

ABSTRAK

Nama : Annur Hangga Prihadi
Program Studi : Sistem Informasi
Judul : Implementasi Blockchain Pada Sistem Agrikultur Indonesia

Teknologi Blockchain secara luas dianggap sebagai pilihan dalam perkembangan teknologi yang mengedepankan sistem *peer-to-peer*, dan data yang terdesentralisasi untuk data organisasi. Proses *supply chain* di bidang agrikultur saat ini masih menggunakan teknologi tradisional yang dimana data dan dokumentasi produk agrikultur masih dicatat dan disimpan di atas kertas atau *database* pribadi, dan hanya dapat diperiksa oleh otoritas pihak ketiga yang terpercaya. Teknologi blockchain berpotensi dapat mengubah proses tersebut menjadi lebih modern dikarenakan transparansi dalam setiap kegiatan untuk memudahkan pelacakan dan visibilitas barang dalam *supply chain* berkat auditabilitas pencatatan yang lebih mudah, contohnya seperti Carrefour Italia melaporkan bahwa telah menerapkan sistem pelacakan makanan dengan Blockchain. Penulis fokus dalam membangun solusi bisnis dan sistem Blockchain pada transparansi *supply chain* bidang agrikultur dengan target *Minimum Viable Product* berupa hasil Txn proses *supply chain*, lalu penulis menggunakan jaringan Ethereum dengan produk *Smart Contract*-nya untuk membangun sistem bisnis beserta *blockchain*-nya. Dalam melakukan hal ini penulis perlu mengidentifikasi fungsi-fungsi yang diperlukan dalam menggunakan jaringan Ethereum untuk mengimplementasikan proses bisnis dan sistem *blockchain* yang akan dijalankan. Hasil produk dari penelitian ini berupa prototipe sistem Blockchain yang menghasilkan Txn pada proses *supply chain* untuk transparansi dalam kegiatan bisnis *supply chain* yang sedang berjalan.

Kata kunci:

Blockchain, Ethereum, Smart Contract, Supply Chain, Txn

1. Latar Belakang Masalah

Teknologi Blockchain secara luas dianggap sebagai pilihan revolusi dalam perkembangan teknologi yang mengedepankan sistem *peer-to-peer*, data yang terdesentralisasi untuk data organisasi. Blockchain memungkinkan pembaruan sistem moneter yang terdesentralisasi seperti Bitcoin, *Smart Contract* *Ethereum*, *Binance Smart Chain*, dan sumber daya lain yang dapat dikelola secara online. Awalnya teknologi Blockchain dikembangkan oleh orang yang mengaku bernama Satoshi Nakamoto pada tahun 2008 yang fungsi utamanya untuk memfasilitasi transaksi mata uang kripto. Dalam perkembangan yang lebih baru telah difokuskan tentang bagaimana Blockchain dapat digunakan untuk mendistribusikan sistem buku besar keuangan atau *ledger system* dan transaksi keuangan lainnya. Teknologi Blockchain memungkinkan antar entitas yang berbeda untuk bertukar data dan membuat transaksi dalam beberapa menit tanpa adanya intervensi atau verifikasi oleh pihak ketiga seperti bank saat melakukan proses transaksi yang dilakukan nasabah. Teknologi ini dapat dicapai melalui *shared data framework* yang menggunakan algoritma komputer untuk melakukan pembaruan secara *real time*. Teknologi Blockchain sangat menjanjikan revolusi domain organisasi seperti *supply chain* dalam melakukan kegiatan bisnisnya. Selain itu, teknologi Blockchain memungkinkan keamanan pertukaran data terdistribusi yang dapat memiliki dampak besar pada tata kelola organisasi. Hal itu juga bisa mengubah cara bisnis pihak dalam *supply chain* menyusun keterhubungan mereka dan bagaimana mereka akhirnya bertukar produk dan data.

Saat ini *supply chain* dalam bidang agrikultur sangat terstruktur, global dan saling berhubungan. Data dan dokumentasi produk agrikultur mengenai keamanan, *sustainability*, sumber, dan atribut lainnya biasanya dicatat dan disimpan di atas kertas atau database pribadi, dan hanya dapat diperiksa oleh otoritas pihak ketiga yang tepercaya. Situasi ini membuat akses ke data menjadi mahal, memerlukan waktu yang lama, syarat akan manipulasi, korupsi dan kesalahan yang menyebabkan ancaman kerugian dalam proses bisnisnya terutama bidang finansial. Banyak industri yang bekerja sama dengan

pemerintah, pengawas independen untuk memungkinkan transparansi informasi yang lebih baik dan membangun kepercayaan di antara para *stackholder* dalam *supply chain* produk agrikultur.

Terlepas dari tren digitalisasi dalam bidang ekonomi yang terus berlanjut, produk agrikultur masih menjadi salah satu industri yang kurang terdigitalisasi. Teknologi Blockchain berpotensi mempengaruhi situasi ini dalam banyak hal, dikelompokkan dalam empat arah: pertama, sektor pangan dapat memperoleh manfaat dari *digital smart contract* yang terdesentralisasi, otomatis berjalan secara independen hingga otomatisasi pemrosesan transaksi dan validasi antar pelaku *supply chain*. *Smart Contract* juga dapat berkontribusi terhadap otomatisasi peran badan pengatur dan interaksi pertukaran informasi di bidang pangan, namun ada kekhawatiran tentang kualitas yang dilaporkan data, dan validitas dan konsistensi *smart contract*. Kedua, Blockchain dapat memfasilitasi integrasi perangkat keras dan perangkat lunak, yang berpotensi mengarah pada integrasi sistem dan kinerja yang lebih baik. Ketiga, Blockchain menawarkan sesuatu berupa data yang tidak dapat diubah dalam catatan transaksi blok, dan dapat diakses di seluruh entitas. Dengan demikian, Blockchain bisa menjadi instrumen untuk menciptakan lebih banyak kepercayaan di antara para pelaku *supply chain* di bidang agrikultur berkat auditabilitas catatan yang lebih mudah. Keempat, teknologi Blockchain dapat memudahkan pelacakan dan visibilitas barang dalam *supply chain*, dengan melacak barang dari satu entitas ke entitas lainnya. Misalnya Carrefour Italia melaporkan bahwa telah menerapkan sistem pelacakan makanan dengan Blockchain.

2. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, penulis fokus dalam membangun solusi bisnis dan sistem Blockchain pada transparansi *supply chain* bidang agrikultur.

3. Batasan Masalah

Batasan masalah pada Tugas Akhir ini adalah

- 3.1 *Minimum Viable Product* berupa hasil Txn proses *supply chain* (hanya manufaktur).
- 3.2 Memilih jaringan Ethereum
- 3.3 Menggunakan *Smart Contract* yang di jaringan Ethereum

4. Tujuan Penelitian

Tujuan dari penelitian Tugas Akhir ini adalah membuat prototipe sistem Blockchain yang menghasilkan Txn pada proses *supply chain* untuk transparansi dalam kegiatan bisnis *supply chain* yang berjalan.

5. Manfaat Penelitian

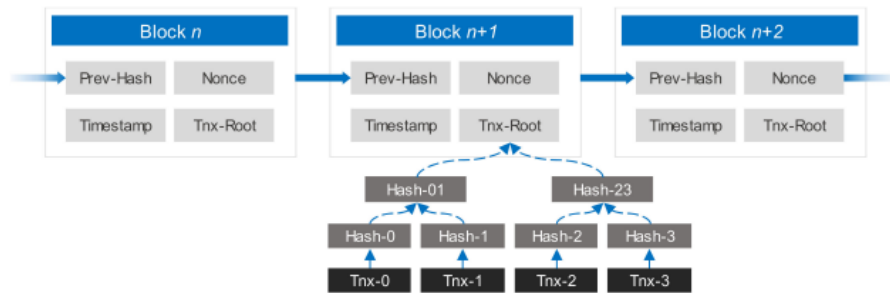
Manfaat yang diperoleh pada penelitian Tugas Akhir ini adalah

- 5.1 Adanya transparansi pada proses *supply chain* antar entitas
- 5.2 Mengembangkan sistem Blockchain pada bidang **agrikultur** di Indonesia

6. Kajian Pustaka

6.1 Pengertian Blockchain

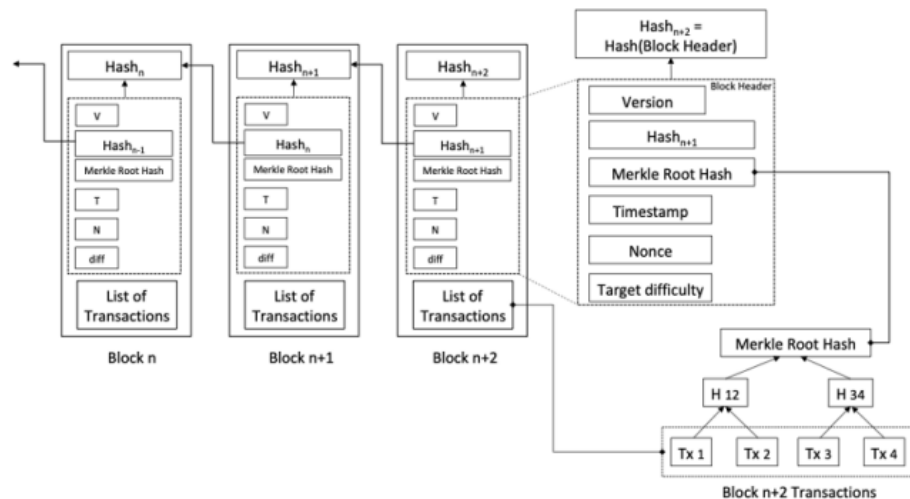
Teknologi Blockchain adalah jenis buku besar atau ledger terdistribusi dan telah digunakan dalam implementasi mata uang kripto seperti Bitcoin. Blockchain membangun data rantai kronologis dengan cara data yang tidak dapat diubah dan sifatnya abadi. Data transaksi diatur di dalam blok, dan untuk menambahkan blok baru ke rantai node dari blockchain perlu mencapai konsensus. Konsensus adalah sebuah sistem yang memastikan bahwa semua pengguna yang terlibat dalam rantai Blockchain menyetujui keadaan tertentu dari sistem sebagai keadaan sebenarnya. Semua blok itu dikonfirmasi dan divalidasi melalui mekanisme konsensus yang dijalankan bersama dari blok tervalidasi bagian pertama hingga terakhir, oleh karena itu disebut dengan Blockchain.



Gambar 6.1 Struktur Blockchain

(Sumber: A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management)

Sistem Blockchain mendistribusikan catatan waktu dari semua transaksi jaringan, direplikasi pada antar node dari jaringan peer-to-peer. Blok validator node berpartisipasi dalam algoritma konsensus, untuk memvalidasi dan menambahkan blok baru ke blockchain, serta mempertahankan yang tidak dapat diubah dalam canonical shared-state dari blockchain. Informasi transaksi dikelompokkan bersama ke dalam blok, dan setiap blok ditautkan ke blok awal, mirip dengan sistem linked list. Ketika ada suatu entitas ingin melakukan modifikasi blok saat terjadinya transaksi, entitas tersebut harus mengubah isi dari satu blok, serta semua blok lainnya yang dimana sebagian besar transaksi telah terjadi di blok entitas blockchain lainnya pada saat yang sama. Oleh karena itu, untuk meningkatkan sifat desentralisasi, ketangguhan dan keamanan dalam penyebaran blockchain, perlu memiliki kumpulan blok validator besar. Untuk framework yang diusulkan, komponen dasar yang diperlukan adalah blockchain itu sendiri, smart contract untuk perjanjian tingkat layanan yang dapat di program, dan penyimpanan file terdesentralisasi untuk hosting data transaksi.



Gambar 6.2 Detail Struktur Blockchain

(Sumber: Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study)

6.2 Kerangka Kerja Blockchain

6.2.1 Transaksi dan Alamat

Setiap entitas di Blockchain memiliki pasangan kunci publik/pribadi yang digunakan untuk pengalamatan, dan membuat tanda tangan digital pada setiap transaksi untuk jaminan tanpa adanya intervensi. Karena pasangan kunci ini tidak terkait dengan identitas kehidupan nyata, blockchain menawarkan "nama samaran" kepada penggunanya. Transaksi yang ditandatangani dibuat untuk transfer token mata uang kripto, atau berinteraksi dengan fungsi Application Binary Interface (ABI) yang di-*deploy* di dalam *smart contract*.

6.2.2 Smart Contract

Smart contract hanyalah potongan kode yang disimpan di Blockchain itu sendiri dan mampu menerapkan syarat dan ketentuan terprogram atas transaksi yang terjadi di jaringan. Dalam kerangka kerja yang penulis usulkan, untuk transaksi data *supply chain* yang dirancang secara pribadi, penulis menggunakan *smart contract*

untuk memungkinkan para pelaku memutuskan kapan terjadinya transaksi dan berapa banyak data yang akan ditransaksikan dengan entitas yang mereka pilih, seperti pertukaran dibagian moneter dan/atau jasa.

6.3 Algoritma Konsensus Blockchain

Algoritma konsensus adalah mekanisme yang memungkinkan pengguna atau mesin untuk berkoordinasi dalam pengaturan terdistribusi yang sudah diatur. Sistem ini perlu memastikan bahwa semua entitas dalam sistem dapat menyetujui satu sumber kebenaran, bahkan jika beberapa entitas mengalami kegagalan. Dengan kata lain, sistem harus toleran terhadap kesalahan.

Dalam sistem pengaturan yang terpusat, satu entitas memiliki kekuasaan atas sistem yang sedang berjalan. Dalam kebanyakan kasus, entitas tersebut dapat membuat perubahan sesuka mereka, tidak ada sistem tata kelola yang rumit untuk mencapai konsensus di antara banyak administrator. Tetapi dalam pengaturan yang terdesentralisasi, entitas bekerja dengan sistem yang terdistribusi untuk menghasilkan “bagaimana kita mencapai kesepakatan tentang data transaksi yang sedang ditambahkan?”

Contohnya dalam mata uang kripto, saldo suatu entitas dicatat dalam database blockchain. Sangat penting bahwa setiap entitas (atau lebih tepatnya, setiap node) memelihara salinan data transaksi yang identik. Jika tidak, transaksi akan segera berakhir dengan informasi yang saling bertentangan atau berlawanan, merusak seluruh tujuan jaringan mata uang kripto. Kunci entitas publik memastikan bahwa suatu entitas tidak dapat menghabiskan koin satu sama lain. Tetapi masih perlu ada satu sumber kebenaran yang diandalkan oleh seluruh entitas jaringan, untuk dapat menentukan apakah suatu koin telah ditransaksikan.

Entitas yang ingin menambahkan blok (kami akan menyebutnya validator) untuk menyediakan pasak. Taruhannya adalah semacam nilai

yang harus dikemukakan oleh validator, yang mencegah mereka bertindak tidak jujur. Jika mereka curang, mereka akan kehilangan taruhannya. Contohnya termasuk daya komputasi, cryptocurrency, atau bahkan reputasi. Mengapa mereka repot-repot mempertaruhkan sumber daya mereka sendiri? Nah, ada juga hadiah yang tersedia. Ini biasanya terdiri dari cryptocurrency asli protokol dan terdiri dari biaya yang dibayarkan oleh pengguna lain, unit cryptocurrency yang baru dibuat, atau keduanya. Hal terakhir yang kita butuhkan adalah transparansi. Kita harus bisa mendeteksi ketika seseorang selingkuh. Idealnya, harus mahal bagi mereka untuk memproduksi blok, tetapi murah bagi siapa saja untuk memvalidasinya. Ini memastikan bahwa validator tetap diperiksa oleh pengguna biasa.

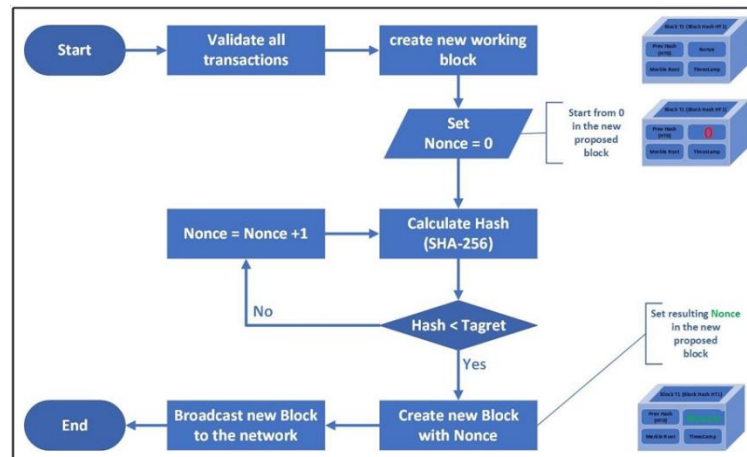
Ada 2 jenis algoritma konsensus yang sering digunakan yaitu

6.3.1 *Proof of Work (PoW)*

Proof of Work (PoW) adalah algoritma konsensus blockchain pertama. Jenis konsensus ini pertama kali diterapkan di Bitcoin, tetapi konsep ini sebenarnya telah ada sebelum adanya Bitcoin. Dalam *Proof of Work*, validator (disebut sebagai penambang atau entitas) melakukan hash pada data yang ingin mereka tambahkan hingga mereka menghasilkan solusi produk tertentu.

Hash adalah string huruf dan angka yang tampaknya acak yang dibuat saat suatu entitas menjalankan data melalui fungsi hash. Namun, jika entitas menjalankan data yang sama lagi, entitas tersebut akan selalu mendapatkan hasil yang sama. Perlu mengubah satu detail yang berada di dalam transaksi saja, maka hash entitas tersebut akan benar-benar berbeda. Berdasarkan output yang ada, suatu entitas tidak mungkin mengetahui informasi apa yang dimasukkan ke dalam fungsi. Oleh karena itu, seluruh entitas di blockchain berguna untuk membuktikan bahwa antar entitas mengetahui sepotong data sebelum waktu tertentu. Entitas A dapat memberikan hashnya kepada entitas B, dan ketika entitas A tersebut

mengungkapkan datanya, maka entitas B tersebut dapat menjalankannya melalui fungsi untuk memastikan outputnya sama. Dalam *Proof of Work*, protokol menetapkan kondisi bagaimana suatu blok dikatakan valid. Misalnya, hanya blok yang hashnya dimulai dengan 00 yang akan valid. Satu-satunya cara bagi penambang untuk membuat transaksi yang cocok dengan kombinasi itu adalah dengan memaksa input. Mereka dapat mengubah parameter dalam data mereka untuk menghasilkan hasil yang berbeda untuk setiap tebakan sampai mereka mendapatkan hash yang tepat. Dengan blockchain utama, standar ditetapkan sangat tinggi. Untuk bersaing dengan penambang lain, suatu entitas akan membutuhkan gudang yang penuh dengan perangkat keras hashing khusus (ASIC) agar dapat menghasilkan blok yang valid. Biaya saat menambang, adalah biaya mesin dan listrik yang dibutuhkan untuk menjalankannya. ASIC dibuat untuk satu tujuan, sehingga tidak digunakan dalam aplikasi di luar penambangan mata uang kripto. Sangat mudah bagi jaringan untuk memverifikasi bahwa penambang memang telah membuat blok yang benar. Bahkan jika penambang telah mencoba triliunan kombinasi untuk mendapatkan hash yang tepat, mereka hanya perlu menjalankan data penambang melalui suatu fungsi satu kali. Jika data penambang menghasilkan hash yang valid, itu akan diterima, dan penambang tersebut akan mendapatkan hadiah. Jika tidak, jaringan akan menolaknya, dan penambang akan membuang-buang waktu dan listrik dengan sia-sia.



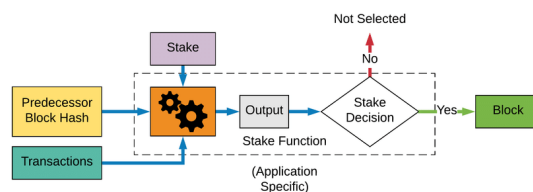
Gambar 6.3 Algoritma Konsensus *Proof of Work*

(Sumber: https://www.alibabacloud.com/blog/comprehensive-review-of-proof-of-work-consensus-in-blockchain_597042)

6.3.2 *Proof of Stake (PoS)*

Proof of Stake (PoS) diusulkan alternatif *Proof of Work*. Dalam sistem *PoS*, tidak ada konsep penambang, perangkat keras khusus, atau konsumsi energi yang besar. Pelaku hanya membutuhkan perangkat komputer biasa. Di *Proof of Stake*, Pelaku tidak mengedepankan sumber daya eksternal (seperti listrik atau perangkat keras), tetapi sumber dayanya berupa internal mata uang kripto. *PoS* memiliki aturan yang berbeda setiap protokol, tetapi umumnya ada jumlah minimum dana atau koin yang harus pelaku pegang agar memenuhi syarat untuk menjalankan konsensus ini. Dari persyaratan itu, pelaku mengunci dana di dompet (tidak dapat dipindahkan saat konsensus telah berjalan). Pelaku biasanya akan setuju dengan validator lain tentang transaksi apa yang akan masuk ke blok berikutnya. Dalam arti tertentu, pelaku menjalankan konsensus pada blok yang akan dipilih, dan protokol akan memilih salah satu yang dipilih oleh pelaku. Jika blok pelaku dipilih oleh konsensus pelaku lain, maka pelaku akan menerima sebagian dari biaya transaksi, tergantung pada dana atau koin pelaku di awal yang

terkunci. Semakin banyak dana yang dikunci oleh pelaku, semakin banyak keuntungan yang pelaku peroleh. Tetapi jika pelaku mencoba menipu atau membatalkan dengan mengusulkan transaksi yang tidak valid, pelaku akan kehilangan sebagian (atau semua) dana atau koin yang dikunci. Umumnya, tidak ada koin yang baru dibuat sebagai bagian dari hadiah untuk validator. Mata uang asli blockchain dengan demikian harus dikeluarkan dengan cara lain. Ini dapat dilakukan baik melalui distribusi awal (yaitu, ICO atau IEO) atau dengan meluncurkan protokol dengan PoW sebelum kemudian beralih ke PoS. Sampai saat ini, *Proof of Stake* murni baru benar-benar digunakan dalam mata uang kripto yang lebih kecil. Oleh karena itu, tidak jelas apakah itu dapat berfungsi sebagai alternatif yang layak untuk PoW. Meskipun secara teori tampak baik, namun dalam praktiknya akan sangat berbeda. Setelah PoS berjalan pada jaringan dengan nilai yang besar, sistem tersebut menjadi arena permainan dalam transaksi insentif finansial maupun data. Siapa pun yang memiliki pengetahuan untuk "meretas" sistem PoS kemungkinan hanya akan melakukannya jika mereka dapat memperoleh manfaat dalam peretasan tersebut. Oleh karena itu, satu-satunya cara untuk mengetahui apakah sistem tersebut layak dilakukan adalah melalui jaringan langsung. PoS akan diuji dalam skala besar dan akan diimplementasikan sebagai bagian dari serangkaian peningkatan di jaringan Ethereum (secara umum dikenal sebagai Ethereum 2.0).



Gambar 6.4 Algoritma Konsensus *Proof of Stake*

(Sumber: https://www.researchgate.net/figure/Proof-of-Stake-flow_fig3_335337656)

Mekanisme untuk mencapai konsensus sangat penting untuk berfungsinya sistem yang terdistribusi. Banyak yang percaya bahwa inovasi terbesar dalam Bitcoin adalah penggunaan Proof of Work untuk memungkinkan pengguna menyetujui serangkaian fakta transaksi yang dikelola bersama. Algoritma konsensus saat ini tidak hanya mendukung sistem uang digital, tetapi juga blockchain yang memungkinkan pengembang menjalankan kode di seluruh jaringan terdistribusi. Mereka sekarang menjadi landasan teknologi blockchain dan sangat penting untuk kelangsungan hidup jangka panjang dari berbagai jaringan yang ada. Dari semua algoritma konsensus, Proof of Work tetap menjadi penawaran yang dominan. Alternatif yang lebih andal dan lebih aman belum diusulkan. Karena itu, ada banyak penelitian dan pengembangan untuk menggantikan PoW.

6.4 Blockchain Untuk Manajemen *Supply Chain*

Integrasi Blockchain dengan manajemen *supply chain* dapat mengarah pada perubahan dalam industri yang berbeda. Metode tradisional dalam menjalankan bisnis *supply chain* sedang ditinjau kembali, dimana fungsi utamanya untuk mengurangi kebutuhan manusia dalam suatu transaksi. Blockchain berperan dalam kegiatan transaksi antara penyedia mewakili entitas pertama dalam *supply chain*, sedangkan konsumen adalah yang terakhir.

Oleh karena itu teknologi Blockchain, menawarkan banyak keuntungan yang berpotensi meningkatkan manajemen *supply chain* dalam berbagai cara.

- a. Entitas dapat melihat dan mengaudit transaksi dalam suatu sistem melalui seluruh siklus produksi, pengiriman, pemeliharaan, penyebaran, dan penghentian. Blockchain juga menyediakan pemantauan dan lacak blok semua perangkat lapangan di seluruh kegiatan siklus *supply chain*.

- b. Komponen perangkat keras, firmware, dan perangkat lunak sistem tidak diarsipkan pada satu server yang rentan terhadap penghapusan atau perubahan data. Sebagai gantinya, kriptografi hash metadata memungkinkan untuk melihat informasi transaksi saat ini dan sebelumnya dari data blockchain yang disepakati bersama.
- c. Mengakses dan melihat data *supply chain* lebih mudah, yang akan meningkatkan dan mempercepat sistem kerjasama antar vendor.
- d. Pihak ketiga yang rentan terhadap manipulasi digantikan oleh sistem blockchain yang dapat meningkatkan keamanan proses *supply chain*
- e. Algoritme konsensus blockchain akan menandai perangkat lapangan yang belum menjadi validator, memblokir setiap perubahan berbahaya dalam konfigurasi perangkat bidang ke mode *default*. Hal ini memungkinkan untuk peningkatan pemantauan sumber daya digital, keamanan perangkat.

Teknologi blockchain menunjukkan potensi besar dalam manajemen *supply chain*, penggunaan blockchain secara luas di industri masih pada tahap awal. Teknologi Blockchain masih perlu beradaptasi terhadap kebijakan umum, dan ini menciptakan berbagai tantangan terkait kebijakan. Perdebatan yang diperdebatkan tentang blockchain telah menyebabkan tantangan bagi regulator yang bertugas memahami teknologi. Perdebatan yang didefinisikan dengan buruk juga dapat mencegah regulator menggunakan teknologi blockchain dan menawarkan saran yang umum untuk tidak memakai blockchain.

Sumber kebingungan yang umum dalam definisi terkait blockchain adalah persepsi bahwa teknologinya sama dengan Bitcoin. Meskipun blockchain dapat mentransparansi rekaman transaksi publik terhadap mata

uang kripto, Blockchain yang diizinkan atau pribadi biasanya tidak melibatkan transaksi moneter.

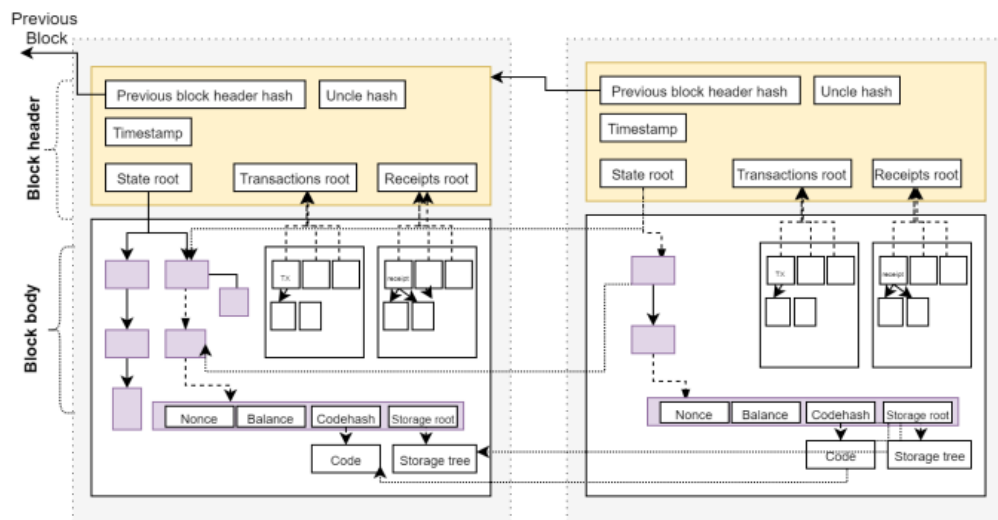
Blockchain digambarkan sebagai buku besar atau *ledger* digital publik di mana transaksi mata uang kripto dicatat. Dengan cara yang sama, blockchain telah didefinisikan sebagai buku besar atau *ledger* transaksi mata uang kripto terdesentralisasi. Definisi ini mungkin terbukti kontradiktif dalam industri yang berbeda. Mereka memiliki pandangan yang berbeda sebagai akibat dari peran yang mereka perlukan untuk memenuhi atau teknologi yang mereka gunakan. Sistem *zero-proof*, PoW, PoB, atau otoritas adalah beberapa cara dalam algoritma konsensus yang mengatur mekanisme transaksi untuk data buku besar atau *ledger* terdistribusi yang keamanannya dapat dijelaskan.

6.5 Ethereum

Ethereum adalah platform komputasi berbasis blockchain dengan fungsionalitas *smart contract* yang memungkinkan pengguna membangun aplikasi terdesentralisasi yang berjalan pada teknologi blockchain. Selain buku besar atau *ledger* yang didistribusikan, Ethereum menyediakan mesin virtual, yang disebut Ethereum Virtual Machine (EVM) yang dapat mengeksekusi skrip yang ditulis dalam bahasa pemrograman level tinggi (seperti, Solidity). Di Ethereum, struktur data blockchain lebih kompleks daripada pendahulunya yaitu Bitcoin. Tajuk atau *header* blok terdiri dari metadata, dan *body* terdiri dari beberapa jenis data, yaitu, transaksi, penerimaan, dan status sistem (status akun). Masing-masing data ini diatur seperti *Merkle tree* atau *Patricia tree* (Radix tree) di *state tree*. *State tree* (atau pohon penyimpanan akun) merupakan komponen yang sangat penting dalam buku besar atau *ledger* Ethereum. Hal ini digunakan untuk mengimplementasikan model akun, di mana setiap akun ditautkan ke status terkaitnya (saldo akun, status *smart contract*, dll.). Setiap node dapat mengurai *tree* menggunakan alamat akun dan mendapatkan status yang diperbarui tanpa setiap perhitungan mengalami overhead. *State tree* tumbuh

setiap kali terjadi perubahan dalam suatu keadaan. *State tree* tumbuh dengan menambahkan node baru (disimpan di blok baru) memegang status baru yang merujuk ke node (disimpan di blok sebelumnya) yang berisi nilai lama untuk status yang sama.

Untuk menegakkan keabadian data transaksi, Ethereum menyimpan hash root di header blok. Dalam hal ini *tree* mengelola dua akun: akun milik eksternal (EOA) dan akun *smart contract*. Jenis pertama adalah akun yang dikendalikan oleh kunci pribadi yang dipegang oleh entitas tertentu, sedangkan yang kedua adalah akun yang dikendalikan oleh Bytecode *smart contract*. Kedua akun diwakili oleh alamat yang dihasilkan secara kriptografis sebesar 20 byte. Untuk mencegah serangan Denial of-Service (DoS), *Ethereum Virtual Machine* mengadopsi sistem gas, dimana setiap perhitungan program harus dibayar dalam unit khusus yang disebut *gas fee* sebagai mana didefinisikan oleh protokol. Jika jumlah gas yang disediakan tidak menutupi biaya eksekusi maka transaksi gagal.



Gambar 6.5 Struktur *Blockchain* Ethereum

(Sumber: Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare)

'*Gas Price*' menentukan tingkat konversi gas ke eter. 'Gas' pada dasarnya adalah biaya transaksi untuk mendorong penambang untuk

memasukkan eksekusi transaksi ke dalam blok blockchain Ethereum. Dengan demikian, gas adalah standarisasi yang memperkirakan biaya mengeksekusi kode pada jaringan Ethereum. Setiap transaksi memiliki biaya gas berdasarkan waktu eksekusi yang diharapkan.

'*Gas limit*' diatur untuk mencegah loop tak terbatas, yang akan menyalahgunakan sumber daya di Blok Ethereum. Jika melebihi batas, transaksi tidak selesai, dan blok yang sesuai tidak ditambang.

Struktur transaksi Ethereum seperti berikut

- Dari: tanda tangan dari pemilik EOA diperlukan untuk mengotorisasi transaksi.
- Kepada: penerima transaksi dapat berupa EOA atau CA
- Data: kode untuk menyebarkan kontrak baru atau untuk melakukan transaksi untuk kontrak tersebut.
- *Gas Price*: tingkat konversi dari gas ke mata uang kripto ether.
- Total gas: jumlah maksimum gas yang dapat dikonsumsi setiap transaksi.
- Nonce: penghitung yang bertambah per transaksi baru dari sebuah akun.

Area	Contoh
Dari	EOA (<i>External Owned Account</i>) entitas A
Kepada	CA (<i>Contact Address</i>)
Data	Kode kontrak yang dibuat oleh entitas A
<i>Gas Price</i>	2×10^{-8} ether
Total Gas	2.000.000
Nonce	35

Tabel 6.1 Ilustrasi Struktur Transaksi Ethereum

(Sumber: A Scalable Implementation of Anonymous Voting over Ethereum Blockchain)

6.6 Aktivitas Diagram

Aktivitas diagram menunjukkan proses bisnis dan perangkat lunak sebagai perkembangan suatu tindakan. Tindakan ini dapat dilakukan oleh suatu orang, komponen perangkat lunak atau komputer. Aktivitas diagram digunakan untuk menggambarkan proses bisnis dan kasus penggunaan serta untuk mendokumentasikan implementasi proses sistem. Bahkan progres yang paling kompleks pun dapat divisualisasikan dengan diagram aktivitas. Alur kerja yang berurutan digambarkan oleh aliran kontrol dan objek. Aktivitas diagram mewakili aktivitas yang dibuat oleh aliran tindakan.

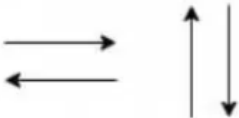
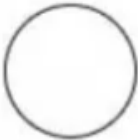
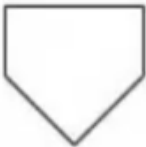
Aktivitas diagram dapat digunakan di berbagai situasi yang berbeda. Selain itu, berbagai hubungan antara aktivitas diagram dan diagram UML lainnya pun dapat terjadi. Aktivitas diagram sangat cocok untuk memvisualisasikan model prosedur dan manajemennya. Aktivitas diagram menggambarkan langkah-langkah individu dalam aktivitas serta urutan penyajiannya. Aktivitas digunakan dapat digunakan untuk berbagai fungsi seperti mulai dari pemodelan proses bisnis hingga penggambaran aliran kontrol. Aktivitas diagram dapat digunakan di mana saja di mana perilaku perlu dijelaskan atau di mana aliran kontrol perlu dimodelkan.

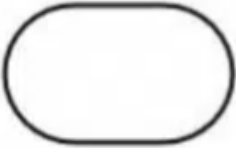

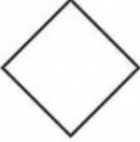




Aktivitas diagram memungkinkan untuk memodelkan aspek dinamis dari suatu sistem dengan mudah. Pengguna menggunakan aktivitas diagram dengan cara yang mudah dibaca sesuai dengan urutan sistem yang mungkin berurutan. Aktivitas diagram pada dasarnya adalah diagram alir yang menggambarkan aliran kontrol dari satu aktivitas ke aktivitas berikutnya, termasuk pemodelan langkah-langkah berurutan atau paralel dalam suatu proses. Manajemen proyek menggunakan diagram aktivitas untuk memvisualisasikan detail alur kasus penggunaan dengan cara yang dapat dimengerti. Dengan cara ini, kasus penggunaan dapat menjadi lebih detail dan dapat membentuk fondasi yang lebih kuat untuk produk dan sistem.


6.7 Flowchart

Flowchart adalah ilustrasi visual yang menggambarkan alur kerja atau proses dan solusi dari sebuah studi atau masalah. Flowchart adalah alat bisnis yang menunjukkan proses linier dari suatu pekerjaan. Kebanyakan orang biasanya menggunakan diagram ini untuk menjelaskan proses proyek, dan aliran wewenang dalam suatu organisasi. Untuk menjelaskan alur kerja kepada publik, menggunakan *flowchart* adalah pilihan yang baik dan ringkas. Maksud dari flowchart itu sendiri adalah untuk menggambarkan suatu tahapan penyelesaian suatu masalah secara sederhana, rapi, bersih, dan terurai serta dapat menggunakan simbol-simbol sesuai dengan standarnya.

Pada dasarnya dalam proses membuat *flowchart* tidak ada syarat mutlak yang harus dipenuhi. Karena diagram/bagan ini dibuat berdasarkan pemikiran untuk menganalisis suatu masalah dalam bisnis.

Simbol	Fungsi
	Flow Simbol yang fungsinya untuk menggabungkan antar simbol
	On-Page Reference Simbol yang fungsinya untuk menyambungkan proses keluar masuk dalam lembar kerja yang sama
	Off-Page Reference Simbol yang fungsinya untuk menyambungkan proses keluar masuk dalam lembar kerja yang berbeda

	Terminator Simbol yang fungsinya untuk mengawali maupun mengakhiri suatu proses
	Process Simbol yang fungsinya untuk menyatakan suatu proses dijalankan oleh komputer
	Decision Simbol yang fungsinya untuk menunjukkan kondisi tertentu yang memungkinkan output berupa 2 jawaban antara ya atau tidak
	Input/output Simbol yang fungsinya untuk menyatakan proses masukan atau luaran
	Manual Operation Simbol yang fungsinya untuk menyatakan suatu proses tidak dilakukan oleh komputer
	Document Simbol yang fungsinya untuk menyatakan masukan berasal dari dokumen dalam bentuk fisik dan luaran yang perlu dicetak
	Predefine Proses Simbol yang fungsinya untuk menjalankan suatu bagian (sub-program) atau prosedur

	<p>Display</p> <p>Simbol yang fungsinya untuk menyatakan peralatan luaran seperti layar, printer, dan lainnya</p>
---	--

Tabel 6.2 Simbol dan Fungsi *Flowchart*

(Sumber: <https://www.hashmicro.com/blog/flowchart-symbol-example-types/>)

6.8 Penelitian Sebelumnya

Judul penelitian	Pembahasan
Blockchain in Food and Agriculture Supply Chain: Use-Case of Blockchain in Indonesia	Pada jurnal ini penulis bekerja sama dengan perusahaan Hara untuk menggunakan Hara Token (Mata uang kripto Indonesia) dalam kegiatan transaksi menggunakan <i>blockchain</i> untuk kegiatan berdagang produk makanan
A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management	Pada jurnal ini penulis mencoba memanfaatkan produk teknologi <i>blockchain</i> untuk optimisasi penggunaan <i>Internet of Things</i> dalam transaksi yang sedang berjalan di proses <i>supply chain</i> contohnya seperti penggunaan <i>barcode</i>

Tabel 6.3 Penelitian sebelumnya

7. Metodologi Penelitian

Metodologi penelitian yang digunakan di dalam Tugas Akhir ini adalah

- 7.1 Mengumpulkan referensi atau pustaka terkait Blockchain, sistem Auditing, jaringan Ethereum, dan sistem informasi manajemen.
- 7.2 Mengidentifikasi fungsi-fungsi yang diperlukan dalam membuat sistem blockchain ini
- 7.3 Implementasi proses bisnis dan sistem Blockchain

8. Rencana Pelaksanaan Kegiatan

		September				Oktober				November				Desember			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	Tugas																
1	Mencari Referensi																
2	Riset mendalam mengenai Ethereum																
3	Riset mengenai proses bisnis yang akan digunakan																
4	Riset mendalam mengenai Solidity																
5	Implementasi Blockchain																
6	Front-End																
7	Penutup																

DAFTAR PUSTAKA

- [1] C. D. Clack, "A Blockchain Grand Challenge: Smart Financial Derivatives," vol. 1, no. 1, pp. 1-3, 2018.
- [2] G. A. Motta, B. Tekinerdogan and N. Athanasiadis, "Blockchain Application in the Agri-Food Domain: The First Wave," vol. 3, pp. 1-13, 2020.
- [3] A. K. Shrestha, et al. "A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives," vol. 3, pp. 1-22, 2020.
- [4] N. Sulaiman, S. Sakinah and S. Ahmad, "Logical Approach: Consistency Rules between Activity Diagram and Class Diagram," *Advanced Science Engineering Information Technology*, vol. 9, no. 2, pp. 552-559, 2019.
- [5] C. Supaartagorn, "Web Application for Automatic Code Generator," pp. 114-117, 2017.
- [6] A. Akhtar, et al. "Blockchain Based Auditable Access Control for," *International Conference on Distributed Computing Systems (ICDCS)*, vol. 40, pp. 12-22, 2020.
- [7] A. Hasselgren, Jens-Andreas, K. Kralevska, D. Gligoroski and A. Faxvaag, "Blockchain for Increased Trust in Virtual Health Care:," *Journal Medical Internet Research*, vol. 23, no. 7, pp. 1-15, 2021.
- [8] I. T. Javed, et al., "Health-ID: A Blockchain-Based Decentralized Identity," *Healthcare*, vol. 9, no. 712, pp. 1-21, 2021.
- [9] A. Maghfirah and Hara, "Blockchain in Food and Agriculture Supply Chain: Use-Case of Blockchain in Indonesia," *International Journal of Food and Beverage Manufacturing and Business Models*, vol. 4, no. 2, pp. 53-66, 2019.
- [10] G. Gursoy, C. M. Brannon and M. Gerstein, "Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts," *BMC Medical Genomics*, vol. 13, no. 74, pp. 1-11, 2020.
- [11] M. S. Ali, M. Vecchio, G. D. Putra and S. S. Kanhere, "A Decentralized Peer-to-Peer Remote Health Monitoring System," *Sensors*, vol. 20, no. 1656, pp. 1-18, 2020.
- [12] M. S. Al-Rakhami and M. Al-Mashari, "A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management," *sensors*, vol. 21, no. 1759, pp. 1-15, 2021.
- [13] J.-G. Song, M. Sung-Jun and J. Ju-Wook, "A Scalable Implementation of Anonymous Voting over Ethereum Blockchain," *Sensors*, vol. 21, no. 3958, pp. 1-19, 2021.
- [14] H. Shah, M. Shah, S. Tanwar and N. Kumar, "Blockchain for COVID-19: a comprehensive review," *Personal and Ubiquitous Computing*, pp. 1-28, 2021.
- [15] H.-J. Kim and e. al, "Smart Decentralization of Personal Health Records with Physician Apps and Helper Agents on Blockchain: Platform Design and Implementation Study," *JMIR Medical Informatics*, vol. 9, no. 6, pp. 1-14, 2021.