

Pemanfaatan Blockchain Sebagai Sistem Tracking Produk Perikanan di Tingkat Industri: Tinjauan Dari Perspektif Matematika Diskrit

Fazri Arrashy Putra - 13524127

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jalan Ganesha 10 Bandung

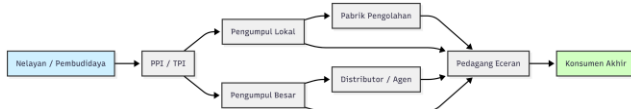
E-mail: fazriarrashyputra@gmail.com , 13524127@std.stei.itb.ac.id

Abstrak— Teknologi blockchain adalah suatu jenis teknologi data yang terdesentralisasi yang dapat menyimpan informasi dengan aman dan transparan tanpa bisa diubah-ubah lagi oleh pihak lainnya. Di sektor perikanan terdapat manfaat penggunaan blockchain untuk mengawasi produk dari awal hingga akhir demi menjamin keaslian produk serta meningkatkan keamanan dan transparansi rantai pasokan dalam industri perikanan. Matematika Diskrit adalah ilmu dasar yang menjadi landasan bagi pengembangan teknologi blockchain seperti teori bilangan, graf, logika. Fungsi hash yang menjadi tulang punggung pada teknologi blockchain sangat didasarkan pada teori bilangan. Selain itu, struktur blockchain bisa diwakili sebagai graf terarah. Sementara itu, verifikasi transaksi dan smart contract menggunakan logika proposisional.

Kata Kunci— blockchain, matematika diskrit, teori bilangan, fungsi hash, rantai pasok perikanan.

I. PENDAHULUAN

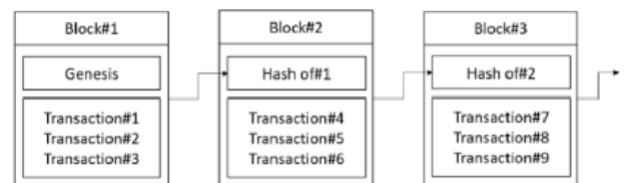
Industri perikanan memainkan peran vital dalam memenuhi kebutuhan pangan global dengan menyediakan sumber protein utama bagi miliaran orang di seluruh dunia. Namun demikian, kendala yang dihadapi oleh industri ini terletak pada masalah transparansi rantai pasok serta praktik ilegal penangkapan ikan dan pemalsuan informasi produk. Para konsumen semakin menuntut keterbukaan yang jelas terhadap asal-usul dan jalannya distribusi produk perikanan demi memastikan keaslian dan keamanan produk serta transparansi rantai pasok.



Gambar 1. Rantai Pasok Perikanan

Teknologi blockchain telah muncul sebagai solusi yang berpotensi untuk mengatasi tantangan yang ada ini. Blockchain merupakan teknologi data yang terdesentralisasi, transparan, dan tidak dapat diubah, yang membuatnya sangat sesuai untuk mencatat setiap data dalam rantai pasok perikanan. Mulai dari tahap penangkapan ikan, pengolahan, distribusi, hingga produk sampai ke tangan konsumen.

Di balik penggunaan teknologi blockchain yang rumit, tersembunyi dasar teoritis yang kokoh dari Matematika Diskrit, yaitu cabang matematika yang mempelajari teori bilangan, graf, dan logika. Untuk menjaga integritas data, blockchain mengandalkan fungsi hash yang berbasis pada teori bilangan dan aritmatika modular.



Gambar 2. Kedudukan hash pada blockchain, diambil dari [1]

Selain itu, struktur data blockchain dapat direpresentasikan sebagai graf berarah asiklik (DAG), sedangkan proses validasi dan eksekusi smart contract banyak bergantung pada logika proposisional.

Makalah ini akan membahas prinsip-prinsip Matematika Diskrit yang mendasari sistem blockchain serta menjelaskan penerapannya secara langsung dalam pelacakan produk perikanan di tingkat industri. Dengan pendekatan interdisipliner ini, diharapkan makalah ini dapat memperlihatkan hubungan antara teori matematika dan solusi teknologi dalam skala global.

II. LANDASAN TEORI

A. Blockchain

Blockchain adalah teknologi data terdesentralisasi yang mengelola data dalam blok-blok yang saling terhubung secara kriptografis. Setiap blok memuat kumpulan data, timestamp, dan hash dari blok sebelumnya. Sifat utama dari blockchain adalah:

- *Immutability* (tidak dapat diubah)

Data yang dicatat tidak bisa diubah tanpa mengubah seluruh rantai blok.

- *Transparency*

Semua pihak dalam jaringan *blockchain* dapat melihat riwayat transaksi data.

- *Decentralization*

Tidak ada yang mengatur otoritas data, data disimpan di banyak node dan dapat dikelola oleh siapapun.

B. Graf dan Struktur Data Berarah

Blockchain dapat direpresentasikan sebagai graf berarah asiklik (*Directed Acyclic Graph/DAG*), di mana setiap blok menunjuk ke blok sebelumnya melalui hash. Struktur ini menjamin urutan kronologis dan keutuhan data.



Gambar 3. Representasi Graf Berarah pada struktur *blockchain* sederhana

C. Fungsi Hash Kriptografis

Fungsi hash adalah algoritma yang mengubah input data menjadi karakter string dengan panjang yang sama. Dalam *blockchain*, hash digunakan untuk membuat identitas unik setiap blok, menjaga keaslian data (jika ada perubahan data sedikit saja, nilai hash akan berubah signifikan), dan membangun rantai blok yang saling terhubung satu sama lain.

$$H(x) = (a \cdot x + b) \bmod p$$

Fungsi hash di atas adalah fungsi hash sederhana dengan a adalah sebagai “kunci”, x sebagai data dan b sebagai konstanta penambah atau dikenal *salt* dalam kriptografi.

Blockchain menggunakan fungsi hash yang lebih kompleks daripada fungsi hash di atas. Salah satunya adalah menggunakan SHA256 (*Secure Hash Algorithm 256 Bit*). Algoritma Hash ini bukan hanya sekedar rumus matematis eksplisit tetapi berbasis bitwise. SHA256 dibangun dari operasi bitwise seperti AND, OR, NOT, XOR, rotasi bit (ROTR), aritmetika modular, dan logika proposisional.



Gambar 4. Contoh kode python untuk mendapatkan hash dari string “IKAN”

D. Logika Proposisional

Logika proposisional digunakan untuk membuat dan mengevaluasi kondisi logis dalam *smart contract*, yaitu kode dalam *blockchain* yang hanya akan dieksekusi jika kondisi tertentu dipenuhi. Hal ini sangat penting dalam mengotomatisasi transaksi dalam sistem.

Contoh penggunaan Logika Proposisional dalam tracking ikan adalah seperti ini, misalnya dalam rantai distribusi produk ikan, kita ingin memastikan bahwa data yang dicatat di *blockchain* valid dan sesuai kondisi tertentu, seperti:

- Produk ditangkap oleh nelayan yang terdaftar.
- Produk disimpan dalam suhu yang sesuai.
- Produk belum kadaluarsa.

Jika semua ini benar, maka produk boleh melanjutkan ke tahap berikutnya (misal: pengemasan, ekspor, penjualan, dll). Jika diterjemahkan ke dalam logika proposisi hasilnya akan seperti berikut ini:

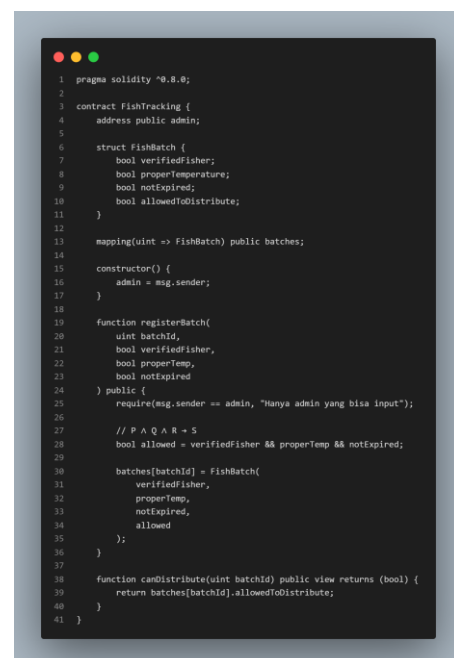
P: Ikan yang berasal dari nelayan terverifikasi

Q: Suhu penyimpanan selama distribusi $< 4^{\circ}\text{C}$

S: Produk dapat didistribusikan

$$(P \wedge Q \wedge R) \Rightarrow S$$

Kemudian hasil dari logika proposisi di atas bisa diterapkan pada kode *smart contract* berikut ini:



Gambar 5. Contoh pengaplikasian logika proposisi terhadap *smart contract solidity*.

Hasil penerapan logika proposisi di atas dapat diterapkan dengan sempurna untuk memvalidasi input, sehingga tidak ada nelayan, suhu, dan status kadaluarsa yang tidak sesuai.

E. Blockchain dalam tracking produk perikanan

Dalam konteks pelacakan produk perikanan, *blockchain* digunakan untuk mendaftarkan setiap tahap rantai pasok, seperti penangkapan, pengolahan, distribusi, hingga sampai ke tangan konsumen. Data dari setiap tahap akan disimpan di dalam blok dan tidak dapat diubah, sehingga memungkinkan transparansi dan auditabilitas. Dengan *QR Code*, konsumen dapat melacak asal-usul ikan hanya dengan memindai kode pada kemasan.

III. PENERAPAN

Pada bagian ini akan dibahas bagaimana teknologi *blockchain* dapat diimplementasikan untuk melacak pergerakan rantai pasok industri perikanan. Pembahasan mencakup rancangan sistem berbasis *blockchain*, penggunaan fungsi hash untuk menjamin integritas data, serta penerapan logika dalam *smart contract*. Selain itu, akan dijelaskan juga representasi alur distribusi menggunakan konsep graf yang menggambarkan interaksi antarblok dalam rantai pasok.

A. Desain Sistem Pelacakan Berbasis Blockchain

Rantai pasok produk perikanan umumnya terdiri dari beberapa tahapan berikut:

- Penangkapan ikan oleh nelayan atau kapal penangkap
- Distribusi awal ke pelabuhan atau tempat pelelangan ikan (TPI)
- Penyimpanan dan pengemasan oleh distributor atau perusahaan pengolah
- Transportasi dan distribusi ke pengecer atau eksportir
- Konsumen Akhir

Setiap tahapan menghasilkan data penting, seperti waktu dan lokasi penangkapan, identitas nelayan, suhu penyimpanan, informasi kadaluarsa, serta identitas pengirim dan penerima.

Setelah mengetahui rantai pasok, selanjutnya adalah membahas tentang arsitektur sistem. Secara umum, sistem pelacakan ini terdiri dari beberapa komponen seperti: 1). Sensor atau input manual untuk mencatat data suhu, waktu, lokasi, dll, 2). *Smart contract* untuk memverifikasi dan menyimpan data ke *blockchain*, 3). *Blockchain network* untuk menyimpan semua data transaksi pelacakan disimpan.



Gambar 6. Diagram alir desain sistem pelacakan.

Diagram alir di atas menunjukkan bahwa setiap tahapan disertai dengan validasi dan pencatatan menggunakan *smart contract* dan hash kriptografis.

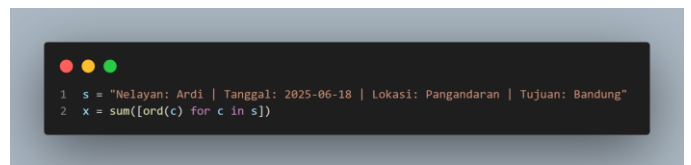
B. Pemanfaatan Fungsi Hash Dalam Pencatatan Data

Salah satu komponen penting dari teknologi *blockchain* adalah penggunaan fungsi hash kriptografis, yang secara langsung berkaitan dengan teori bilangan dalam Matematika Diskrit. Fungsi hash memastikan bahwa data yang tercatat di *blockchain* tidak dapat diubah dan diverifikasi secara kriptografis.

Dalam pelacakan produk perikanan, fungsi hash dapat digunakan untuk membuat ID unik untuk setiap produk berdasarkan data, seperti nama nelayan, tanggal dan lokasi penangkapan, suhu penyimpanan, dan tujuan distribusi. Misalkan kita akan membuat blok produk dengan data sebagai berikut:

“Nelayan: Ardi | Tanggal: 2024-06-12 | Lokasi: Pangandaran | Tujuan: Bandung”

Langkah selanjutnya adalah ubah seluruh string menjadi representasi numerik dengan cara sederhana contohnya konversi ke kode ASCII, lalu jumlahkan.



Gambar 7. Kode untuk menjumlahkan string

Hasil dari $X = 6952$, karena kita akan menggunakan fungsi hash sederhana yaitu:

$$H(x) = (a \cdot x + b) \bmod p$$

Maka langkah selanjutnya adalah menentukan parameter hash

$$H(x) = (a \cdot x + b) \bmod p$$

$$a = 37$$

$$x = 6952$$

$$b = 123$$

$$p = 7919$$

$$H(6952) = (37 \cdot 6952 + 123) \bmod 7919$$

$$H(6952) = (257224 + 123) \bmod 7919$$

$$H(6952) = 257347 \bmod 7919$$

$$H(6952) = 4298$$

Hasil hash ini kemudian di simpan ke *blockchain network* untuk disimpan ke dalam block dan melanjutkan ke tahap berikutnya.

Ini adalah representasi hash dari data di atas menggunakan fungsi hash sederhana. Perlu diingat bahwa fungsi ini bukan fungsi hash kriptografi, untuk aplikasi pelacakan ikan perlu diganti dengan fungsi seperti SHA-256.



Gambar 8. Diagram alir melakukan hash pada blockchain

C. Struktur Graf dan Jejak Distribusi Produk

Pelacakan produk dalam rantai pasok perikanan dapat direpresentasikan menggunakan struktur graf, yaitu salah satu topik penting dalam matematika diskrit. Dalam konteks ini, setiap blok atau lokasi dalam pelacakan dapat direpresentasikan sebagai simpul (node), sedangkan hubungan antar proses distribusi direpresentasikan sebagai sisi (edge). Penggunaan graf mempermudah visualisasi alur distribusi dan memungkinkan analisis terhadap jalur pergerakan produk secara matematis dan sistematis.

- Representasi Graf Dalam Rantai Pasok

Graf yang digunakan dalam pelacakan produk perikanan adalah graf berarah, karena distribusi produk mengikuti aturan tertentu.

Simpul: Nelayan, TPI, Distributor, Retailer, Konsumen.

Sisi: Aliran distribusi produk antar simpul.

- Contoh representasi Graf



Gambar 9. Representasi Graf Rantai Pasok

Gambar di atas merupakan graf yang merepresentasikan rantai pasok industri perikanan yang sederhana yang nantinya akan menggambarkan pada *blockchain network*.

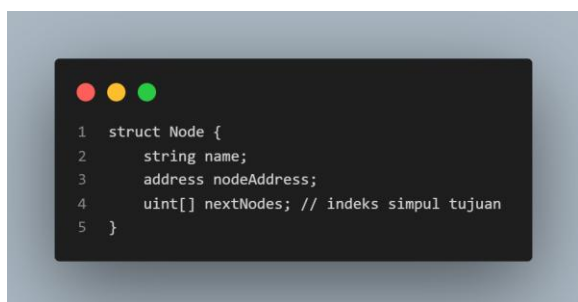
- Pemanfaatan Graf dalam Sistem Pelacakan

Dengan struktur graf, sistem *blockchain* pelacakan ikan dapat melakukan:

1. Menelusuri jalur distribusi produk secara menyeluruh.
2. Mendeteksi simpul (node) atau sisi (edge) yang mencurigakan (misalnya rantai distribusi ilegal).
3. Mendeteksi siklus distribusi.
4. Mengukur efisiensi jalur distribusi (mencari lintasan terpendek).

- Model Data Graf di *Blockchain*

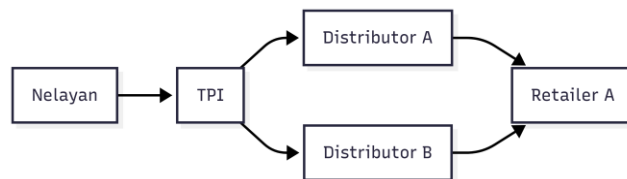
Di dalam *smart contract*, struktur graf dapat di simpan sebagai relasi antar block



Gambar 10. Kode solidity aplikasi dari graf

Kode di atas akan membentuk graf berbasis simpul dan sisi yang digunakan untuk memverifikasi arah aliran barang.

- Kasus Pemanfaatan Graf



Gambar 11. Aplikasi Graf.

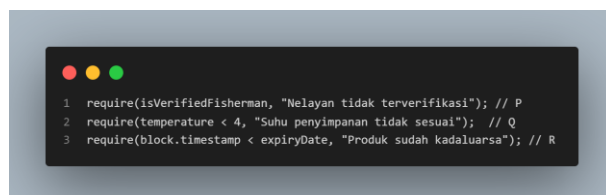
Terlihat bahwa retailer A menerima produk dari dua distributor berbeda, hal ini bisa dianalisis lebih lanjut untuk mendeteksi duplikasi atau penyaluran yang salah.

D. Logika Proposisional untuk Validasi Kondisi Produk

Logika proposisional merupakan salah satu cabang utama dalam matematika diskrit yang sangat relevan dalam implementasi sistem berbasis *blockchain*. Dalam pelacakan produk perikanan, logika proposisional dapat digunakan untuk menentukan kondisi-kondisi yang harus dipenuhi agar suatu produk dianggap layak untuk didistribusikan atau dijual ke konsumen.

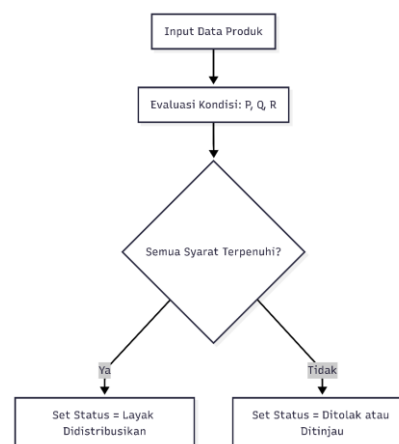
- Aplikasi Logika Proposisional dalam *Smart Contract*

Dalam *smart contract* berbasis *blockchain*, logika proposisional diterapkan menggunakan fungsi `require()` yang secara logik menyaring kondisi.



Gambar 12. Aplikasi logika dalam smart contract

- Integrasi ke dalam Alur Pelacakan.



Gambar 13. Penerapan logika proposisional pada flowchart

Dalam sistem ini, logika proposisional digunakan untuk menentukan status kelanjutan distribusi ikan.

E. Implementasi Smart Contract untuk Pelacakan Ikan

Salah satu fitur unggulan teknologi *blockchain* adalah kemampuannya menjalankan *smart contract*, yaitu program yang berjalan otomatis ketika kondisi tertentu terpenuhi. Dalam sistem pelacakan produk perikanan, *smart contract* berfungsi untuk:

- 1) Mencatat data ikan secara transparan.
- 2) Melakukan validasi.
- 3) Menyimpan status distribusi berdasarkan hasil validasi.
- 4) Memberikan akses terbuka bagi pihak yang ingin memverifikasi asal-usul produk.

Seluruh implementasi telah diunggah pada tautan GitHub yang tercantum dalam lampiran di halaman akhir.

F. Integrasi dan Simulasi Penggunaan Sistem

Setelah sistem pelacakan produk perikanan dirancang dan *smart contract* diimplementasikan, tahap selanjutnya adalah integrasi ke dalam alur sistem yang sebenarnya serta simulasi penggunaannya untuk memastikan efektivitasnya di lapangan.

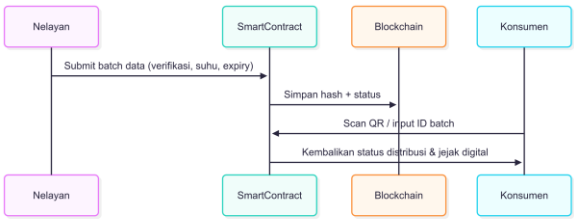
- Komponen sistem yang terintegrasi

Sistem pelacakan ikan berbasis *blockchain* akan menggabungkan beberapa komponen teknologi dan teori diskrit, yaitu:

Tabel 1. Komponen dan Teori diskrit dalam sistem pelacakan

No	Komponen	Deskripsi
1	Smart Contract	Bertindak sebagai validator otomatis terhadap data input
2	Fungsi Hash (SHA-256)	Menghasilkan ID unik tiap batch dan memastikan integritas data
3	Graf distribusi	Menyimpan struktur aliran produk
4	Logika Proposisional	Menentukan kelayakan produk berdasarkan kondisi yang ditetapkan
5	Sensor IoT (Opsional)	Mencatat suhu, waktu dan lokasi secara otomatis
6	User Interface	Memberikan akses bagi nelayan, distributor, dan konsumen untuk input dan verifikasi data

- Simulasi Skenario Penggunaan



Gambar 14. Diagram proses skenario penggunaan

Diagram di atas menjelaskan bagaimana alur dari pihak-pihak yang terlibat hingga sampai ke konsumen. *Smart Contract* berperan penting untuk menjembatani antara input pengguna dengan data yang akan disimpan.

- Simulasi Data Ikan

Tabel 2. Simulasi Data

No	field	nilai
1	Nama Nelayan	“Asep”
2	Terverifikasi	true
3	Suhu Penyimpanan	3
4	Tanggal Kadaluarsa	14 Agustus 2026

Karena semua data valid, maka *smart contract* menyimpan data ke *blockchain network* dan ikan layak didistribusikan.

Selanjutnya, konsumen dapat menggunakan *QR Code* untuk memverifikasi data dan melihat rantai pasok yang terjadi pada produk ikan ini, sehingga dapat menumbuhkan kepercayaan konsumen yang lebih tinggi.

IV. KESIMPULAN

Sistem pelacakan produk perikanan yang menggunakan teknologi *blockchain* menawarkan cara yang aman, transparan, dan efisien untuk mengelola rantai pasok komoditas yang sangat bergantung pada kepercayaan dan keaslian data. Makalah ini membahas fungsi hash kriptografis (berbasis teori bilangan), struktur graf untuk pelacakan distribusi, logika proposisional untuk validasi data, dan *smart contract*, serta bagaimana konsep matematika diskrit memainkan peran penting dalam hal teknis sistem *blockchain*.

Aplikasi hash seperti SHA-256 memastikan integritas data yang tidak dapat diubah (*immutability*) dan representasi graf memungkinkan melihat dan menganalisis jalur distribusi produk dari sumber ke konsumen. Dalam *smart contract*, logika proposisional menyatakan bahwa setiap proses dapat divalidasi berdasarkan kondisi tertentu, sehingga memungkinkan pengambilan keputusan yang logis dan deterministik.

Melalui pendekatan ini, *blockchain* tidak hanya meningkatkan efisiensi dan kepercayaan dalam sistem industri perikanan, tetapi juga menjadi wadah nyata penerapan prinsip-prinsip Matematika Diskrit dalam kehidupan nyata. Hal ini menunjukkan bahwa konsep teoretis seperti fungsi hash, graf, dan logika bukan hanya sekadar abstraksi, tetapi dapat diintegrasikan secara langsung dalam teknologi industri modern.

V. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada:

1. Allah Subhanahu Wa Ta'ala,
2. Mah Yuli, Pak Dede, Aa Bimbim,
3. Bapak Rinaldi Munir dosen pengampu Matematika Diskrit IF1220 K-01,
4. Teman-teman penulis, dan
5. Pihak-pihak lain

yang telah mendukung penulis dalam pembelajaran hingga akhirnya berakhir juga proses penyusunan makalah ini.

TAUTAN VIDEO ADA DI YOUTUBE

https://youtu.be/SoqU43_PuWc

REFERENSI

- [1] Arham. J. Indrawan, 'IoT dan blockchain: Tinjauan Tantangan Solusi Keamanan dan Privasi', https://www.researchgate.net/publication/370074287_IoT_dan_Blockchain_Tinjauan_Tantangan_Solusi_Kemampuan_dan_Privasi. [Diakses 16 Juni 2025]
- [2] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- [3] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.)
- [4] R. Munir, *Matematika Diskrit*, Revisi Ketujuh, Bandung, Indonesia: Informatika, 2020.
- [5] Y. R. Perdana and J. Soemardjito, "Model Jaringan Rantai Pasok Komoditi Perikanan Dalam Rangka Mendukung Sistem Logistik Nasional," *Jurnal Transportasi Multimoda*, vol. 13, no. 1, pp. 31-40, 2017.
- [6] C. G. Nicolae, L. M. Moga, G. V. Bahaciu, and M. P. Marin, "Traceability system structure design for fish and fish products based on supply chain actors needs," *Scientific Papers: Series D, Animal Science-*

The International Session of Scientific Communications of the Faculty of Animal Science, vol. 60, 2017.

- [7] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," *Ethereum White Paper*, 2014. [Online]. Tersedia: <https://ethereum.org/en/whitepaper/>
- [8] "Aquafarming becomes main global source for fish, U.N. food agency says," *Reuters*, Jun. 7, 2024. [Online]. Available: <https://www.reuters.com/business/environment/aquafarming-becomes-main-global-source-fish-un-food-agency-says-2024-06-07/>

LAMPIRAN

https://github.com/fazridep/sol_tugas_makalah

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Juni 2025



Fazri Arrashyi Putra, 13524127