting yang terstruktur supaya *Blockchain* dapat digunakan. Menurut Laurance (2017), struktur dari *Blockchain* terdiri dari 3 bagian komponen utama yaitu:

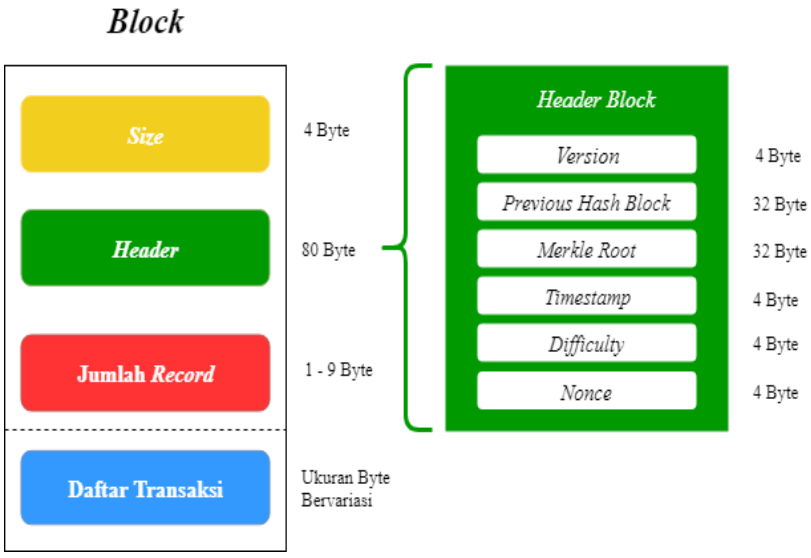
a. *Blok (block)*

Blockchain tersusun dari banyaknya *block* yang merupakan representasi untuk sebuah daftar transaksi yang sah dan disimpan. Setiap blok memiliki sebuah *hash* kriptografis sebagai *pointer* atau sebagai identitas setiap blok supaya dapat saling terhubung antara satu dengan yang lainnya.

Menurut Antonopoulos et al., (2017) struktur dari sebuah blok terdiri dari *header*, diikuti dengan metadata dan daftar transaksi yang disimpan. Pada Gambar 2.1, terdapat representasi struktur sebuah blok yang memiliki berbagai komponen. Berikut penjelasan terkait komponen yang ada pada setiap blok pada jaringan *Blockchain:*

1. *Block Size* merupakan bagian pertama dari struktur blok yang menyimpan informasi terkait dengan ukuran sebuah blok dalam bytes.

2. *Block Header* merupakan bagian dari sebuah blok yang memiliki ukuran 80 bytes dan menyimpan sekumpulan metadata, seperti:
    - *Version:* Menyimpan informasi versi sebuah blok dan memiliki ukuran sebesar 4 bytes.
    - *Previous Block Hash:* Metadata yang menyimpan *hash* pada blok sebelumnya, juga berfungsi sebagai "rantai" yang menghubungkan dengan blok tersebut dengan blok sebelumnya dan memiliki ukuran sebesar 32 bytes.
    - *Merkle Root:* Merupakan sekumpulan informasi dari semua transaksi yang telah dilakukan *hash* pada blok tersebut dengan memiliki ukuran sebesar 32 bytes dan bertujuan untuk memberikan kesimpulan dari semua transaksi yang dilakukan blok tersebut.
    - *Timestamp:* Menyimpan informasi terkait *timestamp* atau kapan waktu blok tersebut dibuat dengan memiliki ukuran sebesar 4 bytes.
    - *Difficulty Target:* Menyimpan informasi terkait tingkat kesulitan algoritma PoW (*Proof of Work*) yang digunakan dan memiliki ukuran sbesar 4 bytes.
    - *Nonce:* Merupakan angka acak yang disimpan dengan ukuran sebesar 4 bytes dan digunakan dalam proses penambangan blok baru.
3. Jumlah *Record* adalah bagian dari blok yang menghitung sebarapa banyak transaksi yang dilakukan dan biasanya memiliki ukuran 1-9 bytes.
4. Daftar Transaksi merupakan bagian yang menyimpan kumpulan data transaksi yang telah dilakukan pada sebuah blok tersebut dengan ukuran data yang bervariasi.



Gambar 2.1 Struktur Sebuah *Block*

b. Rantai (*chain*)

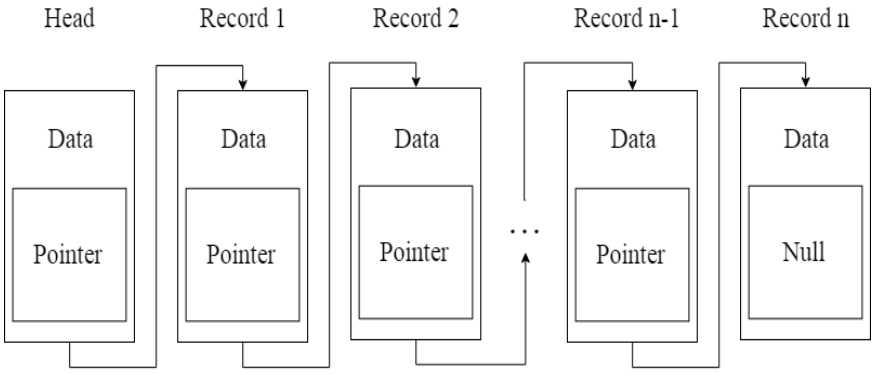
Supaya setiap *block* pada *Blockchain* saling terhubung, diperlukanlah "rantai" dalam bentuk *hash* yang menghubungkan antara satu *block* dengan *block* lainnya. Mekanisme *hash* merupakan salah satu konsep yang rumit secara matematis untuk diterapkan pada *Blockchain*. Meskipun *Blockchain* dianggap merupakan inovasi teknologi terbaru. Namun, tidak dengan *hash*. Konsep *hashing* tentunya sudah ada sejak sekitar 30 tahun yang lalu, dan digunakan pada konsep *Blockchain* karena *hash* hanya dapat membuat fungsi satu-arah yang tidak dapat dilakukan dekripsi. Fungsi sebuah *hashing* menciptakan algoritma matematis yang memetakan data dengan segala ukuran ke dalam karakter bit yang biasanya memiliki panjang sebanyak 32 karakter, yang mana panjang ukuran bit tersebut mempresentasikan data yang telah di-*hash*. *Secure Hash Algorithm* (SHA) merupakan salah satu fungsi *hash* yang digunakan oleh *Blockchain*, sedangkan algoritma yang biasa digunakan untuk melakukan *hash* pada *Blockchain* menggunakan algoritma SHA-256 yang dapat mengubah panjang ukuran data apapun menjadi sebuah karakter *hash* dengan ukuran 256 bits (32 bytes), sehingga pada *Blockchain, hash* bisa dianggap sebagai sidik jari digital yang bersifat unik dari data pada sebuah *block* untuk mengunci *block* supaya tetap berurutan di dalam *Blockchain*.

c. Jaringan (*networ*k)

Istilah jaringan atau *network* pada *Blockchain* merupakan representasi dari banyaknya *nodes* atau komputer yang saling terhubung satu sama lain dan menjalankan sebuah algoritma untuk mengamankan jaringan. Pada setiap *node* memiliki rekaman dari seluruh transaksi yang terekam pada *Blockchain.* Para *node* tersebut berlokasikan di seluruh dunia dan dikelola oleh setiap orang yang tergabung dalam jaringan *Blockchain*. Sudah sangat jelas terkait dengan topologi jaringan yang digunakan oleh *Blockchain* yaitu *Peer-to-Peer*, yang mana dari seluruh *node* dapat saling berkomunikasi antar satu *node* dengan *node* yang lain untuk menerima maupun mengirim pesan.

2.2.6 Cara Kerja *Blockchain*

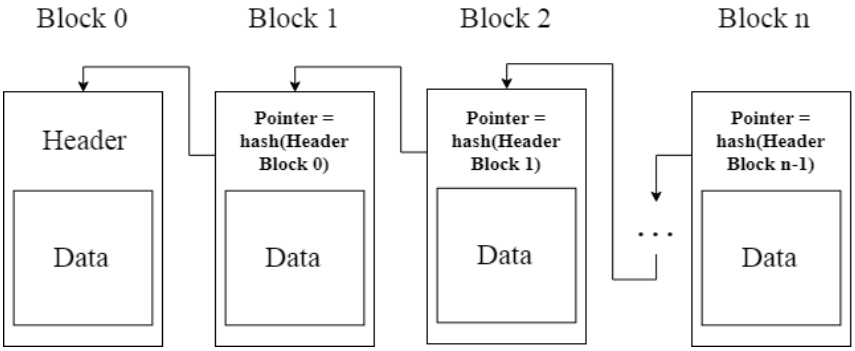
Blockchain dapat digambarkan seperti sekumpulan banyak blok yang tersambung dan membentuk seperti rantai. Pada hakikatnya *Blockchain* memiliki persamaan dengan cara kerja salah satu sebuah koleksi linear dari struktur data yaitu *linked list* atau sernarai berantai, di mana pada *linked list* terdiri dari struktur data yang digambarkan sebagai *node* tersebut berisi data yang disimpan dan akan merujuk pada *node* lain dengan bantuan *pointer* Gambar 2.2. Untuk mencari data dalam *linked list,* perlu dilakukan penelusuran dari *node* pertama hingga *node* yang menyimpan data yang dicari itu ditemukan.



Gambar 2.2 Diagram Skema *Linked List*

Sama halnya seperti pada *Blockchain*, di mana sebuah blok pada *Blockchain* tersebut terdiri dari data yang terstruktur dan memiliki tujuan untuk menyimpan sekumpulan data atau daftar transaksi, serta mendistribusikannya kepada seluruh *node* atau komputer pada jaringan. Pada proses transaksi setiap blok yang telah melakukan transaksi akan disimpan pada *Blockchain* dan setiap transaksi tersebut terdapat nilai *hash* yang didapatkan dari nilai *hash* blok sebelumnya kemudian dimasukan ke dalam blok, selanjutnya untuk menghitung nilai *hash*-nya yang baru, sehingga *hash* tersebut dapat dianggap sebagai *pointer* atau penghubung dari setiap blok tersebut. Namun, untuk nilai *hash* yang didapat harus memenuhi persyaratan tertentu yang disebut dengan *difficulty* supaya mendapat blok yang valid. Proses pencarian *hash* yang menghasilkan blok yang valid disebut juga sebagai PoW (*Proof of Work*).

Selain untuk menghasilkan blok yang valid, *hash* juga berfungsi sebagai identitas unik yang dimiliki oleh setiap blok, dan bermanfaat untuk menjaga integritas data supaya tidak mudah diubah. Apabila terdapat sedikit saja perubahan data pada blok, nilai *hash* pada blok tersebut akan berubah dan mempengaruhi nilai *previous hash* pada blok-blok selanjutnya, karena *Blockchain* menerapkan fungsi algoritma *hash* seperti SHA-256 yang telah dibahas pada penjelasan sebelumnya. Seperti yang diilustrasikan pada Gambar 2.3, dalam blokchain selalu diawali dengan blok ke-0 atau yang disebut dengan *genesis block*, sedangkan untuk menghasilkan blok ke-1 dan seterusnya atau blok baru, diperlukanlah *miner*. Istilah miner dalam *Blockchain* merupakan suatu pihak khusus yang memvalidasi transaksi dan menyimpan hasil transaksi pada *Blockchain*. Miner akan melakukan proses *mining* dengan menggunakan peralatan komputasi *hash* untuk menghasilkan blok baru. Meskipun ketika sebuah blok baru berhasil dihasilkan oleh *miner*, terkadang juga memungkinkan apabila terdapat *miner* lain yang menghasilkan blok baru secara bersamaan akan membuat sebuah *fork* atau percabangan pada *Blockchain* (Hanifatunnisa, 2017)



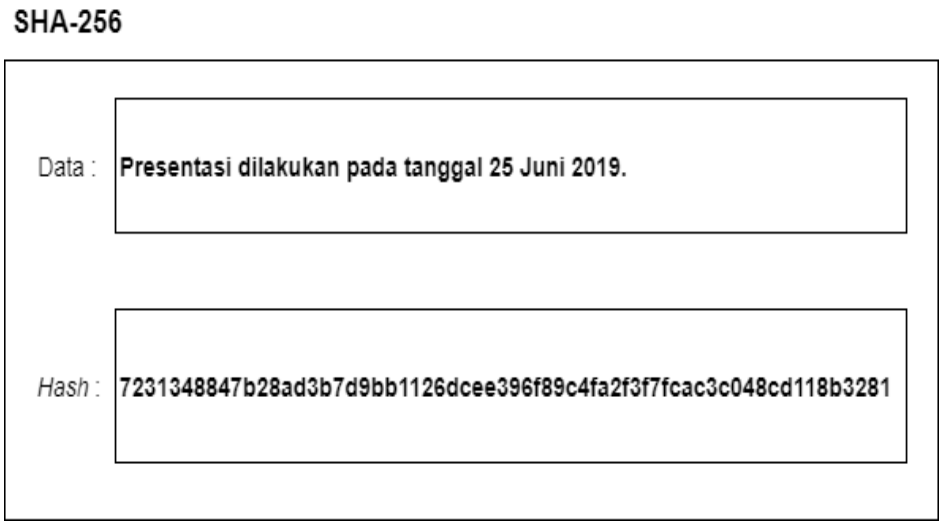
Gambar 2.3 Diagram Skema *Blockchain*

2.2.7 Fungsi Kriptografi *Hash*

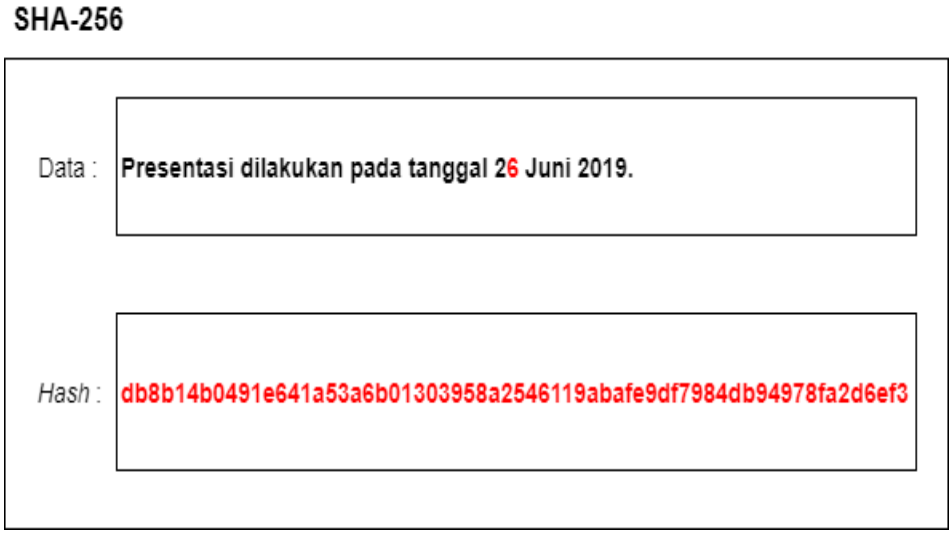
Kriptografi adalah sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf dan karakter di luar bentuk aslinya. Menurut Munir (2014), keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak memiliki makna, serta dengan kriptografi dapat membantu dalam mengirimkan dan menyimpan data yang tidak mudah untuk dibaca dengan menggunakan kunci yang dimiliki. Selain itu juga pada kriptografi terdapat proses yang disebut dengan *hashing* dengan menggunakan fungsi *hash*.

Hashing merupakan proses untuk mengubah segala data *input* menjadi data *output* yang terdiri susunan karakter acak dengan panjang yang telah ditentukan, dan dapat ditentukan sebagai karakter yang unik terhadap masing-masing data yang telah diproses. Berapa pun panjang *string* yang dimasukan, hasil keluaran data tersebut memiliki panjang yang tetap, dan juga proses *hashing* memastikan bahwa apabila terdapat sedikit perubahan pada data yang telah dimasuka akan mengubah dan mempengaruhi hasil data *output* tersebut.

Sebagai contoh dalam *Blockchain* diterapkan salah satu algoritma *hash* yaitu SHA-256 yang akan melakukan *hashing* terdapat data *input* menjadi data *output* dengan panjang 256 bit atau 64 karakter, sehingga kevalidan dan integritas data akan tetap terjaga dan tidak mudah dimanipulasi seperti pada Gambar 2.4 dan Gambar 2.5, yang mendemonstrasikan hasil *hasing* terhadap data *input* dan *output* apabila terdapat perubahan pada data aslinya.



Gambar 2.4 Data yang Dilakukan *Hashing* dengan SHA-256



Gambar 2.5 Perubahan pada Data yang Dilakukan *Hashing* dengan SHA-256

Selain itu *hash* pada *Blockchain* juga dijadikan sebagai *pointer* atau penghubung antar blok dan digunakan untuk menghasilkan dan memvalidasi blok baru seperti yang sudah dijelaskan pada bagian sebelumnya, sedangkan pada Ethereum juga menggunakan teknik *hashing* yang disebut dengan Keccak256 dengan cara yang rumit dan melakukan *hash* pada setiap transaksi yang terjadi, dari proses *hash* tersebut juga menghasilkan *transaction hash* atau sebagai bukti bahwa pihak tertentu telah melakukan transaksi melalui *Blockchain* Ethereum.

2.2.8 Pemanfaatan Teknologi *Blockchain*

Telah diketahui dari pembahasan perkembangan teknologi *Blockchain,* khususnya dimulai dari era *Blokchain* 2.0, di mana teknologi *Blockchain* pada kenyataannya sudah mulai diimplementasikan pada beberapa sektor selain bidang keuangan, dan juga pada bidang lain seperti kesehatan, industri, hukum, dan lainnya untuk memberikan solusi dalam pelayanan yang berkaitan dengan integritas atau keaslian data (Laurance, 2017). Berikut terdapat beberapa contoh pemanfaataan dari teknologi *Blockchain* adalah sebagai berikut:

a. Bidang hukum tentu dapat menerapkan teknologi *Blockchain* terutama saat dibutuhkan pada proses peradilan, dengan memanfaatkan *Blockchain*, informasi mengenai barang bukti tetap terjaga integritasnya dan mencegah adanya pemalsuan data kasus.
b. Bidang kesehatan juga dapat menerapkan *Blockchain* yang dapat diimplementasikan terutama terkait dengan kepentingan kerahasiaan data riwayat kesehatan pasien melalui rekam medis elektronik.
c. Bidang rantai persediaan seperti Walmart yang merupakan perusahaan dari Amerika Serikat yang mengoperasikan jaringan *departement store*. Bekerjasama dengan IBM, Walmart telah mengimplementasikan *Blockchain* sebagai bagian dari persyaratan keamanan pangan baru untuk para pemasoknya. Hal tersebut didasari supaya Walmart dapat melacak informasi bahan pangan dari pertanian ke toko dalam waktu dekat, dengan menggunakan sistem *ledger* terdistribusi *Blockchain* dan menghindari pemalsuan maupun kerugian lainnya.
d. Bidang keuangan terkait dengan melakukan transaksi mata uang digital (*cryptocurrency*) yang bisa dilakukan pada berbagai *platform* apa pun dengan syarat harus dapat terhubung dengan jaringan *internet*. Contoh penerapannya seperti Bitcoin, Litecoin, dan Ripple.

2.3 Ethereum

2.3.1 Definisi Ethereum

Ethereum (ETH) pertama kali diperkenalkan pada tahun 2013 oleh salah satu pengembangnya yaitu Vitalik Buterin yang merupakan seorang penulis dan *programmer* pada komunitas Bitcoin. Secara definisi Ethereum merupakan salah satu implementasi dari *Blockchain* yang memperkenalkan kemampuan komputasi untuk membangun kembali pemanfaatan *Blockchain* yang hanya dapat melakukan pertukuran mata uang digital menjadi transaksi nilai terutama aset digital antar pengguna melalui bahasa *script* (Buterin, Wiederhold, Riva, & Graffigna, 2013). Latar belakang penemuan Ethereum ini adalah pada saat tersebut terjadi perdebatan terkait dengan jaringan *Blockchain* yang “membengkak” dikarenakan

banyaknya transaksi yang bernilai rendah dari aplikasi-aplikasi berbasis *Blockchain* Bitcoin. (Laurance, 2017). Kekhawatiran utamanya adalah bahwa setiap aplikasi yang dibangun dengan protokol Bitcoin, akan memiliki permasalahan utama yaitu dalam masalah penskalaan volume transaksi yang terjadi, karena Bitcoin tidak dibangun untuk menangani jumlah transaksi yang dibutuhkan oleh setiap aplikasi yang dibangun. Berdasarkan permasalahan tersebut Vitalik dan rekan-rekannya melihat hal tersebut sebagai sebuah kesempatan supaya orang-orang dapat membangun aplikasi terdesentralisasi dalam *Blockchain*, sehingga dari hal tersebut dikembangkanlah sebuah *platform Blockchain* baru yang bernama Ethereum. Menurut latar belakang tersebut Ethereum dapat dianggap sebagai pengembangan dari Bitcoin yang mampu membangun aplikasi berbasis teknologi *Blockchain*.

Secara komponennya Ethereum memiliki dua komponen penting yaitu prosesor virtual turing (*Turing-complete virtual processor*) yang disebut sebagai *Ethereum Virtual Machine* (EVM) yang memungkinkan prosesor Turing dalam Ethereum tersebut menjalankan *script* atau bahasa pemrograman yang disebut Solidity untuk membangun aplikasi terdesentralisasi dan juga nilai token yang disebut dengan Ether, supaya dapat digunakan sebagai mata uang atau *cryptocurrency* yang disahkan oleh jaringan untuk melakukan transaksi antar pengguna atau sebagai kompensasi bagi para *miner* (Dhillon, Metcalf, & Hooper, 2017), sehingga dapat terlihat jelas, perbandingan antara Bitcoin dan Ethereum. Bitcoin merupakan *implementasi* dari *Blockchain* yang bersifat *public* dan memiliki batasan terhadap bahasa *script* untuk membangun sebuah aplikasi berbasis *Blockchain*. Namun, dengan Ethereum pengembang aplikasi dapat lebih fleksibel untuk mengembangkan aplikasi berbasis *Blockchain* yang dapat diatur berdasarkan konsensusnya maupun jenis *Blockchain* yang digunakan yaitu *private* atau *public Blockchain* (Bashir, 2017).

2.3.2 Akun pada Ethereum

Akun pada Ethereum merupakan hal yang mendasari bagaimana cara kerja *Blockchain* Ethereum. Akun-akun tersebut digunakan untuk menyimpan dan menelusuri informasi pengguna dalam jaringan. Menurut Modi (2018) pada *platform* Ethereum terdapat dua jenis akun, yaitu:

a. *User Account* (*externally owned accounts*) merupakan akun yang dimiliki oleh pengguna pada Ethereum. Ketika akun pengguna Ethereum dibuat, pada saat itu juga menghasilkan sebuah kunci *public* dan kunci *private*. Kunci *private* disimpan aman secara individu, dan kunci *public* digunakan sebagai alamat akun atau identitas *User account*. Kunci *public* umumnya terdiri dari 256 karakter. Namun, untuk Ethereum hanya menggunakan 42

karakter pertama untuk mewakili identitas akun, dan ditulis dalam bentuk hexadesimal seperti: **"0x19afA8C970AaB2D3a24F42d85244e8756d23293a"** Akun ini juga sering disebut sebagai akun eksternal yang menyimpan nilai (*balance*) dalam satuan Ether. Karena kedudukan akun ini bersifat eksternal, akun ini dapat melakukan transaksi dengan menjalankan fungsi yang sudah didefenisikan pada kontrak.

b. *Contract Accounts* (*contract address*) terkait pembahasan pada Ethereum, akun kontrak merupakan jenis akun yang mirip dengan *User account* (*externally owned accounts*), karena dapat diidentifikasi dengan menggunakan kunci publik (*public key*) namun, tidak memiliki p*rivate key*. Sebuah akun kontrak memiliki nilai Ether yang mirip dengan akun pengguna atau *User account* yang digunakan apabila terdapat fungsi yang dijalankan, karena pada akun kontrak memiliki *script* kode untuk menjalankan fungsi dan variabel seperti yang dituliskan pada *smart contract* yang digunakan.

2.3.3 *Smart Contract*

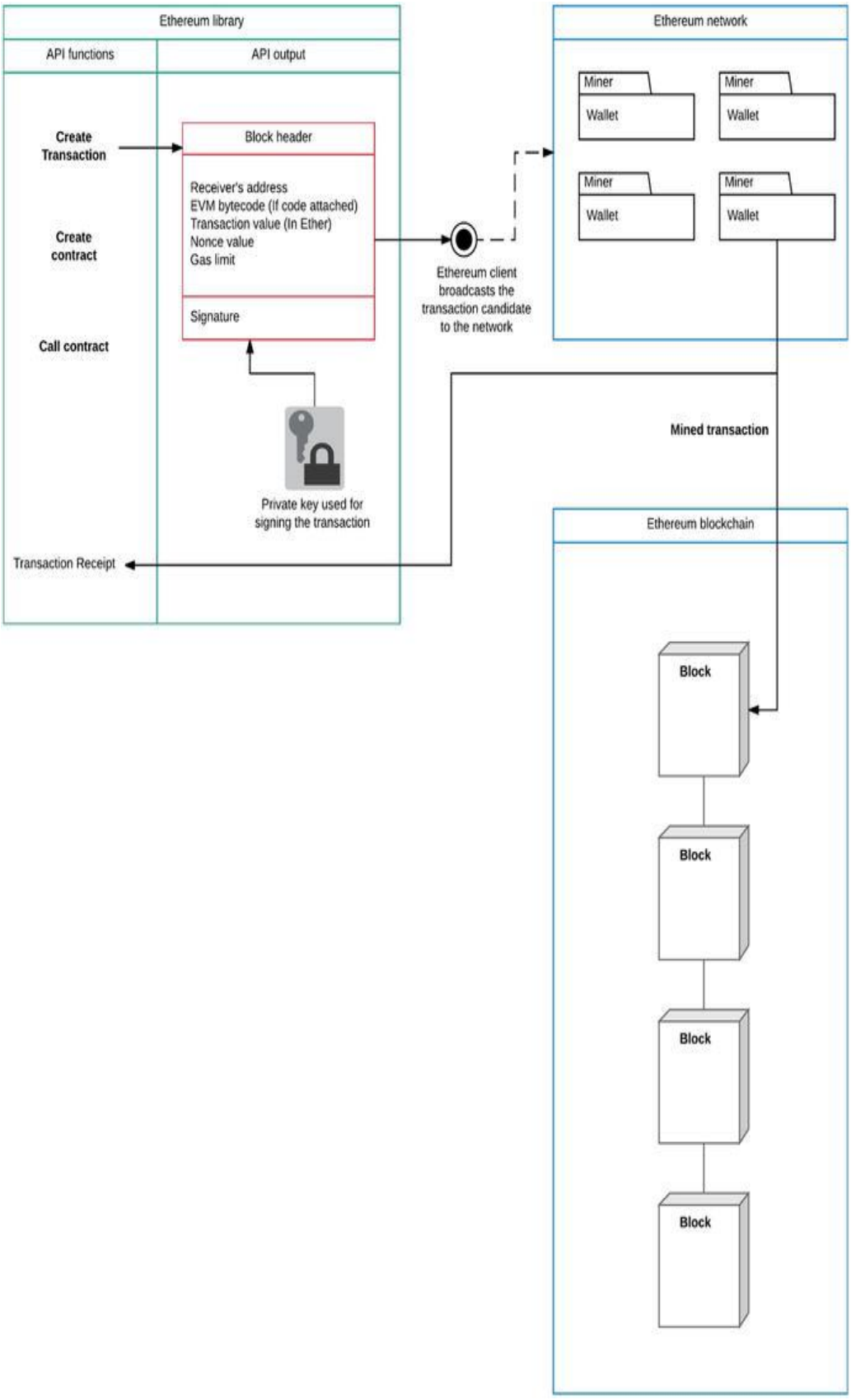
Perkembangan *Blockchain* hingga saat ini ternyata sudah banyak dimanfaatkan dan diterapkan pada berbagai bidang seperti yang telah dibahas sebelumnya. Supaya pihak pengembang dapat menerapkan aplikasi yang dibangun berbasis *Blockchain,* solusi yang tepat adalah dengan menggunakan *smart contract*. Kontrak cerdas atau s*mart contract* merupakan penerapan dari *platform Blockchain* yang memiliki tujuan untuk menentukan kesepakatan (*consensus*) antara beberapa pihak berdasarkan jenis konsensus yang digunakan dan diaplikasikan dalam bentuk *script* atau kode sebagai logika bisnis yang terkait dalam penggunaan sistem atau aplikasi berbasis teknologi *Blockchain* (Laurance, 2017).

Implementasi *smart contract* tentunya dapat dibangun sesuai dengan kebutuhan yang diinginkan dan digunakan secara aktif melalui *platform Blockchain* manapun seperti Ethereum dengan menggunakan bahasa pemrograman yang bernama Solidity. Untuk merancang *smart contract,* serta melakukan transaksi tanpa adanya pihak ketiga dengan menggunakan satuan Ether di jaringan Ethereum, seperti yang terlihat pada Gambar 2.6, dengan adanya kesepakatan dalam bentuk *smart contract* seharusnya dapat meningkatkan transparansi serta kepercayaan terhadap aplikasi *Blockchain* bagi penggunanya.

2.3.4 Cara Kerja Ethereum

Penerapan dari arsitektur *Blockchain* terhadap Ethereum tentunya memiliki persamaan arsitektur yang terdiri dari berbagai komponen yang saling berinteraksi dan bekerja sama untuk menjalankan fungsinya. Terkait dengan bagaimana Ethereum bekerja dalam *Blockchain*, tentunya terdapat beberapa komponen penting di balik proses tersebut. Komponen Ethereum yang dimaksud meliputi *Ethereum Virtual Machine* (EVM), *miner*, blok, *mining*, Ether, dan gas (Dhillon et al., 2017). Seperti yang telah dijelaskan sebelumnya bahwa jaringan *Blockchain* terdiri dari sekumpulan *node* yang dimiliki oleh para *miner* (penambang) dan juga beberapa *node* yang tidak dimiliki oleh siapa pun namun, tetap membantu melakukan eksekusi terhadap *smart contract* dan transaksi.

Proses eksekusi terhadap *smart contract* dan transaksi tersebut dijalankan pada *Ethereum Virtual Machine* (EVM) yang merupakan perangkat *Turing-complete* yang berjalan pada jaringan Ethereum seperti yang digambarkan pada Gambar 2.6. EVM juga digunakan sebagai tempat penyimpanan bagi *smart contract* untuk dapat membantu dalam memperluas Ethereum dengan menuliskan fungsionalitas atau logika bisnis dalam pengembangan aplikasi berbasis *Blockchain*. Tahapan berikutnya adalah s*mart contract* dapat dieksekusi sebagai bagian dari transaksi dan dalam proses *mining*, sedangkan Ether digunakan sebagai satuan *cryptocurrency* dalam jaringan Ethereum yang memiliki fungsi seperti halnya untuk melakukan transaksi dari satu akun ke akun yang lain atau juga dapat digunakan dalam menjalankan fungsi-fungsi yang telah ditetapkan pada *smart contract.*

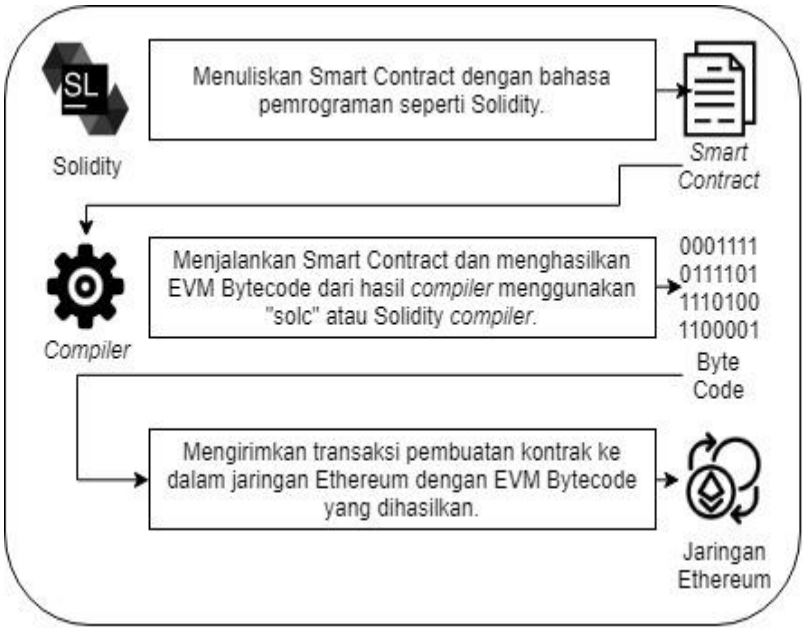


Gambar 2.6 Skema Cara Kerja Jaringan Ethereum

Selain itu juga terdapat komponen yang disebut dengan gas, yaitu sebuah bagian internal yang menjaga nilai Ethereum atau merupakan bentuk biaya untuk melakukan transaksi secara mikro supaya dapat menjaga proses komputasi pada *Blockchain.* Gas akan dibayarkan ketika terjadi proses operasi eksekusi pada fungsi yang ada pada *smart contract*. Terkait dengan berapa jumlah besaran gas yang dibayarkan pada setiap melakukan eksekusi sebuah kode terbilang sangat kecil karena mengadopsi sifat transaksi mikro. Apabila gas tersebut habis, pengguna tentu tidak dapat melanjutkan operasi transaksi. Dalam proses transaksi menggunakan Ethereum, transaksi juga harus ditandatangani secara digital dengan menggunakan *private key* pemilik akun. Hal tersebut untuk memastikan bahwa identitas pengirim dapat digunakan pada saat melakukan proses verifikasi akun (Modi, 2018).

2.3.5 Bahasa Pemrograman Solidity

Solidity merupakan bahasa pemrograman berorientasi objek (kontrak) yang memiliki tujuan untuk merancang *smart contract* supaya dapat berjalan pada *Ethereum Virtual Machine* (EVM), serta disimpan dalam sebuah file dengan ekstensi (.sol). Segala kode yang dituliskan dalam bahasa pemrograman Solidity akan dikompilasi menggunakan Solidity *compiler* atau biasa disebut dengan “solc” yang menghasilkan bytecode (sekumpulan fungsi yang telah di-*encode*), supaya dapat dijalankan dan dieksekusi pada EVM seperti yang digambarkan pada Gambar 2.7.



Gambar 2.7 Proses *Compile* dan *Deploy* Kontrak

Pada proses *encoding* dengan *compiler* supaya menghasilkan Bytecode yang digunakan sebagai referensi fungsi dan kontrak untuk diekseskusi pada EVM. Proses *encoding* tersebut dibantu dengan menggunakan ABI (*Application Binary Interface*) yang merupakan daftar definisi fungsi dalam kontrak dan beberapa argumen yang ditulis dalam format *Javascript Object Notation* (JSON). Daftar fungsi dan argument tersebut diubah dengan *hash* menjadi ABI, kemudian dapat diolah oleh EVM. ABI sangat diperlukan supaya dapat menentukan fungsi mana yang ada pada kontrak untuk dijalankan, serta menjamin fungsi tersebut akan mengembalikan data dalam format yang sudah ditentukan (Dhillon et al., 2017).

2.4 Penelitian Terdahulu

Sistem verifikasi dokumen hasil investigasi laporan forensik digital berbasis teknologi *Blockchain* merupakan salah satu contoh penerapan dari berbagai sistem verifikasi dokumen yang menggunakan *Blockchain* dalam proses bisnisnya. Sistem verifikasi khususnya dokumen elektronik biasa digunakan pada instansi-instansi tertentu dalam membuktikan keaslian dokumen yang telah terverifikasi dan juga memudahkan pengguna yang melakukan verifikasi dokumen. Terlebih lagi apabila sistem verifikasi dokumen elektronik tersebut telah menerapkan teknologi *Blockchain*, sehingga diharapkan integritas data dokumen tersebut terjamin pada sistem verifikasi yang telah dikembangkan.

Perlu diketahui terkait dengan penelitian yang penulis lakukan, bahwa hingga saat ini belum ditemukan kajian penelitian terhadap pengembangan sistem verifikasi dokumen laporan investigasi forensik digital serupa yang menerapkan teknologi *Blockchain*. Meskipun belum ada yang membahas mengenai penelitian yang penulis lakukan. Penulis menemukan beberapa penelitian yang mengkaji penerapan teknologi *Blockchain* pada sistem verifikasi dokumen elektronik yang berupa sertifikat maupun ijazah kelulusan perguruan tinggi. Meskipun tidak berkaitan dengan dokumen laporan investigasi forensik digital, penelitian-penelitian tersebut diharapkan bisa dijadikan sebagai referensi sebagai landasan teori mengenai cara atau alur sistem verifikasi dokumen yang menerapkan teknologi *Blockchain*. Adapun rangkuman dari penelitian-penelitian tersebut dapat dilihat pada Tabel 2.2.

Tabel 2.2 Penelitian Terdahulu

No	Penulis	Judul	Pembahasan
1	Kumavat, dkk. (2019)	*Certificate Verification System using Blockchain*	Pengembangan sistem verifikasi sertifikat menggunakan *Blockchain* Ethereum.
2	Winarno (2019)	Desain e-Transkrip dengan Teknologi *Blockchain*	Mendesain rancangan sistem verifikasi dokumen ijazah perguruan tinggi dengan menerapkan implementasi teknologi *Blockchain* yang berupa Blockcert.
3	Karatas (2018)	*Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System*	Membangun sistem verifikasi untuk sertifikat digital berbasis *Blockchain* Ethereum yang menerapkan *smart contract* dengan sistem manajemen pembelajaran Moodle.

Penelitian yang dilakukan oleh Kumavat dan kawan-kawan di tahun 2019, membahas tentang cara mengembangkan sistem verifikasi untuk dokumen sertifikat yang dimiliki oleh mahasiswa di sebuah universitas menggunakan *Blockchain* Ethereum. Masalah utama dari penelitian ini adalah untuk mencegah adanya pemalsuan sertifikat dan juga untuk membantu proses verifikasi secara konvensional menjadi proses verifikasi secara praktis melalui sistem yang dikembangkan. Adapun tujuan dari penelitian ini adalah mengembangkan sistem verifikasi sertifikat terdesentralisasi yang menerapkan teknologi *Blockchain* Ethereum. Penulis memilih menerapkan teknologi *Blockchain*, karena data yang disimpan pada *Blockchain* akan mudah untuk ditelusuri (*traceable*), dapat dibuktikan, dan aman, sehingga sertifikat yang sudah disimpan akan terjaga integritasnya. Supaya sistem dapat terhubung dengan *Blockchain*, pada bagian *backend* atau server sistem diterapkan juga *smart contract* supaya sistem dan jaringan *Blockchain* Ethereum dapat saling berinteraksi. Hasil dari pengembangan sistem verifikasi ini adalah sistem akan memberikan ID transaksi (*transaction hash*) yang didapat dari proses transaksi penyimpanan data sertifikat pada *Blockchain* Ethereum, dengan menggunakan ID transaksi tersebut, semua pihak yang mengetahui ID transaksi dapat melakukan pemeriksaan atau verifikasi dokumen sertifikat pada sistem verifikasi yang dikembangkan maupun jaringan *Blockchain* Ethereum.

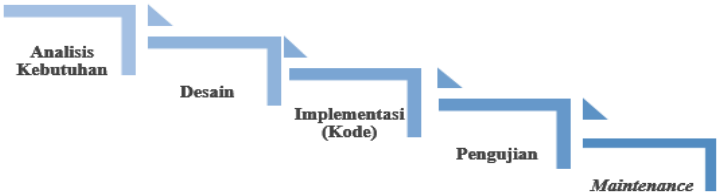
Penelitian lain terkait dengan sistem verifikasi dokumen berbasis *Blockchain* seperti dilakukan oleh Winarno pada tahun 2019, bertujuan untuk mendesain rancangan sistem verifikasi dokumen ijazah perguruan tinggi dengan menerapkan implementasi teknologi *Blockchain* yang berupa Blockcert. Adapun permasalahan yang dibahas pada penelitian ini disebabkan oleh banyaknya kasus pemalsuan dokumen ijazah perguruan tinggi ketika melakukan pelamaran kerja. Berdasarkan dari permasalahan tersebut, diperlukan sebuah pemanfaatan sistem yang mampu menangani proses pelaporan dan verifikasi dokumen ijazah. Salah satunya adalah dengan menggunakan Blockcert. Pada penelitian tersebut diketahui bahwa Blockcert merupakan salah satu implementasi teknologi *Blockchain* yang bertujuan untuk menerbitkan dan memverifikasi dokumen resmi. Berbeda dengan penilitan lainnya yang dibahas, pada penilitian ini penulis menggunakan Blockcert yang berjalan pada jaringan *Blockchain* Bitcoin. Lalu untuk hasil dari penilitian ini adalah menghasilkan sebuah desain skema kerja sistem e-transkrip dengan menerapkan teknologi *Blockchain* yang terbagi menjadi tiga tahapan proses yaitu; tahap penerbitan transkrip, penerbitan ijazah, dan verifikasi dokumen. Ijazah yang telah disimpan dapat diverifikasi pada sistem maupun pada Blockcert, sehingga dengan adanya penerapan *Blockchain* tersebut diharapkan dapat mencegah pemalsuan ijazah perguruan tinggi.

Kemudian, pada penelitian yang dilakukan oleh Karatas di tahun 2018 membahas mengenai pembangunan sistem verifikasi dokumen yang berupa sertifikat digital berbasis *Blockchain* Ethereum yang menerapkan *smart contract* dengan sistem manajemen pembelajaran Moodle. Penelitian tersebut bertujuan untuk memverifikasi sertifikat digital yang diberikan dan membangun sistem verifikasi dokumen berbasis *Blockchain* Ethereum yang menerapkan *smart contract,* serta kemudahan dalam penggunaan sistem manajemen pembelajaran Moodle untuk menerbitkan sertifikat digital. Pada penilitian ini diketahui juga menggunakan *smart contract* yang dirancang untuk menghubungkan sistem dengan jaringan *Blockchain* Ethereum, dan digunakan juga dalam proses penyimpanan data sertifikat digital. Adapun hasil dari penelitian ini sistem dapat melakukan proses verifikasi sertifikat digital dengan memasukan nomor serial yang tertera pada sertifikat yang diberikan, apabila nomor serial yang dimasukan terdaftar pada sistem. Sistem akan menampilkan data sertifikat digital berserta bukti transaksi penyimpanan pada *Blockchain* Ethereum dalam bentuk *transaction hash.*

2.5 Metode Pengembangan Sistem

Metode pengembangan sistem (atau disebut juga model proses rekayasa perangkat lunak) merupakan salah satu cara yang digunakan untuk memadukan proses, metode, dan perangkat (*tools*), dengan menggunakan metode-metode pengembangan sistem tentu saja dapat memberikan panduan dan cara untuk membangun suatu sistem perangkat lunak atau aplikasi (Pressman, 2010.). Berkaitan dengan serangkaian tugas yang luas yang menyangkut analisis kebutuhan, konstruksi program, desain, pengujian, dan pemeliharaan. Pada penelitian untuk membangun sistem verifikasi dokumen hasil investigasi forensik digital ini, penulis menerapkan metode pengembangan sistem yang disebut dengan metode *waterfall*.

Metode *waterfall* merupakan metode yang di mana antar satu fase ke fase pengembangan yang lain dilakukan secara berurutan. Dalam proses implementasi metode *waterfall* ini, sebuah fase atau langkah akan diselesaikan terlebih dahulu yang dimulai dari tahapan pertama sebelum melanjutkan ke tahapan yang berikutnya. Tahapan-tahapan pada metode *waterfall* dimulai dari melakukan analisis kebutuhan, desain sistem, implementasi kode pemrograman, pengujian, dan pemeliharaan atau *maintenane*, seperti pada skema Gambar 2.8**.** Alasan penulis memilih menggunakan metode pengembangan *waterfall* dalam mengembangkan sistem verifikasi dokumen hasil investigasi forensik digital berbasis *Blockchain* adalah supaya kebutuhan sistem dapat didokumentasikan dengan lengkap, sedikit terjadinya perubahan, dan proses pengembangannya dapat dilaksanakan tepat waktu.



Gambar 2.8 Diagram Metode Pengembangan Sistem *Waterfall*

a. Analisis Kebutuhan

Pada tahapan inisisasi awal dalam metode *waterfall* yaitu analisis kebutuhan, pihak pengembang harus dapat melakukan identifikasi terhadap segala jenis kebutuhan yang diperlukan untuk mengembangkan sistem dengan melakukan komunikasi terhadap pihak-pihak yang akan menggunakan sistem tersebut, supaya pengembang dapat memahami aspek kebutuhan dan perangkat apa saja yang digunakan dan juga memberikan batasan pada sistem yang dikembangkan.

b. Desain Sistem

Pada tahapan ini pengembang sistem akan mempelajari hasil identifikasi spesifikasi kebutuhan dari tahapan sebelumnya dan juga melakukan persiapan rancangan desain sistem. Desain sistem membantu dalam menentukan kebutuhan aplikasi *web* dan juga membantu dalam merancang arsitektur sistem secara keseluruhan.

c. Implementasi Kode Pemrograman

Setelah melakukan identifikasi dan perancangan keseluruhan desain dan arsitektur sistem pada tahapan sebelumnya. Pada tahap ini pengembang akan mengubah hasil desain tersebut menjadi kode program yang nantinya akan diintegrasikan menjadi sebuah sistem aplikasi yang utuh.

d. Pengujian

Pada tahapan ini kode pemrograman dan modul sistem yang telah dirancang akan diintegrasikan menjadi sebuah sistem yang lengkap dan juga dilakukan pengujian terhadap fungsionaltias sistem yang telah dibuat dan melakukan pengujian performa transaksi penyimpanan data pada jaringan publik *Blockchain* Ethereum.

e. *Maintenance* atau Pemeliharaan Sistem

Tahap akhir dalam model pengembangan *waterfall* yaitu melakukan *maintenance* atau pemeliharaan sistem secara berkala termasuk di antaranya adalah proses perbaikan sistem apabila ditemukannya kesalahan/*error* yang sudah dapat atau tidak dapat ditemukan dalam tahap sebelumnya (tahap pengujian), supaya dapat segera diperbaiki.