SKRIPSI

IMPLEMENTASI BLOCKCHAIN PADA SISTEM PEREKAMAN NILAI SISWA SMA ATAU SEDERAJAT TINGKAT NASIONAL UNTUK MENCIPTAKAN TRANSPARANSI NILAI SISWA

Disusun dan Diajukan Oleh:

DEA IVANKA MALAHA

D121181008

PROGRAM STUDI SARJANA TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA

2023

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI *BLOCKCHAIN* PADA SISTEM PEREKAMAN NILAI SISWA SMA ATAU SEDERAJAT TINGKAT NASIONAL UNTUK MENCIPTAKAN TRANSPARANSI NILAI SISWA

Disusun dan diajukan oleh

Dea Ivanka Malaha
D121181008

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika
Fakultas Teknik Universitas Hasanuddin
Pada tanggal 8 Maret 2023
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
Dr. Amil Ahmad Ilham, S.T., M.IT.	Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.
NIP 19731010 199803 1 001	NIP 19750313 200912 1 003

Ketua Program Studi,

Prof. Dr. Ir. Indrabayu, S.T., M.T., M. Bus.Sys., IPM., ASEAN. Eng.
NIP 19750716 200212 1 004

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini ;

Nama	: Dea Ivanka Malaha
NIM	: D121181008
Program Studi	: Teknik Informatika
Jenjang	: S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

"Implementasi Blockchain Pada Sistem Perekaman Nilai Siswa Sma Atau Sederajat Tingkat Nasional Untuk Menciptakan Transparansi Nilai Siswa"

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, 9 Maret 2023

ng Menyatakan

Dea Ivanka Malaha

ABSTRAK

DEA IVANKA MALAHA. *Implementasi Blockchain Pada Sistem Perekaman Nilai Siswa Sma Atau Sederajat Tingkat Nasional Untuk Menciptakan Transparansi Nilai Siswa* (dibimbing oleh Amil Ahmad Ilham dan Ady Wahyudi Paundu).

Saat ini, nilai siswa adalah faktor penting untuk kebutuhan studi lanjutan dan karir individu, sehingga rekam jejak nilai siswa perlu diakses dengan mudah dan memiliki transparansi. Sistem yang digunakan oleh sekolah-sekolah menengah atas saat ini mayoritas masih menggunakan sistem manual, yaitu dengan merekap nilai siswa satu persatu menggunakan tools seperti Microsoft Excel. Cara seperti ini rentan terhadap gangguan, seperti komponen data nilai yang hilang ataupun sulit untuk memperoleh detail nilai secara lengkap dikarenakan data hanya bisa diakses oleh guru saja. Berdasarkan situasi tersebut, terdapat kendala dalam mekanisme berbagi data (*sharing*) antar institusi pendidikan yang aman, yaitu transparansi dan integritas data terjaga dengan baik. Sistem perekaman nilai siswa yang dibangun pada penelitian ini memanfaatkan *blockchain* dan integrasi *smart contract* untuk mencapai transparansi dan menjaga integritas data nilai siswa. Sistem ini dibangun menggunakan platform *blockchain* Ethereum dengan integrasi smart cotract menggunakan bahasa pemgrograman Solidity. Hasil implementasi sistem yang dilakukan dapat menyimpan nilai siswa secara local dan on-chain, serta memampukan pihak ketiga untuk melihat nilai siswa secara terbuka dan transparan. Data tercatat secara kronologis dan tidak dapat dimanipulasi karena blockchain bersifat immutable dan terdesentralisasi dengan algoritma konsensus. Meskipun sistem ini menciptakan transparansi nilai, uji performa menunjukkan nilai latency yang lebih tinggi dan throughput yang lebih rendah dibandingkan dengan database lokal.

Kata kunci: sistem perekaman nilai, *blockchain*, *smart contract*, Ethereum

ABSTRACT

DEA IVANKA MALAHA. *Implementation of Blockchain in National-Level High School or Equivalent Student Grade Recording System to Create Transparency in Student Grades* (supervised by Amil Ahmad Ilham and Ady Wahyudi Paundu).

Currently, students' grades are an important factor for their further education and future careers. As such, their grade records need to be easily accessible and transparent. However, many high schools still use a manual system to record each student's grades one by one using tools such as Microsoft Excel. This method is vulnerable to disruptions, such as missing grade data components or difficulty in obtaining complete grade details because the data can only be accessed by teachers. To address this issue, the student grade recording system in this study utilizes blockchain and smart contract integration. By using the Ethereum blockchain platform with smart contract integration using the Solidity programming language, the system achieves both transparency and maintains data integrity. The results of the implemented system can store student grades locally and on-chain, and enable third parties to view student grades openly and transparently. The data is recorded chronologically and cannot be manipulated because the blockchain is immutable and decentralized with consensus algorithms. It is important to note that, while this system creates grade transparency, performance tests show higher latency values and lower throughput compared to local databases. Nonetheless, the system's benefits in terms of transparency and data integrity make it worth considering for educational institutions seeking secure mechanisms for data sharing.

Keywords: student records, student grades, blockchain, smart contract, Ethereum

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

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 *Blockchain* Pada Sistem Perekaman Nilai Siswa SMA atau Sederajat untuk Menciptakan Transparansi Nilai Siswa**" 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 Robert Malaha dan Ibu Hafsah Abu Lias yang selalu menyertai penulis dalam doanya serta mendukung, membantu, memberi semangat serta kasih sayang dalam perjalanan penulis menyelesaikan tugas akhir ini,
3. Saudara penulis, Riza Adella Malaha dan Ryan Malaha atas dukungan dan semangat yang diberikan kepada penulis,
4. Bapak Dr. Amil Ahmad Ilham, S.T., M.IT. selaku pembimbing I dan Bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. selaku pembimbing II, yang senantiasa menyediakan waktu, tenaga, pikiran, dan perhatian dalam mengarahkan penulis untuk menyelesaikan tugas akhir,
5. Segenap Dosen dan Staff Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin yang telah banyak membantu penulis selama masa perkuliahan,
6. Teman-teman Teknik Informatika Angkatan 2018 selaku rekan yang telah memberi bantuan, dukungan dan semangat selama masa perkuliahan dan penyusunan tugas akhir ini,
7. 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, Maret 2023

Penulis,

Dea Ivanka Malaha

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, nilai siswa adalah faktor penting untuk kebutuhan studi lanjutan dan karir individu, sehingga rekam jejak nilai siswa perlu diakses dengan mudah dan memiliki transparansi. Dengan perkembangan teknologi informasi, catatan pendidikan seperti nilai telah dibuat dalam bentuk digital. Tidak seperti arsip fisik, arsip digital disimpan pada media penyimpanan dengan tingkat variasi tinggi, sehingga arsip tersebut tidak dapat dengan mudah dimodifikasi.

Sistem yang digunakan oleh sekolah-sekolah menengah atas saat ini mayoritas masih menggunakan sistem manual, yaitu merekap nilai per komponen capaian mata pelajaran dan menghitungnya di Microsoft Excel, sehingga bisa didapatkan hasil capaian pembelajaran. Untuk laporan hasil akhir siswa juga masih menggunakan cara tradisional dengan menggunakan arsip fisik berupa buku raport. Cara seperti ini rentan terhadap gangguan, seperti komponen data nilai yang hilang ataupun sulit untuk memperoleh detail nilai secara lengkap dikarenakan data hanya bisa diakses oleh pihak tertentu saja. Berdasarkan situasi tersebut, terdapat kendala dalam mekanisme berbagi data (*sharing*) antar institusi pendidikan yang aman, yaitu transparansi dan integritas data terjaga dengan baik. Salah satu contoh kasus adalah pendaftaran mahasiswa baru di perguruan tinggi melalui jalur bebas tes, nilai siswa selama tingkat SMA adalah komponen penting, namun tidak dapat dengan mudah bisa diakses oleh perguruan tinggi, dan tidak adanya transparansi nilai sehingga rentan terjadi manipulasi. Berdasarkan beberapa laporan media massa dalam lima tahun terakhir, setiap tahun selalu terdapat kecurangan dalam SNMPTN karena perbedaan antara data nilai yang tercantum dalam raport dengan yang tercatat dalam Pangkalan Data Sekolah dan Siswa (PDSS). Hal ini berdampak pada pembatalan kelulusan siswa terkait di universitas tujuannya.

Pada penelitian yang dilakukan oleh Satoshi Nakamoto berjudul *Bitcoin: A Peer-to-Peer Electronic Cash System*, Nakamoto memperkenalkan sebuah teknologi yang disebut dengan *blockchain*. *Blockchain* memungkinkan suatu sistem untuk dikembangkan secara desentralisasi sehingga otoritas dari sistem tidak dipegang oleh satu pihak saja, tapi semua entitas di dalam sistem memiliki hak otoritas yang sama. Sifat terdesentralisasi yang dimiliki oleh *blockchain* memberikan dampak signifikan pada properti keamanan dan transparansi dari suatu sistem (Nakamoto, 2008). Menurut (Yaga dkk., 2019), *blockchain* merupakan *ledger* atau buku besar yang terdistribusi dari transaksi yang ditandatangani

secara kriptografi dan dikelompokkan ke dalam blok. Ketika blok baru berhasil dibuat, data pada blok sebelumnya akan hampir mustahil untuk diubah atau dimanipulasi. Hal ini disebabkan salah satunya karena setiap blok memiliki *timestamp*, yaitu informasi mengenai waktu blok tersebut dibuat, sehingga sulit untuk memanipulasinya di kemudian hari. Selain itu, *blockchain* menggunakan *cryptography hash function.*

Blockchain ini sendiri awalnya diperuntukkan untuk transaksi mata uang digital, yang kini dikenal sebagai *cryptocurrency*. Tujuannya adalah untuk membuat biaya pertukaran nilai menjadi rendah dan memiliki *environment* yang aman dalam transaksi *peer-to-peer* dengan siapapun.

Dalam penerapan *blockchain* saat ini, terdapat juga berbagai macam pengembangan, salah satunya adalah integrasi *blockchain* dengan *smart contract*. *Smart contract* adalah bentuk digital dari kontrak tradisional dimana setiap pihak yang terlibat harus mengikuti aturan yang terdapat dalam kontrak (Li & Han, 2019). Dalam *blockchain*, *smart contract* berbentuk perangkat lunak terotomatisasi yang berisi protokol kesepakatan antara kedua pihak atau lebih yang dikelola menggunakan sistem terdesentralisasi.

Seiring dengan perkembangan teknologi, implementasi *blockchain* meluas ke berbagai bidang, salah satunya adalah pendidikan. Penyimpanan rekam nilai siswa adalah salah satu penggunaan teknologi *blockchain* yang makin marak dilakukan. Pemeliharaan rekam nilai tidak mudah karena nilai siswa ada dalam jumlah besar dan ada setiap tahun selama siswa bersekolah. Teknologi *blockchain* dapat digunakan untuk menghemat waktu dan biaya oleh para institusi pendidikan. Penelitian yang dilakukan oleh (Li & Han, 2019) yang berjudul *EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme* memanfaatkan teknologi *blockchain* untuk penyimpanan histori nilai dan pencapaian siswa dalam sebuah institusi pendidikan. Penelitian ini menggunakan Ethereum untuk mengimplementasikan *consortium blockchain* dan *smart contract* untuk mengatur jalannya proses berbagi data antar institusi. Penelitian serupa yang dilakukan oleh (Ocheja dkk., 2019) dengan judul *Managing lifelong learning records through blockchain* mengusulkan sebuah sistem berbasis Ethereum untuk mendaftarkan semua prestasi belajar siswa yang dapat dibagikan secara aman antar institusi dalam satu platform. Sistem ini juga membuat fitur untuk dapat mengatur siapa yang dapat mengakses informasi yang ada di dalam sistem.

Berdasarkan permasalahan yang ada pada sistem perekaman nilai siswa dan pengembangan yang terjadi pada teknologi *blockchain*, maka pada penelitian ini akan dibangun sistem perekaman nilai siswa dengan memanfaatkan penggunaan *blockchain*

untuk menciptakan transparansi dan integritas data nilai, serta integrasi *smart contract* untuk mengatur sistem agar bisa berjalan dengan baik.

1.2 Rumusan Masalah

1. Bagaimana menunjukkan bahwa sistem perekaman nilai siswa tingkat SMA berbasis *blockchain* menciptakan transparansi nilai siswa?
2. Bagaimana membuktikan bahwa sistem perekaman nilai berbasis *blockchain* tidak dapat dimanipulasi?

1.3 Tujuan Penelitian

1. Untuk menciptakan transparansi nilai siswa dengan menggunakan sistem perekaman nilai siswa tingkat SMA berbasis *blockchain*.
2. Untuk membuktikan bahwa sistem perekaman nilai berbasis *blockchain* tidak dapat dimanipulasi.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat membantu:

1. Sekolah, penelitian ini diharapkan dapat digunakan sebagai salah satu opsi untuk menyimpan nilai siswa yang lebih aman secara jangka panjang, dan mempermudah proses berbagi data nilai siswa kepada institusi lain.

1.5 Ruang Lingkup

1. Sekolah diasumsikan memiliki sumber daya untuk menjalankan sistem yang dibuat.

BAB II
TINJAUAN PUSTAKA

2.1 Blockchain

Blockchain awalnya diperkenalkan oleh Satoshi Nakamoto dan dikembangkan dalam Bitcoin (Nakamoto, 2008), yaitu sebuah 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 (Aprialim, 2021.)

Blockchain juga bisa disebut sebagai database terdistribusi, yang menyimpan serangkaian data dalam *block* secara kronologis dengan aman dan tidak dapat diubah (*immutable*) Rangkaian *block* dalam *blockchain* disebut sebagai *ledger*. Isi dari *block* bisa ditentukan sebelumnya ataupun dibuat secara acak oleh *node*s yang ada di dalam *blockchain*. Untuk memastikan keamanan *blockchain* terjamin, mekanisme enkripsi *public key* digunakan agar bisa menjamin konsistensi dan sifat *immutable* dari *ledger* (Turkanović dkk., 2018) Fungsi kriptografi satu arah diterapkan (contoh: SHA256) untuk menjamin anonimitas, *immutability*, dan ukuran *block*.

Perbedaan terbesar antara *blockchain* dan database pada umumnya adalah *blockchain* adalah database yang telah dikembangkan dengan beberapa otomasi di segi penambahan data, validasi, dan distribusi informasi dalam jaringan P2P (Lewis, 2018) Dengan demikian, bisa dikatakan bahwa *blockchain* adalah sebuah struktur data dengan elemen sebagai berikut:

- *data redundant* (setiap *node* memiliki salinan dari *blockchain*),
- melakukan pengecekan terhadap syarat-syarat untuk melakukan transaksi sebelum validasi,
- merekam transaksi dalam bentuk *block*s secara berurutan, yang diatur oleh sebuah algoritma consensus,
- transaksi yang dilakukan berbasis *public key cryptography* dan *transaction scripting language*. (Porru dkk., 2017)

Blockchain memiliki berbagai jenis, yang dibedakan berdasarkan tiga aspek, yaitu aksesibilitas data, partisipasi *node*, dan fungsionalitasnya (Shrivas, 2019). Jenis-jenis *blockchain* dapat dilihat pada tabel berikut.

Tabel 2.1.1 Jenis *Blockchain*

Jenis	**Aspek**	**Penjelasan**
Public Blockchain	Aksesibilitas data	Jenis *blockchain* ini memperbolehkan setiap individu/kelompok untuk bergabung sebagai *node* dalam melakukan pembacaan dan pencatatan data (Lin & Liao, 2017)
Consortium Blockchain	Aksesibilitas data	Jenis *blockchain* ini pada dasarnya bersifat tertutup, tetapi dapat memperbolehkan individu/kelompok tertentu yang tergabung dalam konsortium untuk berpartisipasi sebagai *node* dalam melakukan pembacaan dan pencatatan data (Lin & Liao, 2017)
Private *Blockchain*	Aksesibilitas data	Jenis *blockchain* ini bersifat tertutup dan hanya ada satu pihak *node* saja yang dapat melakukan pembacaan dan pencatatan data (Lin & Liao, 2017)
Permissionless *Blockchain*	Partisipasi *node*	Jenis *blockchain* ini tidak memiliki protokol perizinan yang harus dipenuhi oleh suatu pihak untuk berpartisiapsi sebagai *node* (Rennock dkk., 2018)
Permissioned *Blockchain*	Partisipasi *node*	Jenis *blockchain* ini memiliki protokol perizinan yang harus dipenuhi oleh suatu pihak untuk dapat berpartisipasi sebagai *node* (Rennock dkk., 2018)
Stateless *Blockchain*	Fungsionalitas	Jenis *blockchain* ini hanya dapat menjalankan logika komputasi sederhana saja seperti pencatatan dan transaksi (Hileman & Rauchs, 2018)

Stateful *Blockchain*	Fungsionalitas	Jenis *blockchain* ini dapat menjalankan logika komputasi yang lebih kompleks daripada hanya sekadar komputasi pencatatan data, permrosesan *state* berdasarkan logika bisnis yang ada dalam suatu sistem (Hileman & Rauchs, 2018)

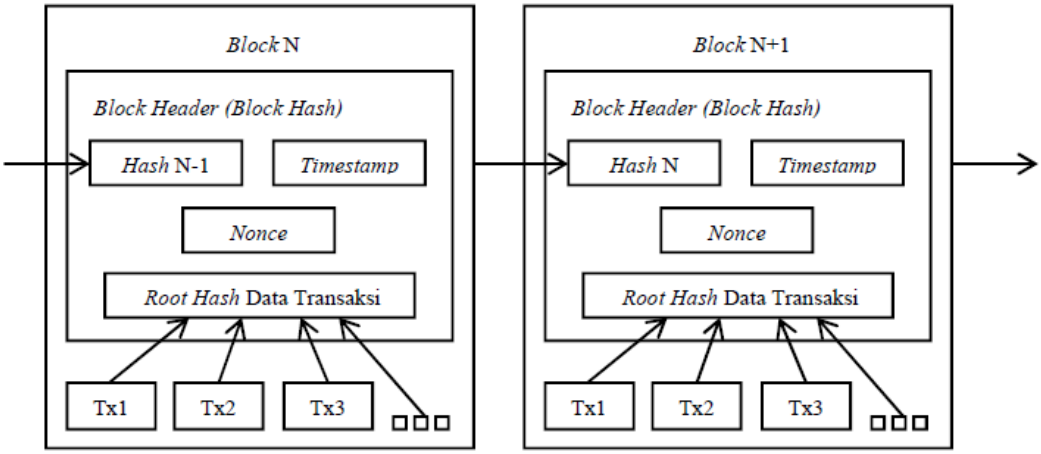
Blockchain adalah jaringan berbasis *peer-to-peer* dimana setiap *node* berperan dalam verifikasi transaksi, *routing* jaringan, membuat *node* baru, dan lain-lain. *Node miner* di dalam *blockchain* harus berkompetisi untuk melakukan validasi terhadap setiap transaksi, dimana hal ini bergantung pada algoritma konsensus yang diterapkan di *blockchain* (Li & Han, 2019)

Beberapa algoritma konsensus yang sering diterapkan:

- *Proof-of-Work* (PoW) : algoritma ini pertama kali diterapkan di Bitcoin, dimana algoritma ini memilih *accounting node* melalui persaingan *computing power*. *Node* bersaing satu sama lain untuk menyelesaikan masalah SHA256, dimana *node* tercepat yang berhasil menyelesaikan masalah tersebut akan mendapatkan *accounting authority* (Li & Han, 2019) dan juga mendapatkan reward berupa Bitcoin. PoW mengharuskan luaran dari *hash* sama dengan *predefined value*. Dalam kasus *miner* (*node* yang melakukan verifikasi) mendapatkan nilai yang diinginkan, *miner* akan melakukan broadcast dari *block* yang baru dibuat ke seluruh *node*s dalam jaringan, dimana *block* tersebut divalidasi dan ketepatannya akan ditambahkan ke salinan *distributed ledger* yang diterima oleh semua *node*s (Zheng dkk., 2017)
- *Proof-of-Stake* (PoS) : Algoritma ini mengusulkan bahwa *accounting authority* diberikan kepada *node*s bedasarkan aset dari *node* tersebut, berbeda dengan PoW yang menerapkan persaingan dari sisi *computing power*. Dalam jaringan Ethereum, *node*s mempertaruhkan sejumlah Ethereum (ETH) miliknya agar dapat dipilih menjadi *node*s validator, dan dalam melakukan validasi dari sebuah transaksi, *node*s perlu memecahkan masalah dan dipilih secara acak oleh suatu algoritme. PoS tidak menghitung adanya konsumsi energi seperti pada algoritma PoW. Selain itu, kecenderungan untuk menyerang jaringan yang menerapkan algoritma ini jauh lebih kecil, karena sama saja seperti menyerang aset kepemilikan milik sendiri (Zheng dkk., 2017)

- *Practical Byzantine Fault Tolerance* (PBFT) : Proses dari algoritma ini terdiri atas 3 tahap: *pre-prepare*, *prepare*, dan *commit*. Algoritma ini mampu mencapai konsensus dengan cepat, namun algoritma ini tidak disarankan untuk dipakai di *public blockchain* karena banyaknya *node*s akan berujung pada *delay* (Li & Han, 2019)

Seperti yang telah dijelaskan sebelumnya, pada sistem *blockchain* Bitcoin oleh Satoshi Nakamoto, mekanisme konsensus yang diterapkan adalah *Proof of Work*, dimana setelah sebuah transaksi dilakukan oleh *node*, maka *node* tersebut kemudian akan mengumumkan transaksi tersebut ke dalam jaringan. *Node* lain dalam jaringan tersebut kemudian menerima informasi tersebut lalu menggabungkannya dengan transaksi lain dengan membentuk *block*. Mekanisme *Proof of Work* ini akan membentuk *block* baru yang akan terhubung pada *block* terakhir dalam rantai *block* menggunakan *cryptographic hash function*, seperti SHA256. Keterkaitan antara satu *block* dengan *block* sebelumnya di dalam sebuah rantai ada pada cara menghitung nilai *hash*-nya. Nilai *hash* ini disebut sebagai *block hash* atau *block* header. *Block hash* didapatkan melakui komputasi fungsi *hash* dari nila idata transaksi yang tergabung dalam *block* dan beberapa value lainnya, seperti timestamp, nonce, dan *block hash* dari *block* sebelumnya dalam sebuah rantai *block*. Hubungan antar *block* terbentuk dengan penggunaan nilai *block hash* terakhir sebagai input dalam pembentukan nilai *block hash* baru (Aprialim, 2021)



Gambar 2.1.1 Detail *Block* pada *Blockchain*

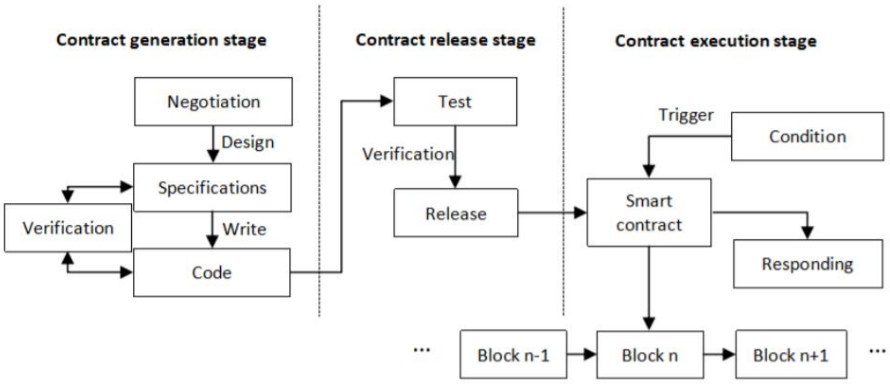
2.2 Smart Contract

Smart contract adalah bentuk digital dari kontrak tradisional. *Smart contract* mendefinisikan aturan-aturan yang harus ditaati oleh partisipan. Hampir semua sistem

blockchain yang ada, seperti Bitcoin, Ethereum, dan Hyperledger Fabric, telah mendukung *smart contract* (Li & Han, 2019)

Dari perspektif runtime environment, *smart contract* dapat dibagi menjadi dua, yaitu *script type* dan *turing complete type*. *Smart contract* yang diterapkan pada Ethereum adalah *Turing Complete language* (Solidity, Serpent) (Li & Han, 2019)

Smart contract memiliki tiga tahap dalam prosesnya, yaitu *generation*, *release*, dan *execution*. Fase *generation* merupakan fase untuk menyusun *smart contract* berdasarkan diskusi dari partisipan *blockchain*. Partisipan berdiskusi untuk menentukan bagaimana cara mencapai konsensus, mendesain spesifikasi dari contract, dan menuliskan kode contract. Fase kedua adalah fase *contract release stage*, yaitu fase untuk melakukan testing dan verifikasi terhadap contract yang dibuat pada fase sebelumnya sebelum contract dirilis. Jika *smart contract* telah di-deploy, maka *smart contract* tersebut tidak dapat dimodifikasi. Contract didistribusikan ke setiap *node* sebagai transaksi, lalu ditambahkan ke *blockchain*. Fase ketiga adalah *execution*. *External account* dibutuhkan untuk meminta kontrak di Ethereum. Jika kondisi tersebut terpenuhi, maka *smart contract* akan segera dieksekusi (Sanka dkk., 2021)



Gambar 2.2.1 Tahap Processing *Smart Contract*

2.3 Ethereum

Ethereum adalah pengembangan dari *blockchain* yang diperkenalkan pada 2015 oleh penggiat Bitcoin bernama Vitalik Buterin. Ethereum dikembangkan untuk memungkinkan pengerjaan komputasi yang lebih kompleks pada framework *blockchain* daripada hanya sekadar komputasi pencatatan data transaksi.

Ethereum pada dasarnya merupakan sistem pembayaran *cryptocurrency* yang terdesentralisasi. Sistem Ethereum dibangun dengan menggunakan bahasa pemrograman turing¬-complete (Ethereum Community, 2020) sehingga memungkinkan pengerjaan

komputasi yang lebih kompleks, seperti *smart contract*, dilakukan dengan mekanisme *blockchain*. Ethereum telah dikenal luas sebagai framework dalam mengembangkan *decentralized application.*

Blockchain Ethereum pada dasarnya merupakan *state machine* berbasis transaksi. *State machine* mengacu pada proses pengelolaan suatu susunan input untuk mengubah *state* yang tersimpan. *State machine* pada Ethereum disebut sebagai Ethereum Virtual Machine (EVM). Pengubahan suatu *state* dilakukan oleh suatu *node* dengan mengirim transaksi yang berisi input untuk melakukan proses pengubahan *state* (Kasireddy, 2017)

State pada Etherum merepresentasikan seluruh transaksi yang terjadi. Sama seperti Bitcoin, transaksi tergabung dalam suatu *block*, dan setiap *block* satu sama lain dengan *block* yang terbentuk sebelumnya. *Block* akan dibentuk dengan menggunakan protokol konsensus yang disebut GHOST (Greedy Heavies Observed Subtree) (Kasireddy, 2017)

Protokol GHOST adalah pengembangan dari protokol *Proof of Work*. Protokol Ghost menyelesaikan permasalahan terkait *stale block*, yaitu *block* lain yang terbentuk bersamaan dengan *block* lain yang telah tervalidasi. Dalam protokol GHOST, *miner* menerima hadiah jika berhasil membentuk *stale block*. Hal tersebut diterapkan karena pembentukan *block* pada Ethereum tergolong lebih cepat jika dibandingkan dengan Bitcoin, yang mengakibatkan kemungkinan terjadinya kondisi stale *block* pada Ethereum lebih besar jika dibandingkan dengan Bitcoin.

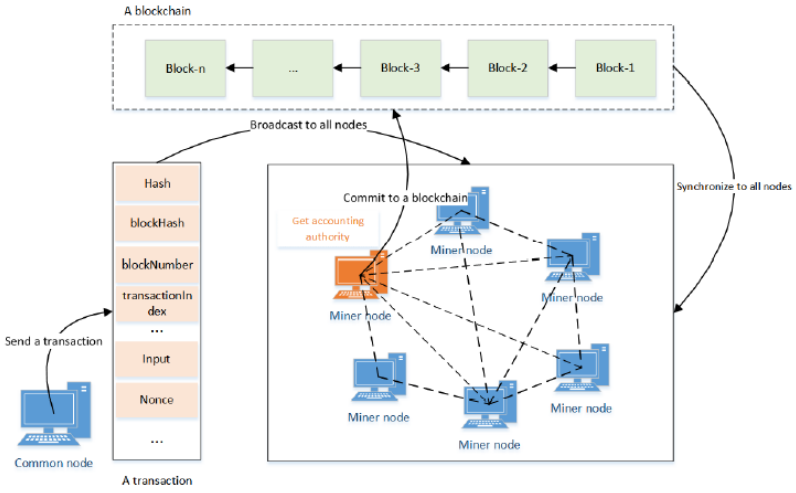
2.4 Transaksi

Transakasi adalah suatu instruksi yang dihasilkan oleh *externally owned account* yang dibuat dengan menggunakan *digital signature* berbasis *public/private key* milik *externally owned account.* Setiap transaksi yang dihasilkan akan tercatat ke dalam *blockchain* (Aprialim, 2021)

Tabel 2.4.1 Parameter pada Transaksi *Blockchain*

Parameter	Deskripsi
blockHash	*Hash* yang menunjukkan lokasi dari sebuah *block*
blockNumber	Panjang *block* dalam *blockchain*
From	Akun yang menginisiasi transaksi
to	*Address* atau akun penerima transaksi

hash	*Hash value* dari transaksi
input	*Hash value* dari records atau *binary bytecode* untuk *smart contract*
nonce	Serial number dari transaksi



Gambar 2.4.1 Ilustrasi *Blockchain*

Iterasi tahapan dari transaksi di dalam *blockchain* adalah sebagai berikut:

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

2.5 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 state *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) dibandingkan dengan *blockchain* lain seperti Bitcoin (10 menit). Semakin cepat pembentukan *block* pada suatu *blockchain* maka besar juga persaingan yang ada dalam proses pembentukan *block*.

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

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

- *parentHash*: *hash* dari *block* header milik parent *block*, yaitu *block* terakhir sebelum *block* terkait.
- *ommerHash*: *hash* dari daftar ommer *block* terkait
- *beneficiary*: address dari account yang menerima biaya pembayaran dalam proses mining *block* terkait
- *stateRoot*: *hash* dari state yang tersimpan pada *block* terkait. *Hash* ini terbentuk menggunakan Merkle Patricia Tree
- *transactionRoot*: *hash* dari transaksi yang tercatat pada *block* terkait. *Hash* ini terbentuk menggunakan struktur Merkle Patricia Tree
- *receiptRoot*: *hash* dari resi transaksi yang tercatat pada *block* terkait. *Hash* ini terbentuk menggunakan struktur Merkle Patricia Tree
- *logsBloom*: struktur data bloom filter yang terdiri atas log/catatan informasi
- *difficulty*: tingkat difficulty dari penyelesaian *block* terkait
- *number*: nilai penjumlahan (count) dari *block* terkait

- *gasLimit*: batas maksimum gas yang dapat digunakan dalam permrosesan komputasi transaksi pada *block* terkait
- *gasUsed*: jumlah total gas yang digunakan pada pemrosesan komputasi transaksi dari *block* terkait.
- *Timestamp* : timestamp yang berbasis unix dari pembentukan *block* terkait
- *extraData*: data ekstra yang berhubungan dengan *block* terkait
- *mixHash*: sebuah *hash*, yang jika dikombinasikan dengan nonce, akan membuktikan bahwa *block* terkait telah dibentuk melalui proses komputasi yang cukup.
- *Nonce*: sebuah *hash*, yang jika dikombinasikan dengan mix*Hash*, akan membuktikan bahwa *block* terkait telah dibentuk melalui proses komputasi yang cukup. (Kasireddy, 2017)

2.6 Account

Pada dasarnya, *blockchain* adalah sekumpulan objek yang dapat berinteraksi satu sama lain melalui sebuah framework. Objek tersebut yang kemudian disebut sebagai *account*. Setiap akun memiliki sebuah *state* dan *address* sepanjang 20 byte (Kasireddy, 2017)

Ada dua tipe akun dalam *blockchain*, yaitu *externally owned account* dan *contract account*. *Externally owned account* tidak memiliki logika bisnis berupa code dan dikontrol oleh *private key*. *Externally owned account* dapat mengirimkan pesan kepada *externally owned account* lainnya atau *contract account* lainnya dengan membuat dan menandatangani sebuah transaksi menggunakan private key-nya. *Contract account* adalah akun yang memiliki logika bisnis dan dikontrol oleh logika bisnis tersebut. Tidak seperti *externally owned account*, *contract account* tidak dapat menginisiasi transaksi. *Contract account* hanya dapat merespon transaksi yang diterimanya, baik dari *externally owned account* atau dari *contract account* lainnya. (Kasireddy, 2017)

State sebuah account, baik *externally owned account* dan *contract account*, memiliki empat komponen, yaitu:

- *Nonce*: Untuk *externally owned account*, angka ini merepresentasikan transaksi yang dikirimkan oleh account tersebut. Untuk *contract account*, nonce adalah jumlah contract yang dibuat oleh account tersebut.
- *Balance*: jumlah Wei yang dimiliki oleh address tersebut.
- *storageRoot*: *hash* dari root *node* dari Merkle Patricia tree

- *codeHash*: *hash* dari kode Ethereum Virtual Machine (EVM) untuk account tersebut.(Kasireddy, 2017)