

**SKRIPSI**

**IMPLEMENTASI TEKNOLOGI BLOCKCHAIN PADA  
SISTEM PENELUSURAN RANTAI PASOK ALAT  
KESEHATAN**

**Disusun dan diajukan oleh:**

**FADHIL KHUSNUL HAKIM  
D121191049**



**PROGRAM STUDI SARJANA TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS HASANUDDIN  
GOWA  
2024**

# LEMBAR PENGESAHAN SKRIPSI

## IMPLEMENTASI TEKNOLOGI BLOCKCHAIN PADA SISTEM PENELUSURAN RANTAI PASOK ALAT KESEHATAN

Disusun dan diajukan oleh

**Fadhil Khusnul Hakim**  
**D121191049**

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian  
Studi Program Sarjana Program Studi Teknik Informatika  
Fakultas Teknik Universitas Hasanuddin  
Pada tanggal 22 Juli 2024  
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,



Dr.Eng. Muhammad Niswar, ST., M.IT  
NIP 197309221999031001



Adnan, ST., M.T., Ph.D  
NIP 197404262005011002

Ketua Program Studi,



Prof. Dr. I. Indrabawati, ST, MT, M.Bus.Sys., IPM, ASEAN.Eng  
NIP 197507162002121004

## PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini;  
Nama : Fadhil Khusnul Hakim  
NIM : D121191049  
Program Studi : Teknik Informatika  
Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

“Implementasi Teknologi Blockchain Pada Sistem Penelusuran Rantai Pasok Alat Kesehatan.”

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini, maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, Senin 22 Juli 2024

ng Menyatakan



Fadhil Khusnul Hakim

## ABSTRAK

**FADHIL KHUSNUL HAKIM.** *Implementasi Teknologi Blockchain pada Sistem Penelusuran Rantai Pasok Alat Kesehatan Fasilitas Kesehatan* (dibimbing oleh Muhammad Niswar dan Adnan)

Data yang ada di Kementerian Kesehatan Republik Indonesia mengenai alat kesehatan dapat dilihat ada banyak alat kesehatan (alkes) yang diimport dari luar negeri, sedangkan ada banyak kasus *illegal* dan pemalsuan alat kesehatan di luar dan dalam negeri. Permasalahan ini dapat mengakibatkan meningkatkan risiko kesehatan dari konsumen atau pasien di fasilitas kesehatan. Berdasarkan situasi dan permasalahan tersebut, pada penelitian ini memanfaatkan *blockchain* dan integrasi *smart contract* untuk mencapai transparansi dan keaslian data dengan baik. Sistem ini dibangun dengan menggunakan platform *blockchain* Ethereum dengan integrasi *smart contract* dengan menggunakan bahasa pemrograman *solidity*. Hasil implementasi sistem yang dilakukan dapat menunjukkan pengujian *vulnerability* terhadap *smart contract* yang dibuat, pengujian *vulnerability* ini dilakukan untuk meningkatkan struktur dari ekosistem *blockchain* yang dibuat agar mencegah peretasan dari luar yang ingin mencoba menyerang sistem *blockchain* dengan cara membuat *block-block* baru berdasarkan kemungkinan-kemungkinan yang ada. Dan penelitian telah merancang 5 aktor diantaranya manufaktur, distributor, kemenkes, faskes, dan pasien. Pada penelitian ini juga telah dapat melakukan 9 aktifitas dalam sistem penelusuran rantai pasok alat kesehatan fasilitas kesehatan ini diantaranya, penginputan alkes oleh manufaktur, permintaan alkes distributor ke manufaktur, persetujuan alkes oleh manufaktur untuk distributor, permintaan nomor izin edar alkes ke kemenkes, pemberian nomor izin edar oleh kemenkes, permintaan alkes fasilitas kesehatan ke distributor, persetujuan alkes oleh distributor, permintaan alkes oleh pasien dan persetujuan alkes oleh faskes. Dan berdasarkan semua aktifitas itu dengan membandingkan penggunaan gas dan besaran ukuran data yang dikirim pada penelitian memperlihatkan bahwa semakin banyak penggunaan gas yang diperlukan dalam membuat sebuah *block* maka semakin besar pula ukuran data yang diinput atau ditransmisikan oleh *user* ke dalam sebuah *block*.

**Kata Kunci:** Alat Kesehatan, Blockchain, Ethereum.

## ABSTRACT

**FADHIL KHUSNUL HAKIM.** *Implementation of Blockchain Technology in Medical Supply Chain Tracking System* (supervised by Muhammad Niswar and Adnan)

The data from the Ministry of Health of the Republic of Indonesia regarding medical devices reveals that there are numerous instances of medical devices being imported from abroad, alongside numerous cases of illegal and counterfeit medical devices both domestically and internationally. This issue can result in an increased health risk for consumers or patients in healthcare facilities. In light of this situation and problem, this study leverages blockchain technology and smart contract integration to achieve transparency and data authenticity. The system is constructed using the Ethereum blockchain platform with smart contract integration through the Solidity programming language. The implementation results of the system demonstrate vulnerability testing against the created smart contracts. This vulnerability testing is conducted to enhance the structure of the blockchain ecosystem created, thereby preventing external hacking attempts seeking to attack the blockchain system by generating new blocks based on existing possibilities. The research has also delineated five types of users, including manufacturers, distributors, the Ministry of Health, healthcare facilities, and patients. Furthermore, this study has successfully executed nine activities within the supply chain tracking system for medical devices in healthcare facilities, such as inputting medical devices by manufacturers, distributor requests for medical devices from manufacturers, manufacturer approvals for distributors, requests for circulation permit numbers for medical devices from the Ministry of Health, issuance of circulation permit numbers by the Ministry of Health, healthcare facility requests for medical devices from distributors, distributor approvals for medical devices, patient requests for medical devices, and healthcare facility approvals for medical devices. Finally, based on all these activities and by comparing the gas usage and data size transmitted in the research, it is evident that the greater the gas usage required to create a block, the larger the data size input or transmitted by the user into a block.

**Keywords:** Medical Devices, Blockchain, Ethereum

## DAFTAR ISI

<b>LEMBAR PENGESAHAN SKRIPSI .....</b>	<b>i</b>
<b>PERNYATAAN KEASLIAN .....</b>	<b>ii</b>
<b>ABSTRAK .....</b>	<b>iii</b>
<b>ABSTRACT .....</b>	<b>iv</b>
<b>DAFTAR ISI.....</b>	<b>v</b>
<b>DAFTAR GAMBAR.....</b>	<b>vii</b>
<b>DAFTAR TABEL .....</b>	<b>ix</b>
<b>DAFTAR SINGKATAN DAN ARTI SIMBOL .....</b>	<b>x</b>
<b>DAFTAR LAMPIRAN.....</b>	<b>xi</b>
<b>KATA PENGANTAR.....</b>	<b>xii</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1. Latar Belakang .....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian/Perancangan.....	3
1.4 Manfaat Penelitian/Perancangan.....	3
1.5 Ruang Lingkup/Asumsi perancangan .....	4
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>5</b>
2.1 Rantai Pasok Alat Kesehatan .....	5
2.2 Alat Kesehatan .....	6
2.3 <i>Blockchain</i> .....	11
2.4 <i>Smart Contract</i> .....	18
2.5 Ethereum .....	19
2.5.1. <i>Account</i> .....	21
2.5.2. Transaksi .....	22
2.5.3. <i>Block</i> .....	24
2.6 Ganache.....	27
2.7 Metamask.....	28
<b>BAB III METODE PENELITIAN/PERANCANGAN.....</b>	<b>29</b>
3.1 Instrumen Penelitian .....	29
3.2 Tahapan Penelitian.....	30
3.3 Rancangan Sistem.....	31
3.4 Use Case Diagram Sistem.....	33
3.5 Activity Diagram Sistem.....	34
3.6 Desain <i>Smart Contract</i> .....	34
3.7 Skenario Analisis dan Pengujian .....	44
<b>BAB iV .....</b>	<b>46</b>
<b>HASIL DAN PEMBAHASAN .....</b>	<b>46</b>
4.1 Implementasi <i>Blockchain</i> pada Sistem .....	46
4.2 Pengujian Fungsionalitas Sistem .....	53
4.3 Analisis <i>Vulnerability Smart Contract</i> Sistem.....	66
4.4 Pengujian Simulasi Perubahan Data pada Rantai Block Penggunaan Gas dan Ukuran Data <i>Blockchain</i> .....	71
4.5 Analisis Penggunaan Gas dan Ukuran Data <i>Blockchain</i> .....	74
<b>BAB v .....</b>	<b>76</b>
<b>KESIMPULAN DAN SARAN .....</b>	<b>76</b>

5.1 Kesimpulan .....	76
5.2 Saran .....	77
<b>DAFTAR PUSTAKA .....</b>	<b>78</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>81</b>

## DAFTAR GAMBAR

Gambar 1. Statistik Izin Edar Alkes (Kemenkes, 2023) .....	2
Gambar 2. Presentase dan Jumlah Produk Dalam dan Luar Negeri .....	2
Gambar 3. Ilustrasi Rantai Pasok Alat Kesehatan .....	5
Gambar 4. Ilustrasi <i>Blockchain</i> .....	13
Gambar 5. Komputasi <i>Block Hash</i> .....	14
Gambar 6. Arsitektur DApp ( <i>Decentralized Application</i> ) .....	19
Gambar 7. <i>Block Header</i> .....	25
Gambar 8. Tahapan Penelitian .....	30
Gambar 9. Desain DApp .....	32
Gambar 10. <i>Use Case Diagram</i> Sistem .....	33
Gambar 11. <i>Activity Diagram</i> Penginputan Alkes oleh Manufaktur .....	35
Gambar 12. <i>Activity Diagram</i> Permintaan Alkes Distributor ke Manufaktur .....	35
Gambar 13. <i>Activity Diagram</i> Persetujuan Alkes oleh Manufaktur untuk Distributor .....	36
Gambar 14. <i>Activity Diagram</i> Permintaan Alkes Distributor ke Manufaktur .....	37
Gambar 15. <i>Activity Diagram</i> Persetujuan Alkes oleh Manufaktur untuk Distributor .....	37
Gambar 16. <i>Activity Diagram</i> Permintaan Alkes Fasilitas Kesehatan ke Distributor .....	38
Gambar 17. <i>Activity Diagram</i> Persetujuan Alkes oleh Distributor untuk Fasilitas Kesehatan .....	39
Gambar 18. <i>Activity Diagram</i> Permintaan Alkes Pasien ke Fasilitas Kesehatan .....	39
Gambar 19. <i>Activity Diagram</i> Persetujuan Alkes oleh Fasilitas Kesehatan untuk Pasien .....	40
Gambar 20. ERD ( <i>Entity Relationship Diagram</i> ) Smart Contract Blockchain .....	44
Gambar 21. Menu Registrasi User .....	46
Gambar 22. Menu Tambah Data Alkes .....	47
Gambar 23. Menu <i>List</i> Data Alkes .....	47
Gambar 24. Menu Daftar Transaksi Manufaktur dengan Distributor .....	48
Gambar 25. Menu <i>Request</i> Alkes ke Manufaktur .....	48
Gambar 26. Menu <i>response</i> Alkes dari Fasilitas Kesehatan .....	49
Gambar 27. Menu Daftar Transaksi Distributor dengan Manufaktur .....	49
Gambar 28. Menu Kemenkes .....	50
Gambar 29. Menu <i>Request</i> Alkes ke Distributor .....	50
Gambar 30. Menu <i>List</i> Transaksi Alkes Fasilitas Kesehatan .....	51
Gambar 31. Menu <i>Request</i> Alkes ke Faskes .....	52
Gambar 32. Menu <i>List</i> Transaksi Alkes Pasien .....	52
Gambar 33. Konfigurasi <i>truffle.js</i> .....	53
Gambar 34. Hasil <i>Deployment Blockchain</i> Ganache .....	53
Gambar 35. Proses Penginputan dan Transaksi Data Alkes .....	54
Gambar 36. <i>Block</i> Hasil Transaksi Penginputan Alkes .....	54
Gambar 37. <i>List</i> Alkes Menu Manufaktur .....	55
Gambar 38. Detail Informasi Alkes Menu Manufaktur .....	55
Gambar 39. Proses Permintaan Alkes Distributor ke Manufaktur .....	56

Gambar 40. <i>Block Hasil Request</i> Distributor ke Manufaktur .....	56
Gambar 41. <i>List</i> Transaksi Alkes Distributor .....	56
Gambar 42. Proses Persetujuan Alkes oleh Manufaktur.....	57
Gambar 43. <i>Block Hasil</i> Persetujuan Alkes oleh Manufaktur .....	57
Gambar 44. Detail Informasi Alkes Menu Distributor .....	58
Gambar 45. Menu Transaksi Permintaan Izin Edar .....	58
Gambar 46. Proses Transaksi Permintaan Nomor Izin Edar.....	58
Gambar 47. <i>Block Hasil</i> Transaksi Permintaan Nomor Izin Edar .....	59
Gambar 48. Daftar Transaksi antar Distributor dan Kemenkes .....	59
Gambar 49. Proses Transaksi Pemberian Nomor Izin Edar.....	60
Gambar 50. <i>Block</i> dari Hasil Transaksi Pemberian Nomor Izin Edar .....	60
Gambar 51. Informasi Detail Alkes Menu Kemenkes .....	60
Gambar 52. Proses Request Alkes ke Distributor .....	61
Gambar 53. <i>Block</i> dari Hasil Request Alkes ke Distributor .....	61
Gambar 54. <i>List</i> Transaksi Alkes Menu Fasilitas Kesehatan .....	62
Gambar 55. Proses Persetujuan Alkes oleh Distributor .....	62
Gambar 56. <i>Block</i> dari Hasil Persetujuan Alkes oleh Distributor.....	63
Gambar 57. Informasi Alkes Menu Fasilitas Kesehatan.....	63
Gambar 58. Proses Request Alkes ke Distributor .....	64
Gambar 59. <i>List</i> Transaksi Alkes Menu Fasilitas Kesehatan .....	64
Gambar 60. Proses Persetujuan Alkes oleh Faskes.....	65
Gambar 61. Informasi Alkes Menu Pasien .....	65
Gambar 62. Analisis <i>Smart Contract</i> Rantai Pasok dengan Slither.....	66
Gambar 63. Analisis Perbaikan <i>Smart Contract</i> Rantai Pasok .....	67
Gambar 64. Analisis <i>Smart Contract</i> Alat Kesehatan .....	68
Gambar 65. Analisis Perbaikan <i>Smart Contract</i> Alat Kesehatan .....	69
Gambar 66. Analisis <i>Smart Contract</i> Transaksi Pengguna .....	70
Gambar 67. Analisis Perbaikan <i>Smart Contract</i> Transaksi Pengguna.....	70
Gambar 68. Rantai <i>Block</i> Peer A .....	71
Gambar 69. Rantai <i>Block</i> Peer B.....	72
Gambar 70. Rantai <i>Block</i> Peer C.....	72
Gambar 71. Kondisi Rantai <i>Block</i> Awal Peer B .....	73
Gambar 72. Kondisi Rantai <i>Block</i> Setelah Perubahan Data Peer B.....	73
Gambar 73. Grafik Analisis Perbandingan Penggunaan Gas dan Ukuran Data <i>Blockchain</i> .....	75

## DAFTAR TABEL

Tabel 1. Bidang Aplikasi <i>Blockchain</i> .....	16
Tabel 2. Variabel <i>Smart Contract</i> .....	41
Tabel 3. Fungsi <i>Smart Contract</i> .....	42
Tabel 4. Tabel Uraian Analisis <i>Smart Contract</i> Rantai Pasok.....	67
Tabel 5. Tabel Uraian Analisis <i>Smart Contract</i> Alat Kesehatan .....	69
Tabel 6. Tabel Uraian Hasil Analisis <i>Smart Contract</i> Transaksi Pengguna .....	70
Tabel 7. Hasil Analisis Penggunaan Gas dan Ukuran Data <i>Blockchain</i> .....	74

## DAFTAR SINGKATAN DAN ARTI SIMBOL

---

Lambang/Singkatan	Arti dan Keterangan
Alkes	Alat Kesehatan
Faskes	Fasilitas Kesehatan
DApps	<i>Decentralized Application</i>
ETH	<i>Ethereum</i>
Tx	<i>Transmitted</i>

---

## DAFTAR LAMPIRAN

Lampiran 1. Source Code <i>Smart</i> Contract (SupplyChain.sol).....	81
Lampiran 2. Source Code <i>Smart</i> Contract (RawAlkes.sol) .....	85
Lampiran 3. Source Code <i>Smart</i> Contract (Transactions.sol).....	88
Lampiran 4. Full Source Code .....	89

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas rahmat dan berkat-Nya, sehingga dapat menyelesaikan tugas akhir skripsi yang berjudul “Implementasi Teknologi *Blockchain* pada Sistem Penelusuran Rantai Pasok Alat Kesehatan” sebagai salah satu syarat dalam menyelesaikan jenjang Strata-1 di Departemen Teknik Informatika, Fakultas Teknik, Universitas Hasanuddin.

Penulis menyadari banyak kesulitan dan kendala yang dihadapi saat penyusunan tugas akhir ini. Dalam prosesnya, penulis memperoleh banyak bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Tuhan Yang Maha Esa melalui berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan tugas akhir ini,
2. Kedua orang tua penulis, Bapak Abd. Hakim dan Ibu Yulianti yang selalu menyertai penulis dalam doanya serta mendukung, membantu, memberi semangat serta kasih sayang dalam perjalanan penulis menyelesaikan tugas akhir ini,
3. Bapak Dr.Eng. Muhammad Niswar, ST., M.IT. selaku pembimbing I dan Bapak Adnan, ST., M.T., Ph.D selaku pembimbing II, yang senantiasa menyediakan waktu, tenaga, pikiran, dan perhatian dalam mengarahkan penulis untuk menyelesaikan tugas akhir,
4. Segenap Dosen dan Staff Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin yang telah banyak membantu penulis selama masa perkuliahan,
5. Teman-teman Teknik Informatika Angkatan 2019 selaku rekan yang telah memberi bantuan, dukungan dan semangat selama masa perkuliahan dan penyusunan tugas akhir ini,
6. Serta berbagai pihak atas segala dukungan dan bantuannya yang tidak dapat penulis tuliskan satu persatu,

Penulis berharap semoga Tuhan membalas segala kebaikan yang telah diterima oleh penulis dari berbagai pihak yang telah membantu mempermudah penulis dalam mengerjakan tugas akhir ini. Penulis menyadari bahwa tugas akhir ini masih jauh dari kata sempurna, oleh karena itu penulis mengharapkan segala bentuk saran serta masukan yang membangun dari berbagai pihak. Semoga tugas akhir ini dapat memberikan pengetahuan dan manfaat bagi penulis dan pembaca

Makassar, Januari 2024

Penulis,  
Fadhil Khusnul Hakim

# BAB I PENDAHULUAN

## 1.1. Latar Belakang

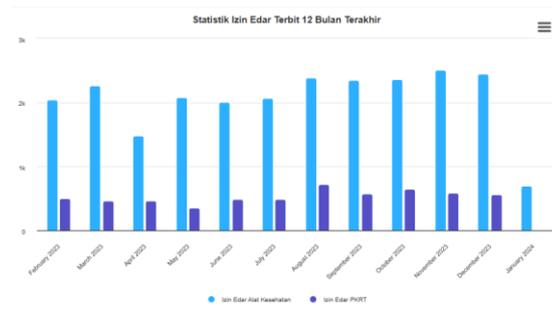
Teknologi *blockchain* telah menjadi topik yang semakin populer dalam beberapa tahun terakhir. Dimulai dari munculnya mata uang digital (*Bitcoin*), dan juga penerapan pada *Supply Chain Management* (SCM). SCM merupakan proses yang kompleks dalam mengelola aliran barang, informasi, dan jasa. Sektor bisnis mencakup pemasok hulu, Perusahaan produksi, distributor hulu, pengecer, dan pelanggan atau konsumen dengan *smart contract* (Fu & Zhu, 2019). *Smart contract* adalah program yang dijalankan di atas teknologi *blockchain* yang secara otomatis mengeksekusi dan mengelola perjanjian kontrak sesuai dengan ketentuan yang telah ditentukan. Smart contract memungkinkan transaksi dilakukan tanpa perantara, dengan keamanan dan transparansi yang terjamin. Fungsi utama dari smart contract dalam konteks SCM adalah untuk mengotomatisasi dan memverifikasi setiap tahap dalam proses distribusi. Dengan menggunakan smart contract, setiap langkah dalam rantai pasok dapat dicatat dan diverifikasi secara otomatis tanpa perlu campur tangan manusia, sehingga mengurangi risiko kesalahan atau manipulasi data. *Smart contract* juga memastikan bahwa setiap produk yang didistribusikan telah memenuhi standar dan regulasi yang berlaku, sehingga meningkatkan kepercayaan dan keamanan dalam rantai pasok.

Dan Salah satu contoh penerapan SCM dengan *Smart Contract* berbasis blockchain yang dapat dilakukan adalah di bidang kesehatan, yaitu dalam manajemen rantai pasok alat kesehatan. Adanya insiden dalam rantai Pasok alat kesehatan seperti pemalsuan data atau alat kesehatan, ataupun penyebaran alat kesehatan tanpa adanya izin edar, yang dapat merugikan ataupun membahayakan kesehatan pasien. Dan jika di lihat dari data statistik yang ada di website kemenkes<sup>1</sup>. Dalam website tersebut menampilkan informasi Alat Kesehatan dan PKRT

---

<sup>1</sup> Kemenkes, "E-Info Alkes PKRT Kemenkes RI" (<https://infoalkes.kemkes.go.id/>, diakses pada 28 Desember 2023)

(Perbekalan Kesehatan Rumah Tangga). Dan pada Gambar 1 menunjukkan izin edar alat Kesehatan kurang lebih 2000 perbulan dalam 12 bulan terakhir .



Gambar 1. Statistik Izin Edar Alkes (Kemenkes, 2023)

Dan dari keseluruhan alat Kesehatan yang memiliki izin edar di Indonesia, ada banyak alat Kesehatan yang diimport dari luar negeri. Sebanyak 54.391 (78.3%) alat Kesehatan dari luar negeri, sedangkan dalam negeri hanya 15.059 (21.7%) alat Kesehatan.



Gambar 2. Presentase dan Jumlah Produk Dalam dan Luar Negeri

Dengan banyaknya alat Kesehatan yang diimport dari luar negeri dapat bisa menyebabkan masalah tentang keaslian alat. Hal ini diungkapkan oleh WHO sendiri dari salah satu artikel dari luar (Bently, 2022). Dalam artikel tersebut bahwa 10 tahun lalu WHO pernah mengatakan bahwa secara global terdapat 8% alat kesehatan yang palsu dan bisa saja bertambah (Bently, 2022). Dan dalam artikel tersebut juga mengatakan bahwa pada tahun 2021 saat pelaksanaan *Interpol Operation Pangea XIII*, Ditemukan produk alat kesehatan *illegal* dengan nilai sebesar \$14 juta (Rp. 209 Miliar) dengan 121 kasus penangkapan dan penutupan

2500 situs web (Bently, 2022). Di Indonesia sendiri kasus pidana yang berkaitan dengan Alkes (Alat Kesehatan) ini juga terjadi beberapa tahun terakhir, seperti Penjualan Alkes Palsu (Tanpa Izin Edar) secara *online*, penyelundupan Alkes, dan juga penggelapan dana Alkes.

Dengan demikian, dengan adanya penerapan SCM dengan smart contract berbasis blockchain pada manajemen rantai pasok alat kesehatan dapat meningkatkan transparansi dan keamanan data, dengan menjadikan blockchain sebagai kunci untuk menciptakan sistem yang transparan, aman, dan efisien dalam manajemen rantai Pasok, sehingga dapat memperkuat kepercayaan pasien dengan menjaga kualitas produk sesuai dengan data digital yang ada, Oleh karena itu, penulis mengangkat judul penelitian "Implementasi Teknologi Blockchain Pada Penelusuran Rantai Pasok Alat Kesehatan."

## **1.2 Rumusan Masalah**

1. Bagaimana membangun sistem rantai pasok alat kesehatan berbasis web3 dengan mengimplementasikan *blockchain*?
2. Bagaimana membuktikan bahwa data yang dihasilkan oleh sistem tidak dapat dimanipulasi?

## **1.3 Tujuan Penelitian/Perancangan**

1. Membangun sistem rantai pasok alat kesehatan berbasis web3 dengan menerapkan teknologi *blockchain*.
2. Membuktikan bahwa data yang dihasilkan oleh sistem data yang dijaga keasliannya dan tidak dapat dimanipulasi.

## **1.4 Manfaat Penelitian/Perancangan**

1. Bagi *stakeholder* rantai pasok peralatan medis, diharapkan dengan penelitian ini dapat dijadikan sebagai rujukan untuk merancang rantai pasok peralatan medis secara transparansi dan aman berbasis *website*.
2. Bagi layanan Kesehatan (konsumen), penelitian ini diharapkan dapat digunakan sebagai cara untuk melakukan pencegahan penggunaan atau pembelian alat kesehatan yang palsu.

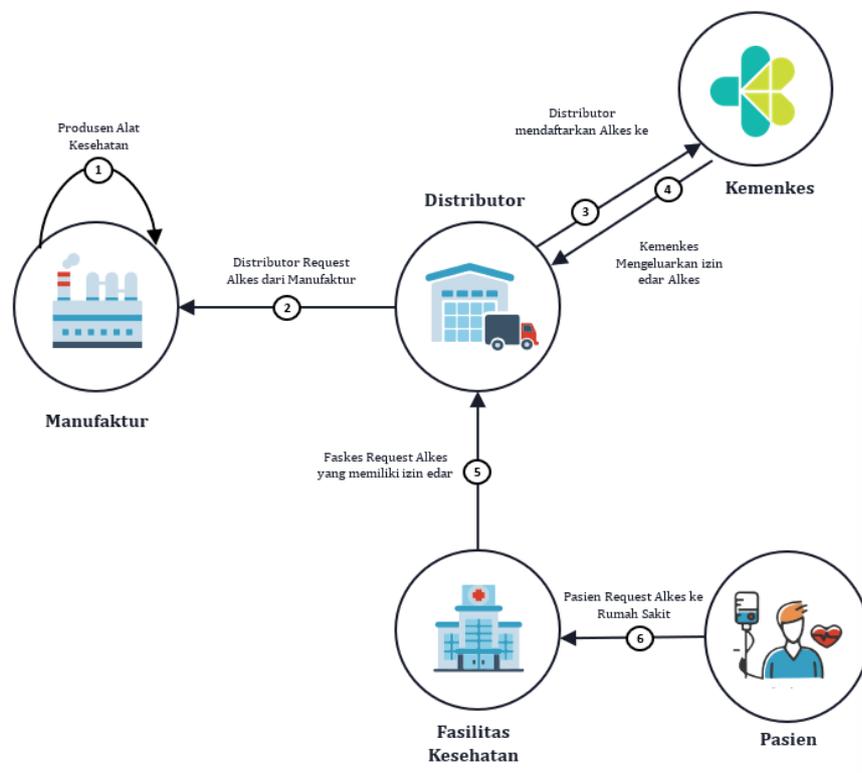
### **1.5 Ruang Lingkup/Asumsi perancangan**

1. Penelitian ini akan melakukan simulasi skenario rantai pasok peralatan medis dari produsen hingga konsumen dengan mengambil contoh data di website Kemenkes Republik Indonesia.
2. Simulasi rantai pasok peralatan medis terdiri dari 5 aktor :
  - a. Produsen (Manufaktur)
  - b. Kemenkes Republik Indonesia
  - c. Distributor
  - d. Fasilitas Kesehatan.
  - e. Pasien.

## BAB II TINJAUAN PUSTAKA

### 2.1 Rantai Pasok Alat Kesehatan

Rantai pasok atau *supply chain* alat kesehatan merupakan suatu rangkaian proses yang melibatkan produksi, distribusi, penyimpanan, dan penggunaan alat kesehatan dari awal hingga akhir. Rantai pasok ini memiliki beberapa tahapan utama dan melibatkan berbagai pihak atau entitas untuk memastikan alat kesehatan dapat tersedia, diakses, dan digunakan dengan efektif. Pada Gambar 3 adalah tahapan umum dari ilustrasi rantai pasok alat kesehatan.



Gambar 3. Ilustrasi Rantai Pasok Alat Kesehatan

Pada Gambar 3, menunjukkan tahapan awal pada manufaktur yang bertugas secara umum sebagai entitas yang bertanggung jawab atas produksi alat kesehatan. Mereka mengonsept, merancang, dan memproduksi berbagai jenis alat kesehatan. Kedua, Distributor sebagai perantara yang bertugas mengelola dan mendistribusikan alat kesehatan dari manufaktur ke berbagai pihak, termasuk fasilitas kesehatan atau layanan kesehatan. Ketiga, Kemenkes merupakan pihak

yang bertanggung jawab atas regulasi, pengawasan, dan persetujuan alat kesehatan demi kepentingan, kesehatan dan keselamatan masyarakat dengan memastikan bahwa alat kesehatan yang beredar aman, efektif, dan sesuai dengan standar kesehatan, Keempat, Fasilitas kesehatan adalah tempat atau layanan yang menyediakan alat kesehatan digunakan untuk pelayanan medis. Mereka juga bertanggung jawab untuk mengelola persediaan dan memastikan alat kesehatan yang digunakan memenuhi standar, Kelima pasien sebagai konsumen atau pengguna terakhir dari alat kesehatan, dengan berhak menerima fasilitas dan alat kesehatan yang efektif dan aman bagi kesehatan dan keselamatan pengguna atau pasien.

## 2.2 Alat Kesehatan

Alat kesehatan (Alkes) didefinisikan sebagai instrumen, apparatus, mesin dan/atau implan yang tidak mengandung obat yang digunakan untuk mencegah, mendiagnosis, menyembuhkan dan meringankan penyakit, merawat orang sakit, memulihkan kesehatan pada manusia, dan/atau membentuk struktur dan memperbaiki fungsi tubuh. Selain kategori diatas, juga ada alat kesehatan Diagnostik in vitro (DIV) adalah setiap reagen, produk, kalibrator, material kontrol, kit, instrumen, apparatus, peralatan atau sistem, baik digunakan sendiri atau dikombinasikan dengan reagen lainnya, produk reagen, kalibrator, material kontrol, kit, instrumen, apparatus, peralatan atau sistem yang diharapkan oleh pemilik produknya untuk digunakan secara *in vitro* untuk pemeriksaan dari setiap spesimen, termasuk darah atau donor jaringan yang berasal dari tubuh manusia, semata-mata atau pada dasarnya untuk tujuan memberikan informasi dengan memperhatikan keadaan fisiologis atau patologis atau kelainan bawaan, untuk menentukan keamanan dan kesesuaian setiap darah atau donor jaringan dengan penerima yang potensial, atau untuk memantau ukuran terapi dan mewardahi spesimen. (Peraturan Menteri Kesehatan Nomor 62 Tahun 2017).

Ada 16 Pengelompokan Alkes dan Alkes *Diagnostik in Vitro* (DIV) sesuai dengan Peraturan Menteri Kesehatan Nomor 62 Tahun 2017, sebagai berikut :

1. Peralatan Kimia Klinik Dan Toksikologi Klinik
  - a. Sistem Tes Kimia Klinik

- b. Peralatan Laboratorium Klinik
  - c. Sistem Tes Toksikologi Klinik
2. Peralatan Hematologi Dan Patologi
    - a. Pewarna Biologi
    - b. Produk Kultur Sel dan Jaringan
    - c. Peralatan dan Aksesori Patologi
    - d. Pereaksi Penyedia Spesimen
    - e. Peralatan Hematologi Otomatis dan Semi Otomatis
    - f. Peralatan Hematologi Manual
    - g. Paket dan Kit Hematologi
    - h. Pereaksi Hematologi
    - i. Produk yang digunakan dalam pembuatan sediaan darah dan sediaan berasal dari darah
  3. Peralatan Imunologi Dan Mikrobiologi
    - a. Peralatan Diagnostika
    - b. Peralatan Mikrobiologi
    - c. Pereaksi Serologi
    - d. Perlengkapan dan Pereaksi Laboratorium Imunologi
    - e. Sistem Tes Imunologikal
    - f. Sistem Tes Imunologikal Antigen Tumor
  4. Peralatan Anestesi
    - a. Peralatan Anestesi Diagnostik
    - b. Peralatan Anestesi Pemantauan
    - c. Peralatan Anestesi Terapetik
    - d. Peralatan Anestesi Lainnya
  5. Peralatan Kardiologi
    - a. Peralatan Kardiologi Diagnostik
    - b. Peralatan Kardiologi Pemantauan
    - c. Peralatan Kardiologi Prostetik
    - d. Peralatan Kardiologi Bedah
    - e. Peralatan Kardiologi Terapetik
  6. Peralatan Gigi

- a. Peralatan Gigi Diagnostik
  - b. Peralatan Gigi Prostetik
  - c. Peralatan Gigi Bedah
  - d. Peralatan Gigi Terapetik
  - e. Peralatan Gigi Lainnya
7. Peralatan Telinga, Hidung Dan Tenggorokan (THT)
- a. Peralatan THT Diagnostik
  - b. Peralatan THT Prostetik
  - c. Peralatan THT Bedah
  - d. Peralatan THT Terapetik
8. Peralatan Gastroenterologi-Urologi (Gu)
- a. Peralatan GU Diagnostik
  - b. Peralatan GU Pemantauan
  - c. Peralatan GU Prostetik
  - d. Peralatan GU Bedah
  - e. Peralatan GU Terapetik
9. Peralatan Fasilitas Kesehatan Umum Dan Perorangan (RSU & P)
- a. Peralatan RSU & P Pemantauan
  - b. Peralatan RSU & P Terapetik
  - c. Peralatan RSU & P Lainnya
10. Peralatan Neurologi
- a. Peralatan Neurologi Diagnostik
  - b. Peralatan Neurologi Bedah
  - c. Peralatan Neurologi Terapetik
11. Peralatan Obstetrik Dan Ginekologi (OaG)
- a. Peralatan OG Diagnostik
  - b. Peralatan OG Pemantauan
  - c. Peralatan OG Prostetik
  - d. Peralatan OG Bedah
  - e. Peralatan OG Terapetik
  - f. Peralatan Bantu Reproduksi
12. Peralatan Mata

- a. Peralatan Mata Diagnostik
- b. Peralatan Mata Prostetik
- c. Peralatan Mata Bedah
- d. Peralatan Mata Terapetik

### 13. Peralatan Ortopedi

- a. Peralatan Ortopedi Diagnostik
- b. Peralatan Ortopedi Prostetik
- c. Peralatan Ortopedi Bedah

### 14. Peralatan Kesehatan Fisik

- a. Peralatan Kesehatan Fisik Diagnostik
- b. Peralatan Kesehatan Fisik Prostetik
- c. Peralatan Kesehatan Fisik Terapetik

### 15. Peralatan Radiologi

- a. Peralatan Radiologi Diagnostik
- b. Peralatan Radiologi Terapetik
- c. Peralatan Radiologi Lainnya

### 16. Peralatan Bedah Umum Dan Bedah Plastik

- a. Peralatan Bedah Diagnostik
- b. Peralatan Bedah Prostetik
- c. Peralatan Bedah Peralatan Bedah Terapetik

Berdasarkan resiko yang ditimbulkan dalam penggunaannya, Alkes dan Alkes DIV dikelompokkan menjadi 4 (empat) kelas, yaitu:

#### 1. Alkes:

- a. Kelas A (resiko rendah), contoh: Film viewer, instrument bedah, sarung tangan bedah, oxygen mask.
- b. Kelas B (resiko rendah sampai sedang), contoh: Blood Pressure cuff, Steam Sterilizer.
- c. Kelas C (resiko sedang sampai tinggi), contoh: Patient Monitor, Mesin X-Ray.
- d. Kelas D (resiko tinggi), contoh: Stent Jantung, Pacemaker.

## 2. Alkes DIV:

- a. Kelas A: Resiko terhadap individu rendah (low individual risk) dan resiko terhadap kesehatan publik rendah (low public health risk), Contoh: Alat uji kimia klinis (Clinical Chemistry Analyzer), alat cek/uji kadar kolesterol, alat cek/uji kadar asam urat;
- b. Kelas B: Resiko terhadap individu sedang (moderate individual risk) dan resiko terhadap kesehatan publik rendah (low public health risk), Contoh: Alat Uji Kehamilan Pemakaian sendiri (pregnancy self testing)
- c. Kelas C: Resiko terhadap individu tinggi (high individual risk) dan resiko terhadap kesehatan publik sedang (moderate public health risk), Contoh: penentuan tipe Human Leukocyte Antigen (HLA), Skrining Prostat Specific Antigen (PSA), Rubella;
- d. Kelas D: Resiko tinggi terhadap individu (high individual risk) dan terhadap kesehatan publik tinggi (high public health risk), Contoh: Skrining HIV darah donor, diagnosa darah HIV.

Berdasarkan sifat pengantaran arus listrik, dikenal Alkes Elektromedik, yaitu perangkat atau instrument medis yang berhubungan dengan sistem elektronik arus lemah. Digolongkan atas 5 (lima) kelompok, yaitu:

1. Alkes Elektromedik Radiasi adalah jenis alat kesehatan yang dalam pengoperasiannya menggunakan arus listrik AC ataupun DC dan memancarkan zat radioaktif atau radiasi pengion selama digunakan untuk mencapai tujuan dari penggunaan. Contoh: General X-Ray, Dental X-Ray, Panoramic.
2. Alkes Elektromedik Non Radiasi adalah jenis alat kesehatan yang dalam pengoperasiannya menggunakan arus listrik AC ataupun DC, namun tidak memancarkan zat radioaktif atau radiasi pengion selama digunakan untuk mencapai tujuan dari penggunaan. Contoh: Ultrasonografi (USG), Electro Encephalo Graph (EEG).
3. Alkes Non Elektromedik Steril adalah jenis alat kesehatan yang dalam penggunaannya tidak memerlukan arus listrik AC ataupun DC dimana sebelumnya telah mengalami proses sterilisasi pada saat produksinya dan merupakan produk steril. Contoh: disposable/jarum suntik, kassa steril, benang bedah, Intra Vena (IV) Catheter, Infusion set.

4. Alkes Non Elektromedik Non Steril adalah jenis alat kesehatan yang dalam penggunaannya tidak memerlukan arus listrik AC ataupun DC dimana sebelumnya tidak mengalami proses sterilisasi pada saat produksinya dan bukan merupakan produk steril. Contoh: Plester, Instrument Bedah, timbangan bayi, kursi roda manual.
5. Produk Diagnostik In Vitro (DIV) adalah jenis alat kesehatan yang digunakan pada saat pemeriksaan *spesimen* yang berasal dari tubuh manusia secara invitro yang menyediakan informasi sebagai pemantauan, diagnose ataupun keduanya, termasuk reagen, penampung spesimen, kalibrator, bahan control, software, dan atau atau bahan kimia lain yang diperlukan. Contoh: Virus Transport Medium (VTM), alat untuk mengecek kadar Gula Darah (Glukocheck), Hematology Analyzer, Alat Tes Kimia Klinik, Rapid test (Rapid Test COVID-19, HIV, Malaria, Narkoba, Sipilis) dan Test Pack Kehamilan.

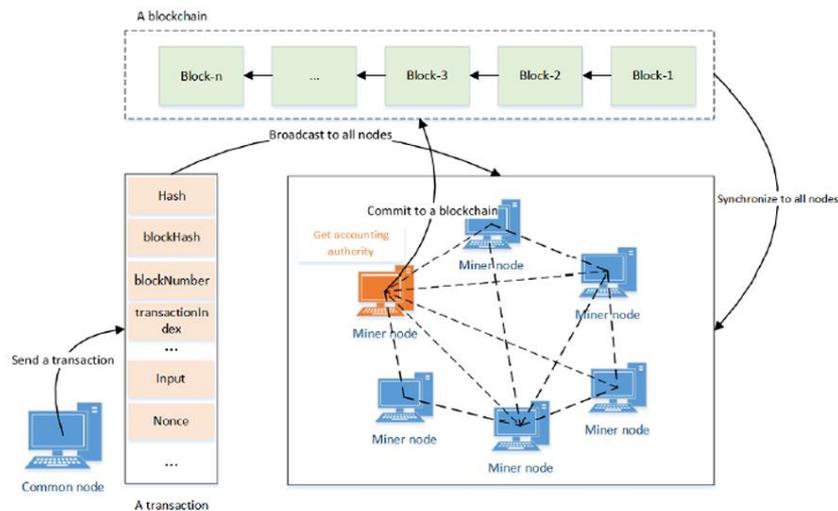
### **2.3 Blockchain**

Teknologi *blockchain* awalnya dikembangkan pada Bitcoin (Nakamoto 2008), yaitu sistem pembayaran elektronik pada jaringan *peer-to-peer* yang bersifat terdesentralisasi tanpa adanya institusi finansial yang bertindak sebagai pengatur jalannya transaksi. *Blockchain* ini diterapkan untuk menghilangkan kebutuhan institusi finansial sebagai pihak ketiga dalam pengelolaan suatu proses transaksi. *Blockchain* pada dasarnya merupakan basis data transaksi yang terdistribusi pada berbagai node yang tergabung dalam suatu jaringan *peer-to-peer*. *Blockchain* merupakan salah satu bentuk dari *Distributed Ledger Technology* (DLT), dimana teknologi ini bersifat terdesentralisasi dan memiliki protokol konsensus yang digunakan untuk mencapai kesepakatan bersama dalam proses pengelolaan basis data yang ada. Akan tetapi, terdapat suatu perbedaan pada *blockchain* jika dibandingkan dengan DLT pada umumnya. Perbedaan ini terletak di struktur basis data yang ada pada *blockchain*, dimana setiap data transaksi yang tercatat akan tergabung ke dalam suatu *block* yang saling terhubung antara satu sama lain dan tidak dapat mengalami perubahan. (Hileman and Rauchs 2017).

Pencatatan data pada teknologi *blockchain* dilakukan melalui beberapa tahap, yaitu :

1. Node akan melakukan transaksi data menggunakan digital signature dan kemudian akan mengumumkannya ke jaringan. *Digital signature* merupakan tanda pengenal yang digunakan oleh suatu node dalam jaringan *blockchain*.
2. Node lain yang tergabung dalam jaringan akan menerima pengumuman transaksi dan kemudian menggabungkannya ke dalam suatu *block* baru.
3. Node penerima akan melakukan eksekusi pembentukan *block* berdasarkan protokol konsensus yang ditetapkan, seperti *Proof of Work*. Pembentukan *block* ini dikenal dengan istilah mining.
4. Setelah node penerima berhasil membentuk *block* baru berdasarkan protokol yang ditetapkan, selanjutnya *block* baru ini akan diumumkan ke jaringan sehingga dapat ditambahkan ke rantai *block* yang ada.

Pada *blockchain* sistem Bitcoin (Nakamoto 2008), setelah transaksi mata uang digital (cryptocurrency) dilakukan oleh suatu node menggunakan digital signature-nya, node tersebut selanjutnya akan mengumumkan transaksi yang terjadi ke jaringan. Node lain kemudian akan menerima pengumuman transaksi-transaksi yang terjadi dan menggabungkannya dengan membentuk *block* menggunakan mekanisme protokol Proof of Work. Mekanisme *Proof of Work* akan membentuk suatu *block* baru yang terhubung ke *block* terakhir pada rantai *block* yang ada menggunakan fungsi hash kriptografi, seperti SHA-256. Block dibentuk dengan cara menghitung nilai hash-nya. Nilai hash ini biasa disebut sebagai *block* hash atau *block* header. Block hash akan didapatkan melalui komputasi fungsi hash dari nilai data transaksi yang tergabung dalam *block* dan beberapa nilai khusus, seperti timestamp, *nonce*, ataupun *block* hash dari *block* terakhir yang sebelumnya terbentuk pada rantai *block*. Hubungan antara suatu *block* dan *block* lainnya akan terbentuk dengan adanya penggunaan nilai *block* hash terakhir sebagai nilai masukan (input) dalam pembentukan nilai *block* hash baru. Ilustrasi *blockchain* dapat dilihat pada Gambar 4..

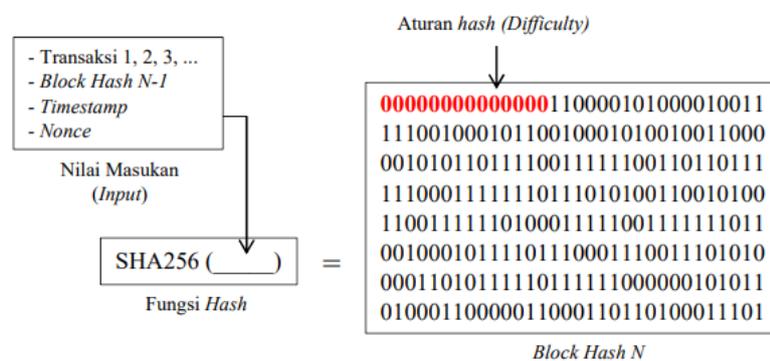


Gambar 4. Ilustrasi *Blockchain*

Iterasi tahapan dari transaksi di dalam blockchain adalah sebagai berikut :

- A. Semua node harus berada di dalam jaringan P2P. Jika node mengirim transaksi ke blockchain, nodes lainnya akan menerima transaksi tersebut.
- B. Semua *nodes* yang menerima transaksi perlu melakukan pengecekan apakah transaksi tersebut merupakan transaksi yang legal, lalu memasukkan transaksi itu ke *transactions pool*.
- C. Semua *nodes* '*miner*' menyelesaikan proses *accounting* terhadap transaksi tersebut berdasarkan algoritma konsensus yang diterapkan.
- D. Setelah transaksi berhasil dieksekusi oleh node miner yang terpilih, maka salinan dari block akan dikirimkan ke seluruh jaringan, lalu nodes melakukan verifikasi apakah nodes tersebut legal atau tidak.
- E. Jika block telah dikonfirmasi, maka transaksi tersebut akan ditambahkan ke dalam blockchain, dan semua nodes akan menyimpan salinan dari blockchain tersebut (Li & Han, 2019)

Protokol konsensus Proof of Work merupakan mekanisme yang digunakan jaringan *blockchain* untuk mencapai kesepakatan bersama dalam pembentukan *block* data yang valid. Kesepakatan didapatkan berdasarkan besar komputasi yang digunakan dalam suatu proses pembentukan *block*. Proof of Work ini dapat diartikan sebagai bukti penggunaan komputasi yang besar dalam proses pembentukan suatu *block*. Dalam mekanisme protokol Proof of Work, terdapat aturan yang perlu dipenuhi dalam perhitungan *block* hash dari suatu *block* baru. Aturan ini biasa disebut sebagai *difficulty*. *Difficulty* mengharuskan nilai dari suatu *block* hash memiliki beberapa angka nol pada bit awalnya. Dalam perhitungan nilai *block* hash yang sesuai berdasarkan *difficulty*, nilai masukan *nonce* merupakan kunci utama dalam penyelesaiannya. *Nonce* adalah nilai masukan yang ditentukan oleh node dalam melakukan komputasi *block* hash. Penggunaan nilai masukan yang dinamis seperti *nonce* akan dibutuhkan untuk mendapatkan *block* hash yang sesuai berdasarkan *difficulty* yang ditetapkan. Nilai *nonce* dibutuhkan oleh node dalam komputasi *block* hash karena nilai masukan lain seperti data utama, timestamp, ataupun *block* hash dari *block* sebelumnya memiliki nilai yang tetap. Gambaran komputasi *block* hash dapat dilihat pada Gambar 6.



Gambar 5. Komputasi *Block Hash*

Fungsi hash kriptografi seperti SHA-256 akan menghasilkan nilai hash yang sangat tidak terduga dan bersifat satu arah. Dengan kata lain, hash yang terbentuk tidak dapat terdekripsi untuk mendapatkan nilai masukan awal yang digunakan pada fungsinya. *Block* hash yang memenuhi kriteria *difficulty* yang ditetapkan hanya dapat dihasilkan dengan cara menjalankan fungsi hash secara berulang kali menggunakan *nonce* yang berbeda. Node akan saling berkompetisi dalam

membentuk suatu *block* dengan cara mencari *nonce* yang sesuai sehingga *block* hash yang didapatkan dapat memenuhi kriteria *difficulty*. Proses ini akan membutuhkan komputasi yang besar. Dengan demikian, didaptkannya nilai *nonce* yang sesuai dapat menjadi bukti bahwa pembentukan *block* telah melalui proses komputasi yang besar. *Block* yang terbentuk dengan nilai *nonce* yang sesuai akan dianggap oleh jaringan sebagai *block* yang valid.

Umumnya, berdasarkan protokol *blockchain* yang ditetapkan, ketika suatu *block* berhasil dibentuk oleh suatu node, node tersebut akan mendapatkan hadiah berupa *cryptocurrency*. Akan tetapi, karena proses pembentukan *block* ini membutuhkan komputasi yang besar, node memiliki pilihan untuk melakukannya atau tidak. Node yang melakukan pembentukan *block* dikenal dengan istilah *miner*.

Ketika *miner* telah menemukan *nonce* yang sesuai, selanjutnya *block* yang dibentuk akan diumumkan ke seluruh node yang tergabung dalam jaringan. Seluruh node akan melakukan verifikasi terkait pembentukan *block* hanya dengan sekali menjalankan fungsi hash menggunakan nilai masukan yang telah didapatkan oleh *miner*. Apabila *block* yang terbentuk sesuai berdasarkan protokol yang ditetapkan, maka *block* tersebut akan dimasukkan ke dalam rantai *block* yang sudah ada.

Teknologi *blockchain* terus berkembang dan telah dikenal secara umum sebagai *framework* dalam pengembangan sistem yang bersifat terdesentralisasi (Gao, Hatcher and Yu 2018). Setiap pengembangan sistem terdesentralisasi akan menerapkan *blockchain* dengan berbagai jenis perubahan berdasarkan kebutuhan yang ada. Perubahan ini mencakup jenis protokol konsensus yang digunakan, implementasi konsep teknologi lain, mekanisme pencatatan data, dan sebagainya.

Dengan penerapan *framework blockchain* pada suatu sistem, berbagai keuntungan dapat tercapai (Sarmah 2018). Keuntungan-keuntungan yang didapatkan antara lain sebagai berikut:

- a. Sistem akan bersifat terdesentralisasi, dimana pengelolaan sistem dilakukan tanpa adanya otoritas yang terpusat.
- b. Pengguna akan memiliki wewenang untuk berpartisipasi dalam melakukan pengelolaan data yang ada.
- c. Data dapat tersedia secara konsisten, lengkap, dan terkini karena tersebar pada setiap node yang tergabung dalam jaringan sistem.

- d. Dikarenakan tidak adanya wewenang yang terpusat, pengguna dapat yakin bahwa data akan dieksekusi berdasarkan mekanisme dari protokol yang ada.
- e. *Blockchain* memberikan kekekalan pada setiap datanya sehingga data yang telah tercatat tidak dapat termanipulasi.
- f. Data yang tercatat dapat terlindungi karena terenkripsi menggunakan mekanisme dari protokol *blockchain*.
- g. Sistem memiliki kekebalan pada berbagai jenis serangan (cyber attack) karena dibangun menggunakan jaringan peer-to-peer. Jaringan sistem dapat beroperasi secara normal walaupun terdapat node yang tidak aktif akibat dari suatu serangan.

Dengan adanya arsitektur yang sangat kompleks dan integrasi berbagai macam teknologi yang diterapkan sehingga dapat menimbulkan bermacam-macam keuntungan, teknologi *blockchain* memiliki bidang penerapan yang luas (Gao, Hatcher and Yu 2018). Penerapan-penerapan ini dapat dilihat pada Tabel 1.

Tabel 1. Bidang Aplikasi *Blockchain*

<b>Bidang Aplikasi</b>	<b>Deskripsi</b>
<i>Internet of Things (IoT)</i>	Sistem IoT dengan skala yang besar dapat dikembangkan secara terdesentralisasi dengan jaringan peer-to-peer menggunakan <i>blockchain</i> . Sifat terdesentralisasi dan dengan adanya protokol <i>blockchain</i> yang diterapkan dapat memberikan proteksi pada sistem IoT dari serangan yang umumnya terjadi pada sistem yang terpusat.
<i>Big Data</i>	<i>Blockchain</i> dianggap mampu memberikan solusi pada permasalahan manajemen data dalam sistem big data seperti proteksi data personal ataupun properti digital. Keandalan dan keamanan yang lebih dalam proses pencatatan data merupakan manfaat yang dapat diberikan oleh <i>blockchain</i> pada sistem big data.

<i>Cloud &amp; Edge Computing</i>	Proteksi data merupakan alasan utama penerapan <i>blockchain</i> dalam sistem cloud ataupun edge computing. Data yang tercatat menggunakan mekanisme <i>blockchain</i> tidak dapat termanipulasi sehingga kredibilitas data dalam sistem cloud/edge computing dapat terjaga.
Manajemen Identitas	Dalam bidang ini, <i>blockchain</i> memberikan kemampuan dalam membentuk suatu identitas menggunakan digital signature. Digital signature akan digunakan sebagai tanda untuk memverifikasi kebenaran suatu identitas.
Finansial & <i>Cryptocurrency</i>	Teknologi <i>blockchain</i> awalnya dikembangkan pada bidang finansial. <i>Blockchain</i> memberikan kemungkinan dalam membentuk suatu sistem transaksi yang terdesentralisasi, dimana kebutuhan akan pihak ketiga sebagai pengelola transaksi dapat dihilangkan.
<i>Smart Contract &amp; Otomatisas</i>	<i>Smart contract</i> pada dasarnya merupakan kode-kode yang dibentuk untuk menjalankan suatu logika bisnis. <i>Smart contract</i> dapat dikembangkan menggunakan <i>blockchain</i> sehingga logika bisnis yang ada dapat dijalankan secara otomatis dengan menggunakan jaringan yang terdesentralisasi.
<i>Supply Chain</i>	Pada rantai pasok ( <i>supply chain</i> ), terdapat berbagai entitas tergabung dalam prosesnya sehingga permasalahan kepercayaan menjadi hal utama di dalamnya. <i>Blockchain</i>

Informasi Medis	<p>memberikan solusi dalam memastikan integritas data pada sistem rantai pasok.</p> <p>Dikarenakan informasi medis bersifat pribadi dan sensitif, <i>blockchain</i> dapat diimplementasikan dalam mengelola aksesibilitas data sehingga pihak yang memiliki wewenang saja yang dapat melihat dan melakukan penyimpanan.</p>
Komunikasi & Jaringan	<p><i>Blockchain</i> memberikan proteksi dalam proses komunikasi yang terjadi pada suatu jaringan menggunakan digital signature sebagai metode dalam melakukan verifikasi kebenaran identitas.</p>

---

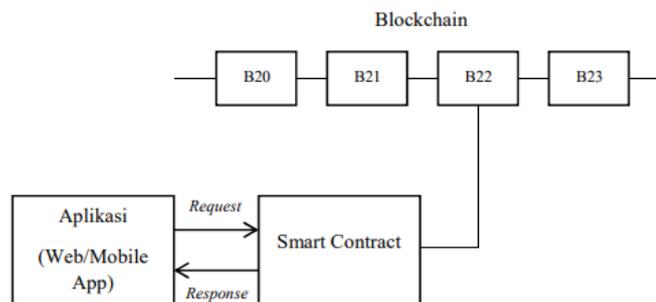
## 2.4 *Smart Contract*

Kontrak pada dasarnya merupakan cara untuk membentuk kesepakatan persetujuan terhadap suatu hal (Szabo 1996). Kontrak secara umum digunakan untuk keperluan dalam membangun protokol persetujuan terhadap suatu hubungan yang dibentuk oleh dua pihak individu/kelompok atau lebih. Kontrak akan dibentuk oleh dua pihak atau lebih dengan menggunakan bantuan supervisi dari pihak ketiga yang dianggap terpercaya. Supervisi ini sangat penting dimiliki untuk menghindari adanya manipulasi oleh salah satu pihak terhadap kontrak yang dibentuk. Seiring dengan perkembangan teknologi, terbentuk suatu konsep kontrak baru yang dinamakan dengan *smart contract*.

*Smart contract* pada dasarnya merupakan perangkat lunak berisi protokol kesepakatan dan hubungan antara dua pihak atau lebih yang dikelola menggunakan sistem terdesentralisasi. Pengawasan terhadap kesepakatan dan hubungan yang terbentuk akan dilakukan oleh semua pihak yang tergabung dalam jaringan berdasarkan protokol konsensus sistem sehingga kebutuhan supervisi dari suatu pihak ketiga tidak diperlukan. *Smart contract* memungkinkan adanya pengembangan yang lebih pada teknologi *blockchain* karena kedua teknologi pada dasarnya diterapkan pada ekosistem yang sama, yaitu dibangun dengan

menggunakan jaringan terdesentralisasi. *Blockchain* yang pada awalnya hanya digunakan untuk melakukan proses komputasi sederhana, seperti pencatatan data transaksi, telah dapat dikembangkan untuk melakukan proses komputasi yang lebih kompleks dengan integrasi *smart contract* (Jani 2020).

Kombinasi dari teknologi *blockchain* dan *smart contract* ini dinamakan *decentralized application*. Arsitektur *decentralized application* dapat dilihat pada Gambar 2.4.



Gambar 6. Arsitektur DApp (*Decentralized Application*)

*Decentralized application*, bekerja dengan tiga komponen utama, yaitu aplikasi klien, *smart contract*, dan *blockchain*. Aplikasi klien dapat berupa aplikasi web ataupun mobile yang memiliki kemampuan untuk berkomunikasi dengan *smart contract* melalui *application programming interface* (API). *Smart contract* sendiri akan bekerja layaknya seperti aplikasi server-side (back-end). *Smart contract* tersimpan pada *blockchain* yang tersebar di setiap node yang tergabung dalam jaringan terdesentralisasi. *Smart contract* akan dieksekusi berdasarkan permintaan yang dikirim oleh aplikasi klien dan hasilnya akan dikembalikan dalam bentuk respon data. (Sayeed, Marco-Gisbert and Caira 2020).

## 2.5 Ethereum

Terdapat beberapa macam platform yang menggunakan jaringan *blockchain*. Salah satunya yaitu ethereum. Ethereum merupakan platform *open-source* yang bisa digunakan untuk membangun aplikasi terdistribusi dan terdesentralisasi pada jaringan *blockchain* (Pănescu and Manta 2018). *Blockchain* ethereum adalah platform komputasi open source yang memproses program yang disebut dengan *smart contract* (Mutar and AL-Huseiny 2019). *Smart contract* memungkinkan

pengguna untuk membuat sistem apapun yang mereka inginkan tidak hanya terbatas pada *cryptocurrencys* saja, cukup dengan menulis logika dalam beberapa baris kode (Buterin 2014). Dengan menggunakan *smart contract* pengguna dapat menulis program apapun pada jaringan *blockchain*. Penerapan *smart contract* yang paling terkenal adalah pada jaringan *blockchain* ethereum. *Smart contract* akan berjalan mandiri setelah *smart contract* tersebut dijalankan. Bahkan pembuatnya tidak dapat menghentikannya atau memodifikasinya. Sehingga akan meminimalkan peluang human error (Yuan et al. 2018). Untuk mencegah pengembang menulis kontrak pintar yang tidak efisien atau berat, ada biaya 'gas' yang dikenakan pada setiap perintah penyimpanan dan pengambilan yang dilakukan. Gas tersebut berupa ether (ETH). Sama seperti user *blockchain* yang memiliki alamat, status *smart contract* juga berada pada alamat unik tertentu pada jaringan global ethereum yang dapat dipanggil oleh user atau node. Jika pengguna tidak memiliki cukup gas sebagai biayanya, panggilan kontrak dan transaksi tersebut tidak dapat diselesaikan (Gürsoy et al. 2020).

Sebelum adanya *blockchain*, penyimpanan data biasanya dilakukan secara tercentralisasi dalam sebuah database pada sebuah server pusat yang memiliki resiko terkait keamanan data yang tersimpan karena kita tidak mengetahui bagaimana pengelolaannya. Tetapi dengan menggunakan *blockchain* khususnya *Blockchain* ethereum, data tersebut bisa dilihat oleh semua node ketika jaringan *blockchain* tersebut masih ada dan node tersebut terhubung dengan jaringan *blockchain* tersebut. Selain itu, dengan tidak menggunakan server pusat, melainkan server dipecah ke semua node yang terhubung sehingga node berperan sebagai client sekaligus servernya sendiri, sehingga akan mengurangi resiko dari pencurian data dan keamanan data akan terjaga (Buterin 2014). Sistem penyimpanan data terdesentralisasi pada *blockchain* juga sekaligus menjadi backup untuk menjaga data semisal ada salah satu jaringan yang crash, sehingga data tidak hilang karena data sudah tersimpan dan disalin ke setiap node yang terhubung. Namun kurangnya privasi menjadi salah satu masalah yang dihadapi jika dalam sebuah kasus membutuhkan tingkat privasi yang tinggi, karena transparansi itu sendiri merupakan salah satu keunggulan yang ditawarkan *blockchain* ethereum dimana transparansi merupakan lawan kata dari privasi (Yuan et al. 2018).

Ethereum mempunyai runtime environment yang bernama Ethereum Virtual Machine (EVM). Virtual Machine pada dasarnya merupakan sebuah lapisan antara kode yang dieksekusi dan mesin yang dijalankan. EVM berfungsi untuk menjalankan *smart contract* yang dibuat menggunakan ethereum. *Smart contract* dapat ditulis dengan bahasa pemrograman seperti solidity. Kemudian kode program *smart contract* akan dieksekusi oleh EVM dan di deploy ke jaringan ethereum.

Ethereum memiliki mata uang kriptonya sendiri yaitu Ether (ETH). Mirip dengan bitcoin, ether merupakan sebuah *cryptocurrency* yang mempunyai nilai jual. Salah satu tujuan penggunaan ether adalah sebagai biaya yang diperlukan untuk bergabung dalam jaringan ethereum tersebut. Biaya ether yang diperlukan pada pengoperasian aplikasi yang dijalankan disebut dengan gas (Pănescu and Manta 2018). Penggunaan ether sebagai biaya pemrosesan dapat mencegah terjadinya serangan DoS seperti meminta pemrosesan beberapa loop tak terbatas dalam *smart contract*. Ethereum memberikan harga tetap atau biaya pada setiap operasi termasuk komputasi atau transfer data berupa ether atau yang dalam hal ini disebut sebagai gas. Sehingga pada kasus DoS yang meminta untuk memproses loop tak terbatas, itu akan menghabiskan gas. Saat suatu fungsi kehabisan gas, fungsi tersebut akan dibatalkan dan semua perubahan status yang disebabkan oleh fungsi tersebut akan dikembalikan ke status sebelum panggilan dilakukan tanpa mengembalikan gas apa pun (Yuan et al. 2018).

### **2.5.1. Account**

*Account* merupakan tanda pengenal (identitas) dari suatu entitas, seperti pengguna, node, ataupun *smart contract*, yang tergabung dalam Ethereum. *Account* pada Ethereum terbagi menjadi dua jenis, yaitu *externally owned account* dan *contract account* (Kasireddy 2017). *Externally owned account* pada dasarnya merupakan akun yang dimiliki oleh pengguna ataupun node. Sementara *contract account* merupakan tanda pengenal dari suatu *smart contract* yang tercatat dalam Ethereum. Pada dasarnya, hanya *externally owned account* yang dapat memulai mengirim pesan ke *account* lainnya dengan cara membuat dan menandatangani transaksi menggunakan digital signature berupa private key, sementara *contract account* hanya bisa melakukan transaksi sebagai bentuk respon apabila telah

menerima suatu transaksi dari *account* lain. *Account* merupakan obyek yang membentuk state pada Ethereum. Setiap *account* memiliki alamat (address) dan terdiri dari empat komponen state (Wood 2019), berupa:

- a. *nonce*, merupakan nilai yang merepresentasikan jumlah transaksi yang telah dilakukan oleh suatu *account*.
- b. *balance*, merupakan jumlah *cryptocurrency* Ethereum (Ether) yang dimiliki oleh suatu *account*.
- c. *storageRoot*, merupakan root hash dari konten-konten milik suatu *account* yang tersimpan. Secara default, *storageRoot* memiliki nilai kosong.
- d. *codeHash*, merupakan *hash* dari kode yang dimiliki oleh suatu *account* yang akan dieksekusi oleh *Ethereum Virtual Machine* (EVM). Pada *contract account*, *codeHash* merupakan hash dari kode *smart contract* yang dibentuk. Sementara pada *externally owned account*, *codeHash* merupakan *hash* dari *string* yang bernilai kosong

### 2.5.2. Transaksi

Pada dasarnya, transaksi merupakan suatu instruksi yang dihasilkan oleh *externally owned account*. Transaksi akan dihasilkan dengan menggunakan digital signature yang berbasis *public/private key* milik *externally owned account*. Setiap transaksi yang dihasilkan akan tercatat ke dalam *blockchain* Ethereum.

Transaksi dalam Ethereum terbagi menjadi dua jenis, yaitu *message call* dan *contract creation* (Kasireddy 2017). *Message call* merupakan transaksi yang dilakukan dalam melakukan suatu perubahan state. *Contract creation* merupakan transaksi yang dilakukan untuk membentuk *contract* baru.

Setiap proses komputasi yang dibutuhkan untuk memproses suatu transaksi dalam Ethereum akan dieksekusi oleh node miner. Miner akan membutuhkan sebuah bayaran sebagai bentuk hadiah dalam mengeksekusi proses komputasi dari suatu transaksi. Biaya pemrosesan ini dibayar oleh *account* selaku pengirim transaksi berdasarkan unit khusus dalam Ethereum yang dinamakan gas (Kasireddy 2017). Gas pada dasarnya merupakan satuan unit yang digunakan untuk mengukur besar komputasi yang dibutuhkan dari suatu transaksi.

Penentuan biaya transaksi akan diukur dengan menggunakan dua variabel yaitu *gasPrice* dan *gasLimit*. *gasPrice* merupakan jumlah Ether yang pengirim transaksi bersedia bayar untuk penggunaan satu gas dalam proses komputasi transaksi. Sementara *gasLimit* merupakan jumlah maksimum gas yang akan dipakai dalam proses komputasi transaksi. Kedua variabel ini akan ditentukan oleh pengirim transaksi. Sebagai contoh, pengirim transaksi menentukan *gasLimit* sebesar 50000 dan *gasPrice* sebesar 20 Gwei (1 Ether = 1000000000 Gwei) sehingga menghasilkan biaya transaksi sebesar  $50000 \times 20 \text{ Gwei} = 1000000 \text{ Gwei} = 0.0001 \text{ Ether}$ .

Adapun komponen-komponen yang terdapat dalam transaksi dapat dilihat pada Tabel 2.

Tabel 2. Parameter pada Transaksi *Blockchain*

Parameter	Deskripsi
<i>nonce</i>	Nomor transaksi yang ditentukan berdasarkan jumlah transaksi yang telah dilakukan oleh <i>account</i> pengirim transaksi.
<i>gasPrice</i>	Jumlah Ether yang ditentukan oleh pengirim transaksi untuk membayar setiap unit gas yang digunakan dalam proses eksekusi transaksi.
<i>gasLimit</i>	Jumlah maksimum unit gas yang dapat digunakan dalam proses eksekusi transaksi. <i>gasLimit</i> akan ditentukan oleh pengirim transaksi.
<i>from</i>	<i>Address</i> dari <i>account</i> pengirim transaksi.
<i>to</i>	<i>Address</i> dari <i>account</i> penerima transaksi.
<i>value</i>	Jumlah Ether yang akan ditransfer dari pengirim transaksi ke penerima transaksi.
<i>v, r, s</i>	Digunakan untuk menghasilkan digital signature sebagai pengidentifikasi pengirim transaksi.
<i>init</i>	Sebuah bagian kode Ethereum Virtual Machine (EVM) yang digunakan untuk menginisialisasi

	contract account baru. Nilai ini hanya ada pada transaksi jenis contract creation.
data	Input yang akan digunakan untuk mengubah suatu state pada Ethereum. Nilai ini hanya ada pada transaksi jenis message call.

---

### 2.5.3. Block

Block pada Ethereum terdiri dari tiga bagian, yaitu *block* header, informasi transaksi-transaksi yang tergabung dalam *block*, dan kumpulan *block* header dari ommer, yaitu stale *block* yang terbentuk secara bersamaan dengan *block* yang tervalidasi. (Kasireddy 2017)

Pada Ethereum, ommer dipertimbangkan sebagai salah satu penunjang mekanisme *blockchain* agar dapat berjalan dengan baik. Hal tersebut dikarenakan Ethereum memiliki waktu pembentukan *block* yang lebih cepat (15 detik) dibanding *blockchain* lain seperti Bitcoin (10 menit). Semakin cepat waktu pembentukan *block* pada suatu *blockchain* maka semakin besar juga persaingan yang ada dalam proses pembentukan *block*.

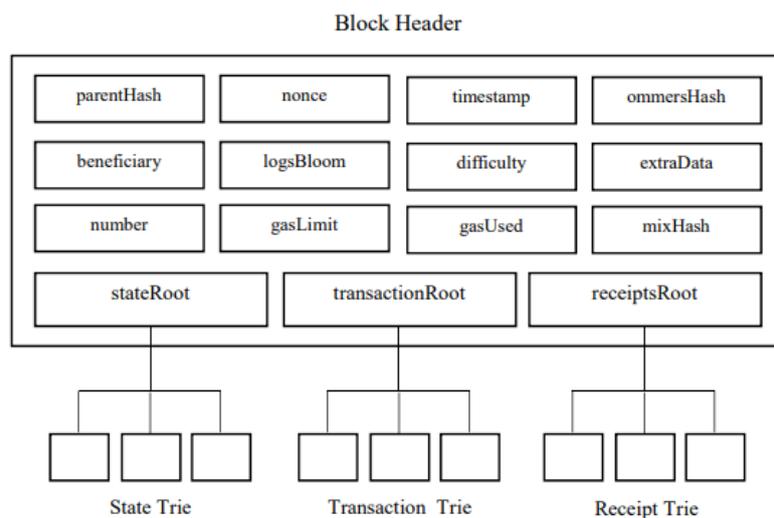
Protokol *blockchain* pada umumnya hanya memberikan hadiah kepada miner yang melakukan pembentukan *block* yang tervalidasi. Pada protokol yang diterapkan Ethereum, miner yang membentuk ommer juga akan mendapatkan hadiah, walaupun jumlahnya tidak sebanyak hadiah *block* tervalidasi. Dengan demikian, insentif miner dapat bertambah dalam melakukan pembentukan *block*.

Block dalam Ethereum pada dasarnya mirip seperti *block* dalam Bitcoin, hanya saja berisi tambahan informasi khusus berdasarkan protokol yang ditetapkan. Setiap informasi yang ada akan tergabung dan membentuk *block* header. Informasi-informasi yang terdapat pada *block* header dari suatu *block* yaitu (Wood 2019):

- a. *parentHash*: hash dari *block* header milik *parent block*, yaitu *block* terakhir sebelum *block* terkait.
- b. *ommersHash*: hash dari daftar *ommer block* terkait.
- c. *beneficiary*: *address* dari *account* yang menerima biaya pembayaran dalam proses *mining block* terkait.
- d. *stateRoot* : *hash* dari *state* yang tersimpan pada *block* terkait.

- e. *transactionRoot* : *hash* dari transaksi yang tercatat pada *block* terkait.
- f. *receiptsRoot* : *hash* dari resi transaksi yang tercatat pada *block* terkait.
- g. *logsBloom* : struktur data *bloom filter* yang terdiri atas *log/catatan* informasi.
- h. *difficulty*: tingkat *difficulty* dari penyelesaian *block* terkait.
- i. *number*: nilai penjumlahan (*count*) dari *block* terkait.
- j. *gasLimit*: batas maksimum gas yang dapat digunakan dalam pemrosesan komputasi transaksi pada *block* terkait.
- k. *gasUsed*: jumlah total gas yang digunakan pada pemrosesan komputasi transaksi dari *block* terkait.
- l. *timestamp*: *timestamp* yang berbasis unix dari pembentukan *block* terkait.
- m. *extraData*: data ekstra yang berhubungan dengan *block* terkait.
- n. *mixHash*: sebuah *hash*, yang jika dikombinasikan dengan *nonce*, akan membuktikan bahwa *block* terkait telah dibentuk melalui proses komputasi yang cukup.
- o. *nonce*: sebuah *hash*, yang jika dikombinasikan dengan *mixHash*, akan membuktikan bahwa *block* terkait telah dibentuk melalui proses komputasi yang cukup.

Ilustrasi *block header* dari suatu *block* pada Ethereum dapat dilihat pada Gambar 2.5.



Gambar 7. *Block Header*

#### 2.5.4. Eksekusi Transaksi

Eksekusi transaksi dalam Ethereum pada dasarnya mengacu pada proses transisi state yang ada (Wood 2019). Sebelum transaksi dieksekusi, terdapat beberapa syarat yang harus dipenuhi terlebih dahulu, yaitu :

1. Transaksi harus memiliki format yang sesuai. Format *Recursive Length Prefix* (RLP) merupakan format data yang diterima oleh Ethereum.
2. *Signature* transaksi yang valid.
3. *Nonce* transaksi yang valid.
4. *gasLimit* transaksi harus memiliki jumlah yang lebih besar atau sama dengan jumlah gas yang terpakai dalam eksekusi komputasi transaksi.
5. Jumlah Ether yang dimiliki oleh pengirim transaksi dapat menutupi biaya pemakaian gas yang terbentuk berdasarkan perhitungan *gasLimit* dan *gasPrice* yang ditentukan.

Apabila syarat-syarat yang diperlukan telah terpenuhi, selanjutnya eksekusi transaksi dapat dilakukan. Eksekusi transaksi secara umum akan dilakukan melalui tahap-tahap sebagai berikut:

1. Biaya transaksi akan diukur berdasarkan *gasLimit* dan *gasPrice* yang ditentukan. Ether pengirim transaksi akan terpotong berdasarkan hasil perhitungan biaya transaksi tersebut.
2. Menginisialisasi jumlah gas yang akan digunakan selama proses komputasi transaksi.
3. Komputasi-komputasi yang diperlukan akan dieksekusi pada *Ethereum Virtual Machine* (EVM) oleh *miner*.
4. Ketika komputasi yang diperlukan oleh transaksi telah terproses, maka biaya yang terbayar untuk sisa gas yang tidak terpakai akan dikembalikan ke pengirim transaksi. Disaat yang bersamaan, biaya gas yang terpakai akan dikirim ke *miner*.
5. *State* baru dan logs yang berisi catatan transaksi yang terjadi akan terbentuk.

### 2.5.5. Arsitektur Blockchain

Ethereum memiliki arsitektur *blockchain* yang hampir sama dengan *blockchain* Bitcoin. Perbedaannya terletak pada informasi yang tersimpan pada *block* dan algoritma yang dipakai pada pembentukan *Proof of Work*. Pada *block* Ethereum, selain daripada transaksi, *state* terbaru juga akan disimpan. Sementara itu, algoritma *Proof of Work* yang digunakan pada Ethereum dinamakan *Ethash*.

Algoritma *Ethash* secara formal didefinisikan pada Persamaan 1.

$$(m, n) = \text{PoW}(HN, Hn, d) \quad (1)$$

Pada Persamaan 1, **m** merupakan mixHash, **n** adalah nonce, **HN** diartikan sebagai *block header* dari *block* baru yang terbentuk (tanpa komponen *nonce* dan *mixHash*), **Hn** sebagai nonce dari *block header*, serta **d** yaitu DAG (data set besar). (Wood 2019). Algoritma *Ethash* pada dasarnya akan mencari nilai *mixHash* dan *nonce* yang sesuai berdasarkan *difficulty* yang ditetapkan pada proses pembentukan *block*. Kedua nilai ini merupakan bukti bahwa suatu pembentukan *block* telah melalui proses komputasi yang besar (*Proof of Work*).

## 2.6 Ganache

Ganache merupakan sebuah software aplikasi yang berfungsi untuk menjalankan local jaringan *blockchain* dalam proses pengembangan aplikasi terdesentralisasi berbasis ethereum. Ganache menyediakan sebuah personal *blockchain* yang dapat digunakan untuk membuat, testing, dan deploy *smart contract*. Dengan menggunakan bantuan ganache, proses pengembangan dan testing aplikasi sistem penelusuran berbasis *blockchain* ethereum ini bisa dilakukan tanpa harus menggunakan jaringan *blockchain* ethereum yang asli secara langsung. Dimana dengan menggunakan ganache bisa menghemat biaya dan waktu. Sedangkan jika menggunakan jaringan ethereum *blockchain* secara langsung akan dapat menghabiskan biaya yang tinggi dalam setiap transaksi yang dilakukan untuk mengevaluasi *smart contract*. Dalam banyak kasus, besarnya biaya seringkali tidak dapat diprediksi sehingga dapat menimbulkan kerugian jika terdapat error pada *smart contract*. Untuk mengatasi masalah tersebut ganache dapat membantu dalam

proses testing *smart contract* pada jaringan local *blockchain* ethereum. Sehingga dapat menghindari kerugian dari biaya transaksi yang tidak diinginkan dalam proses testing dan deploy *smart contract*. Selain itu, dengan menggunakan ganache dapat menghemat waktu, Jika menggunakan jaringan asli *blockchain* ethereum, developer perlu menunggu beberapa saat agar *smart contract* berhasil di deploy ke jaringan *blockchain* ethereum untuk selanjutnya dilakukan pengetesan. Sedangkan jika menggunakan ganache, proses deploy dan testing dapat dilakukan dengan lebih cepat.

## 2.7 Metamask

Metamask merupakan sebuah crypto wallet atau dompet kripto berbasis ethereum yang berupa browser extension yang dapat menghubungkan pengguna ke jaringan *blockchain* ethereum. Fungsi utama dari metamask adalah untuk menyimpan, membeli, atau mengirim ETH. Selain itu, metamask juga digunakan untuk berinteraksi dengan *blockchain* Ethereum. Dengan menggunakan metamask browsing pada web berbasis *blockchain* ethereum menjadi lebih praktis dan mudah diakses. Untuk melakukan transaksi dengan platform berbasis ethereum, diperlukan memiliki deposit ETH. Jumlah deposit ditentukan sesuai dengan seberapa banyak biaya yang dibutuhkan untuk melakukan transaksi. Semua tindakan yang dilakukan dalam *blockchain* akan dikenakan biaya. Sehingga perlu untuk memiliki deposit yang cukup pada wallet agar dapat melakukan transaksi pada jaringan *blockchain*. Pada penelitian ini metamask digunakan untuk menghubungkan user *account* berupa akun wallet dengan jaringan ethereum *blockchain* agar bisa berinteraksi dengan *smart contract*. Dimana dalam penelitian ini interaksi yang dimaksud yaitu melakukan input penilaian tempat wisata oleh user ke web penilaian tempat wisata berbasis *blockchain* ethereum.