RFID Simulation Of Supply Chain Management Using Blockchain

Ahmad Fali Oklilas*[1)] Arif Tumpal Leonardo Sianturi[2)] Huda Ubaya[3)]
Rossi Pasarella[4)] Iman Saladin B.Azhar[5)]

[1,4,5] Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
[2] Laboratorium Elektronika dan Sistem Digital, Fakultas Ilmu Komputer, Universitas Sriwijaya
[3] Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : fali@ilkom.unsri.ac.id*, arifsianturi11@gmail.com[2], huda@unsri.ac.id[3],
passarella.rossi@unsri.ac.id[4] imansaladin@unsri.ac.id[5]

Abstrak

Blockchain merupakan sekumpulan block yang tersusun secara berurut, block-block tersebut mampu menyimpan data berisi transaksi yang telah dilakukan sebelumnya. blockchain memiliki beberapa sifat dan keunggulan diantaranya terdesentralisasi dan immutable. Berkat keunggulan yang dimiliki oleh blockchain, Blockchain banyak dimanfaatkan pada bidang lain yang salah satu contohnya adalah supply chain management. Pada penelitian ini supply chain management dijalankan dengan 2 skenario simulasi menggunakan teknologi RFID, dimana antenna RFID berfungsi sebagai node-node pada supply chain management disusun sedemikian rupa untuk membentuk alur perjalanan penghantaran barang, kemudian perjalanan barang dilakukan dengan Tag RFID sebagai ID produk. Penelitian ini menghasilkan program simulasi yang dapat menampung data supply chain management kedalam blockchain, memiliki transparansi, ketertelusuran, serta menyediakan keamanan pada data.

***Kata kunci** : Blockchain, Supply chain management, RFID, Keamanan Data, Immutable.*

Abstract

Blockchain is a collection of blocks that are placed in a sequential order and can hold data containing past transactions. The blockchain has various qualities and benefits, including the fact that it is decentralized and immutable. Blockchain is widely employed in different sectors due to its advantages; one example is supply chain management. In this study, supply chain management is performed with two RFID simulation scenarios, where RFID antennas operate as supply chain management nodes grouped in such a manner as to establish a flow of goods delivery trips, and then products travel is carried out with RFID tags as product IDs. This study creates a simulation tool that can include supply chain management data into the blockchain, having transparency, traceability, and data security.Keywords: Blockchain, Supply chain management, RFID, Data Security, Transparency, Traceability, Immutable.

1. PENDAHULUAN

Supply chain management merupakan manajemen dari serangkaian (jaringan) yang meliputi penyampaian suplai barang yang dihantarkan oleh supplier (Gudang) kepada *retailer-retailer* di berbagai tempat, dimana pada pengaplikasiannya, *supply chain management* mampu memudahkan dan meningkatkan profitabilitas dari *supplier*. Namun *supply chain management* sendiripun memiliki kelemahan, misalnya didalam *supply chain management* bidang kesehatan yang melibatkan banyak elemen seperti pabrik, *supplier*, apotek, rumah sakit

hingga pasien. Prosesnya masih sangat sulit untuk dipantau, karena kurangnya informasi, *system control* yang masih tersentralisasi, dan hal-hal lainnya. Hal-hal tersebut tidak terkecuali terhadap masalah-masalah tertentu.[1] Juga karena *supply chain* tradisional memiliki kekurangan yakni bersifat tersentralisasi dan masih sangat bergantung pada pihak ketiga pada saat dilaksanakannya *trading*, dimana sifat tersentralisasi, hal ini menyebabkan kurangnya transparansi, akuntablilitas, dan juga keterbukaan.[2]

Pada lingkup informasi, data merupakan aset-aset berharga yang dimiliki oleh pemilik data itu sendiri, oleh karena itu penggunaannya semestinya penuh dibawah kontrol pemilik data tersebut, data dapat mengalami kebocoran karena seringkali berada diluar kendali dari pemilik data tersebut. Karena itu kemampuan untuk secara efektif memanajemen data dan keamanannya masih dinilai kurang.[3] Oleh karena itu pada penelitian yang dilakukan oleh Azzi dkk, menjelaskan bahwa *Blockchain* diperkenalkan pada rantai pasokan untuk mengurangi risiko yang muncul dari sistem pelacakan dan manajemen data, menyebarkan *blockchain* dalam ekosistem *supply chain* membawa banyak manfaat seperti membuat pelacakan yang lebih transparan dan akurat, meningkatkan kepercayaan antara produsen dan konsumen, mengurangi atau menghilangkan penipuan dan produk palsu dan lain-lain. Namun mengintegrasikan *blockchain* ke dalam ekosistem *supply chain* membawa tantangan baru, Pengguna perlu mempertimbangkan properti dan kemampuan implementasi *blockchain* yang tersedia sebelum memilih *blockchain* yang paling cocok untuk ekosistem seperti itu.[4]

Adapun pada penelitian serupa yang pernah dilakukan oleh Susanne dkk, *blockchain* yang diimplementasikan dalam *supply chain* makanan dievaluasi sebagai elemen dalam sistem teknologi yang melihat empat komponen berbeda: teknik, pengetahuan, organisasi, dan produk. Temuan ini digunakan untuk memberikan pemahaman yang lebih dalam tentang peran mutakhir teknologi berbasis *blockchain* dalam *supply chain* makanan. Studi ini mengembalikan gambaran yang serius tentang apa yang canggih dari teknologi berbasis *blockchain* dalam *supply chain* makanan. [5]

Pada penelitian terdahulu [6], sistem yang dibangun adalah *supply chain management* pasokan telur dengan menggunakan *blockchain* dimana transparansi, ketertelusuran dan keaslian data menjadi fokus penelitian ini. Selama proses *supply chain*, paket-paket telur discan melalui *QR Code* yang tertempel di karton paket-paket telur tersebut, Pemindaian diambil di 3 lokasi yang berbeda, yakni saat berada di ladang, dimana data suhu telur, waktu pengambilan, dan kelembapan ikut dicatat. Lalu data kembali diambil di fasilitas pengemasan, data yang dimuat pada fasilitas ini adalah lokasi dan waktu pengumpulan, nama peternakan, riwayat suhu, kelembaban, keberangkatan dan kedatangan transit, waktu pemrosesan dan pengemasan, jenis telur, data sertifikasi, kuantitas batch, terbaik menurut tanggal, merek, warna, label produk, dan kemungkinan pemasok yang tumpang tindih selama waktu pemrosesan dan pengemasan. Terakhir data dapat diambil dari sisi konsumen guna mengetahui informasi terkait produk yang diterima melalui *scanning QR Code* menggunakan aplikasi *web* yang berisikan data-data dari paket telur yang sebelumnya sudah tercatat pada node sebelumnya.

Pada penelitian ini juga digunakan teknologi *Radio Frequency Identification* (RFID) sebagai masukan untuk *input data* barang pada *supply chain management* yang akan dijalankan melalui serangkaian skenario tersusun meliputi peletakan *antenna*, pembacaan tag, dan lain-lain. Teknologi ini dipilih karen pada tahun-tahun awal di abad ini RFID telah terbukti mampu menjadi solusi dalam masalah *tagging* terhadap produk karena kemampuannya untuk melakukan deteksi tanpa harus memperhatikan *Line of Sight* (LoS), dan dapat melakukan deteksi banyak tag secara bersamaan.[7]

Kemudian untuk metode didalam mengamankan data pada penelitian ini digunakan suatu metode yakni blockchain. Blockchain adalah rantai struktur yang mengkombinasikan blok data dalam sebuah urutan kronologis, dimana data tersebut tersebar secara terdesentralisasi didalam setiap node yang ada.[8] Blockchain memiliki kapabilitas untuk memainkan peran penting didalam penyebaran informasi, karena kemampuannya untuk memastikan validnya sebuah data dan aksesibilitas publik dari aliran data yang terjadi. Didukung dengan sifat blockchain yang terdesentralisasi dan terdistribusi, oleh karena sifat inftarstruktur

terdesentralisasinya, blockchain dapat terhindar dari masalah-masalah yang dialami oleh sistem tersentralisasi seperti trust issues, dugaan *corrupt*, kecurangan yang disengaja, masalah kepercayaan seperti penipuan, korupsi, gangguan dan pemalsuan informasi. serta lain-lain. [9]

Namun sistem terdesentralisasi umumnya rentan mengalami masalah, karena satu titik kerusakan dapat menyebabkan seluruh sistem rusak. Namun, karena memang teknologi ini masih dalam masa perkembangan tahap awal. Awalnya, blockchain muncul sebagai lapisan teknologi terdepan untuk aplikasi keuangan. Namun seiring perkembangan zaman, perhatian peneliti mulai mengaplikasikan juga teknologi Blockchain ke domain lain.[10]

Pada penelitian sebelumnya yang dikerjakan oleh penulis ditemukan bahwa *Supply chain management* dapat diintegrasikan dengan teknologi *blockchain* untuk mendapatkan transparansi kualitas produk serta ketertelusuran perjalanan produk. Kemudian didalam proses kemudahan untuk pendataan produk disetiap *node/vendor*, sensor seperti *Radio Frequency Identification* (RFID) juga dapat diterapkan, menurut penulis, kedua teknologi tersebut yang diimplementasikan ke dalam system dan mampu meningkatkan kualitas layanan dari sebuah jaringan *supply chain management*.[11]

Oleh karena itu berdasarkan latar belakang dan penelitan terdahulu, pada penelitian kali ini, selain *input* data yang diintegrasikan dengan teknologi sensor RFID untuk mensimulasikan proses pengambilan data dan perjalanan barang, *Supply chain management* juga akan disajikan dengan metode *blockchain* yang bersifat terdesentralisasi.

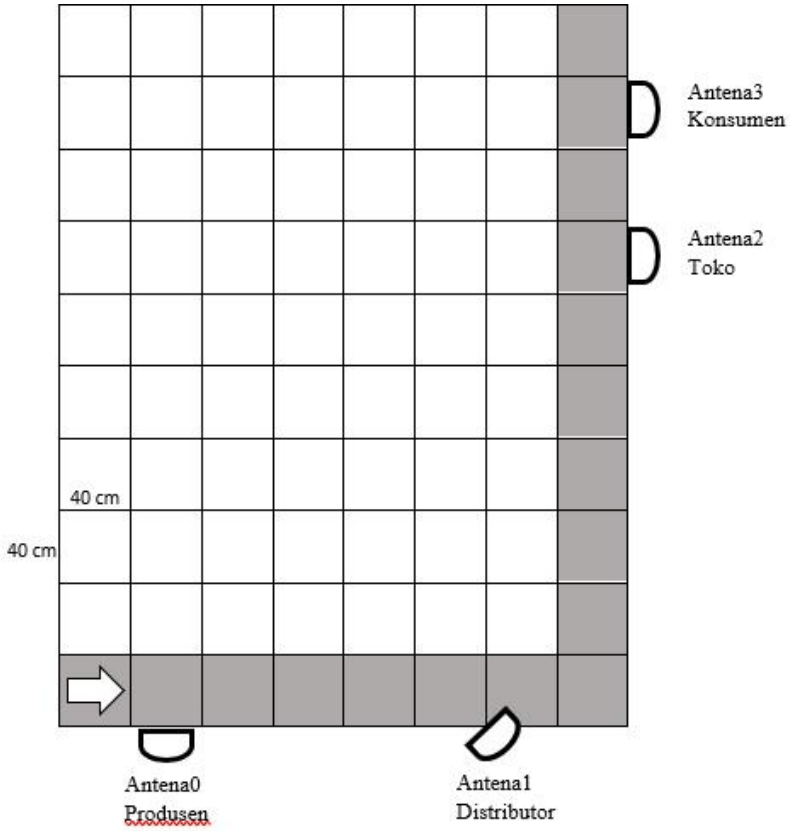
2. METODOLOGI PENELITIAN

Metode didalam pelaksanaan penelitian ini dilakukan dalam beberapa langkah dan tahapan. Tahapan tersebut dimulai dari tahap simulasi *supply chain management* dengan perangkat RFID sekaligus pengumpulan data, dilanjutkan dengan tahap pengolahan data, lalu dilakukan proses peng*input*an data terolah ke program *blockchain* yang telah dibuat, lalu kemudian program akan diuji keamanannya dan terakhir dilakukan analisa terhadap penelitian yang telah dijalankan, tahapan-tahapan tersebut memiliki detail dan penjelasan lebih lanjut adalah sebagai berikut :

1. Pengambilan data melalui simulasi Supply Chain Management
2. Pengolahan data simulasi supply chain management
3. Pembangunan program blockchain
4. Input dan eksekusi program
5. Pegujian keamanan program
6. Analisa simulasi dan program

2.1 Simulasi *Supply chain management*

Pada penelitian ini, *supply chain management* dilakukan melalui simulasi yang diintegrasikan dengan perangkat RFID. Proses ini diawali dengan Menyusun letak dari perangkat RFID yang membentuk lingkungan kerja simulasi. Kemudian simulasi dimulai dengan melakukan perjalanan produk yang di wakilkan oleh *tag* RFID ke setiap *node* tertuju untuk dibaca oleh RFID *Antenna* pada setiap *node*, data pembacaan akan masuk ke RFID *Reader* dan dikirimkan ke perangkat komputer atau laptop dan menghasilkan *log* yang akan diolah sebelum menjadi data *input* pada *program*, untuk *layout* skema perjalanan barang dapat dilihat pada Gambar 1.



Gambar 1 Pemetaan Lingkungan Kerja untuk Simulasi Supply chain management

2.2 Pengolahan Data

Setelah didapat, data pembacaan tidak selalu membaca tag dengan jumlah pembacaan yang sama, oleh karena itu data kemudian akan diolah untuk memfiltrasi data dan menghasilkan data pilihan berdasarkan pembacaan RSSI terbaik pada semua pembacaan di setiap *tag* dan di setiap *antenna*/*node*. Dalam proses pengolahan data, data terlebih dahulu dijadikan *dataset* lalu kemudian dimasukkan ke aplikasi program *Jupyter Notebook* untuk difiltrasi, hasil filtrasi akan disusun kedalam bentuk tabel seperti Tabel 1.

Tabel 1 Data Terolah dari Supply chain management

RFID Antenna Dan Posisi	*Tag ID*	Nama Barang	Jumlah Box	Max RSSI (dBm)	Keterangan
*RFID Antenna*0 Produsen	E200 001A 8319 0100 2310 43FE	Buku Tulis	1	1846.5	Pengambilan Data ke-5
	E200 001A 8319 0100 1960 4486	Kertas A4	1	992.9	
	E200 001A 8319 0094 2770 3B17	Kertas F4	1	1480.7	
	E200 001A 8319 0100 2460 43C2	Papan Ujian	1	1307.4	
	E200 001A 8319 0100 2100 4452	Pena	1	1674.8	

	E200 001A 8319 0095 2680 42DB	Pensil	1	889.2	
	E200 001A 8319 0100 2290 440A	Penghapus	1	668.9	
	E200 001A 8319 0100 2110 444E	Peruncing	1	1284.1	
	E200 001A 8319 0100 2470 43BE	Pensil Warna	1	1199.3	
	E200 001A 8319 0100 2120 4446	Krayon	1	1837.6	
*RFID Antenna*1 Distributor	E200 001A 8319 0100 2310 43FE	Buku Tulis	1	3309.2	Pengambilan Data ke-5
	E200 001A 8319 0100 1960 4486	Kertas A4	1	2070	Pengambilan Data ke-4
	E200 001A 8319 0094 2770 3B17	Kertas F4	1	2798.3	Pengambilan Data ke-4
	E200 001A 8319 0100 2460 43C2	Papan Ujian	1	3823.1	Pengambilan Data ke-2
	E200 001A 8319 0100 2100 4452	Pena	1	3345.2	Pengambilan Data ke-5
	E200 001A 8319 0095 2680 42DB	Pensil	1	2762.6	Pengambilan Data ke-4
	E200 001A 8319 0100 2290 440A	Penghapus	1	5020.5	Pengambilan Data ke-2
	E200 001A 8319 0100 2110 444E	Peruncing	1	4851.3	Pengambilan Data ke-2
	E200 001A 8319 0100 2470 43BE	Pensil Warna	1	5115	Pengambilan Data ke-2
	E200 001A 8319 0100 2120 4446	Krayon	1	4737.4	Pengambilan Data ke-3
*RFID Antenna*2 Toko	E200 001A 8319 0100 2460 43C2	Papan Ujian	1	1307.4	Pengambilan Data ke-1
	E200 001A 8319 0100 2100 4452	Pena	1	1674.8	Pengambilan Data ke-4
	E200 001A 8319 0095 2680 42DB	Pensil	1	889.2	Pengambilan Data ke-5
	E200 001A 8319 0100 2110 444E	Peruncing	1	1284.1	Pengambilan Data ke-5
	E200 001A 8319 0100 2120 4446	Krayon	1	1837.6	Pengambilan Data ke-1
*RFID Antenna*3 Pelanggan	E200 001A 8319 0100 2100 4452	Pena	1	3345.2	Pengambilan Data ke-1
	E200 001A 8319 0100 2120 4446	Krayon	1	4737.4	Pengambilan Data ke-4

2.3 *Input* Data pada Program *Blockchain*

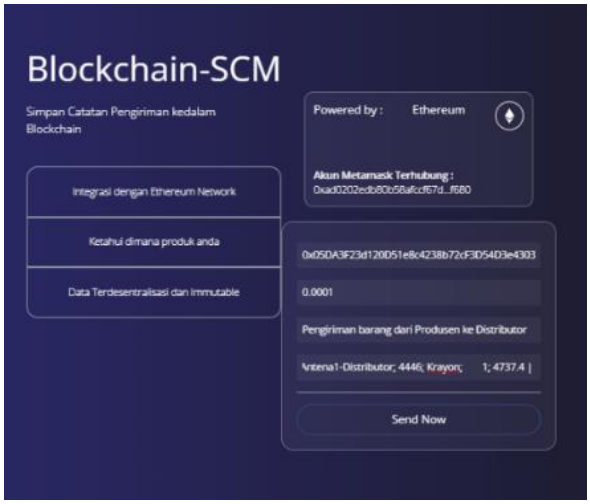
Setelah data siap dipakai, program kemudian dapat dibangun lalu data terolah kemudian dapat dimasukkan kedalam kolom *input* program untuk di publish kepada *node* lain dan disimpan kedalam jaringan *blockchain*. Program yang dibuat akan berbasis website agar dapat dipublish dan dilihat oleh *node* lainnya. Program *blockchain* akan menggunakan *testnet Goerli Ethereum network*.

2.4 Pengujian dan Analisa Keamanan

Setelah dipastikan program berjalan dengan baik, dengan dapat melakukan *input* data dan menampilkan data tersebut, setelah semua data selesai dimasukkan di program *website* dan datanya juga masuk kedalam jaringan *blockchain*, dilakukan pengujian keamanan terhadap data pada program dan program yang dibangun.

3. HASIL DAN PEMBAHASAN

Hasil pada program *blockchain* yang telah dibuat penulis untuk menyimpan sekaligus menampilkan data pada *node* pengguna ditunjukkan pada Gambar 2.



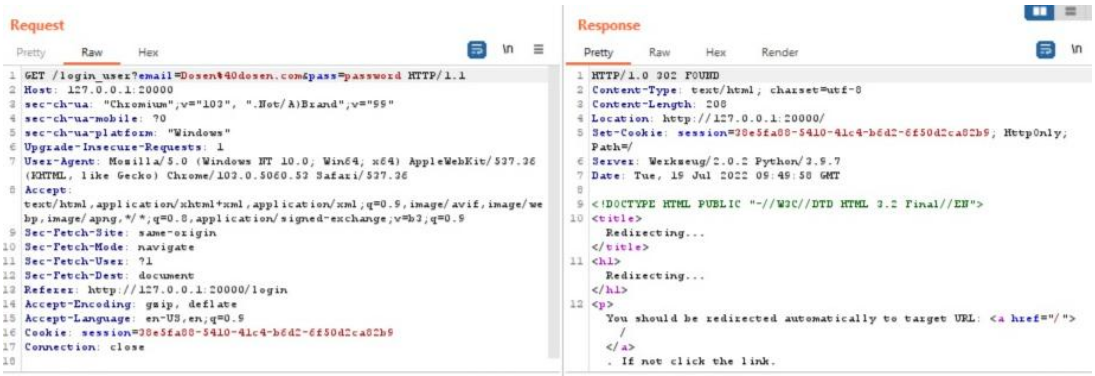
Gambar 2 Tampilan Utama Program Web

Pada Gambar 2, ditunjukkan sebuah aplikasi yang memiliki beberapa kolom *input* yang terbagi menjadi kolom *input* address tujuan, kolom *input* biaya transfer, kolom *input* subyek pengiriman, dan kolom *input* data pengiriman, kolom *input* ini kemudian diberi *input* berdasarkan keterangan masing-masing, setelah diproses data *input* akan dibuat menjadi sebuah *block* dan akan dimasukkan kedalam *blockchain* setelah divalidasi oleh *ethereum metamask,* sehingga hasil akhir akan menghasilkan *output* seperti pada Gambar 3.

Gambar 3 Tampilan Output Data Pada Program Web

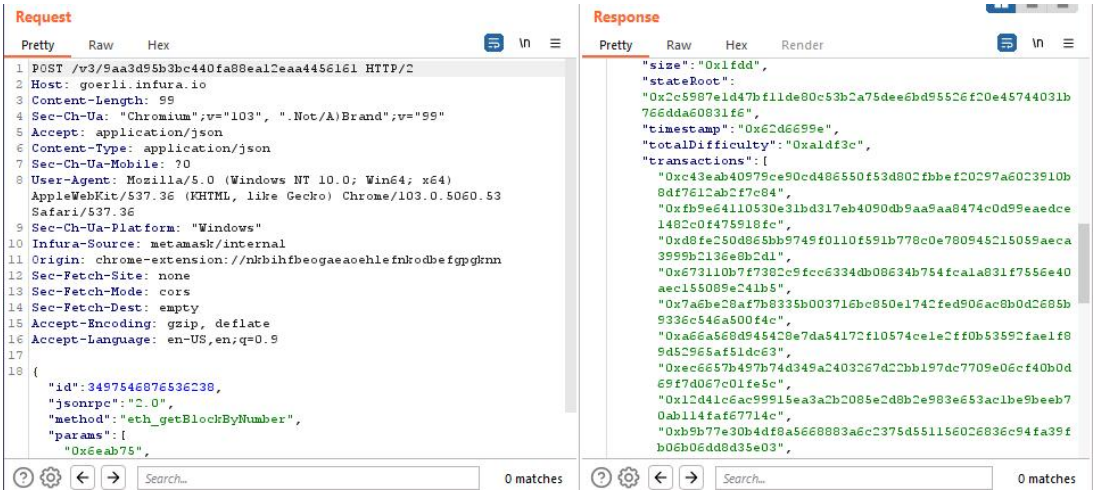
3.1 Pengujian dan Analisa Keamanan

3.1.1 Pengujian pertama dilakukan terhadap data yang telah dimasukkan pada program, normalnya data yang di*input*kan pada sebuah website (terutama http) akan dapat dilihat oleh pihak yang tidak bertanggung jawab menggunakan sebuah teknik atau *tool*s tertentu, hal ini dibuktikan peneliti melalui penggunaan *tool burpsuite* ke salah satu web *testing* yang hasilnya ditunjukkan pada Gambar 4.



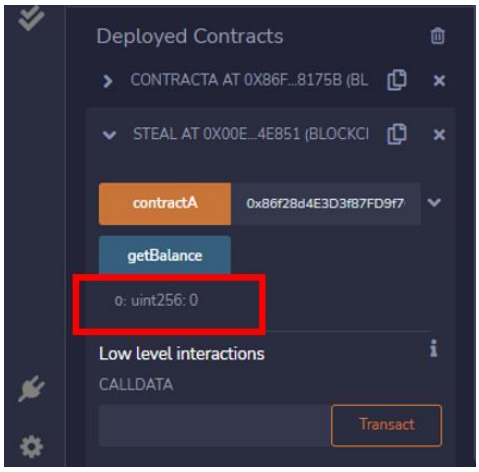
Gambar 4 Tampilan burpsuite pada website test

Namun karena data pada jaringan *blockchain* terenkripsi dengan adanya hashing, sehingga pada tahap pengujian untuk membaca data melalui burpsuite, data tidak dapat dibaca dan dimengerti oleh manusia karena telah terenkripsi, seperti yang terlihat di Gambar 5.



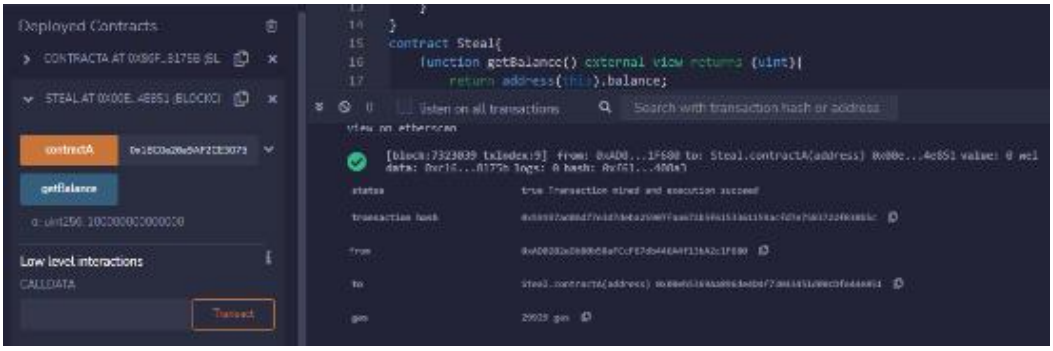
Gambar 5 Tampilan burpsuite pada program

3.1.2 Pengujian kedua berfokus pada *smart contract* yang berjalan pada system, pada system *smart contract* berfungsi untuk menampung dan merangkum *input* yang dimasukkan pada web, membuat *digital signature* dari *private key* pengirim, dan pada saat divalidasi akan menambahkan transaksi kedalam *blockchain*. Meski membawa dampak positif, beberapa oknum pelaku kejahatan dapat saja tetap melakukan kecurangan pada sistem yang dilengkapi dengan *smart contract* ini, salah satunya adalah dengan menguras habis ETH *amount* dari *address* yang dituju si *attacker*, Hal ini dapat ditunjukkan pada Gambar 6 yakni ada sebuah *contract* yang memiliki *balance* awal 0 ETH.



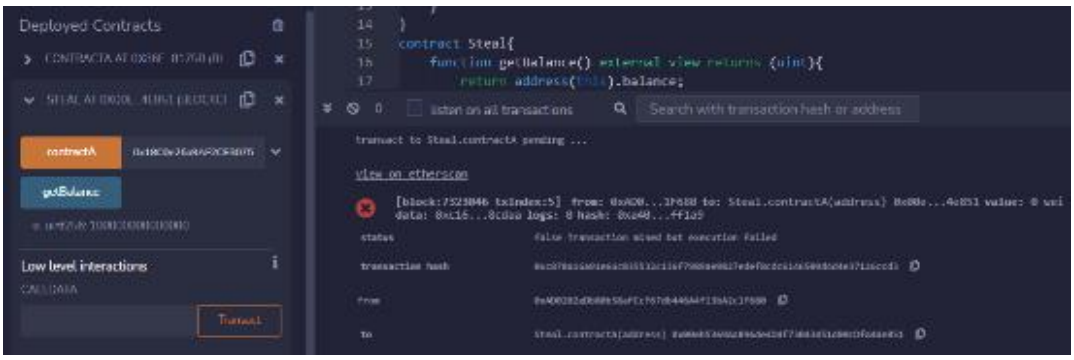
Gambar 6 Balance Awal Steal Contract

Steal Contract yang ada dapat menjalankan fungsi menguras *balance*, seperti yang dilihatkan pada Gambar 7, pada kontrak contoh proses pengurasan *balance* melalui *steal contract* berhasil dilakukan sehingga *balance steal contract* bertambah.



Gambar 7 Balance Stealing Sukses Ke Contract Lain

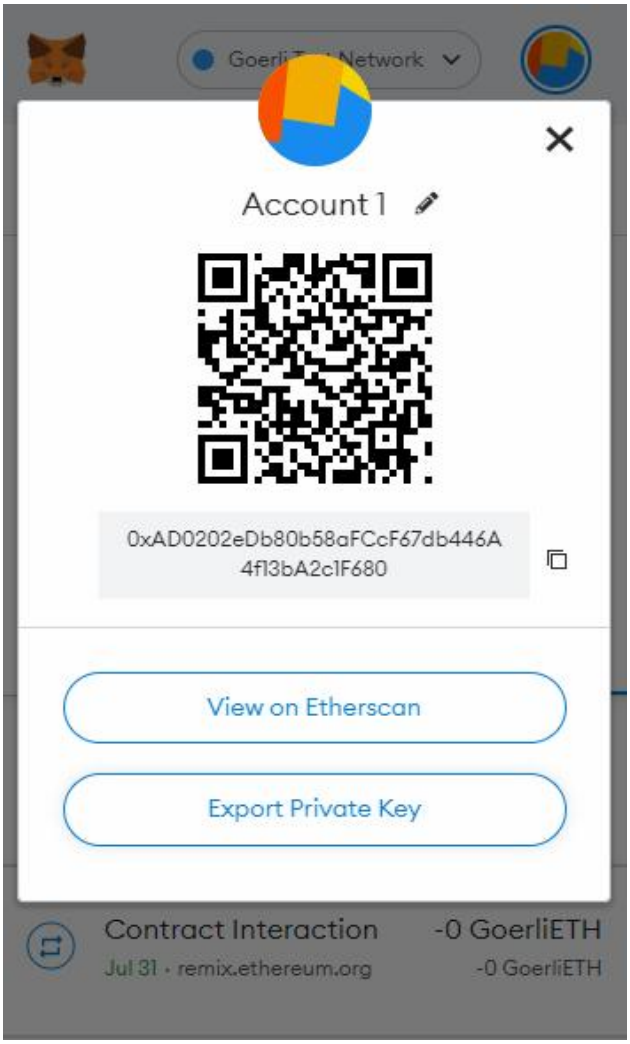
Seperti yang mana telah diketahui bahwa setiap transaksi memerlukan *Ethereum* (ETH) untuk dapat diproses dan masuk kedalam *blockchain*, jumlah ETH yang tidak mencukupi ini akan berdampak langsung pada kelangsungan penyampaian informasi pada *supply chain management* pada sistem yang bergantung pada aplikasi *blockchain* ini, namun seperti yang ditunjukkan pada Gambar 8, program yang dibuat tidak terdampak oleh *contract* jahat.



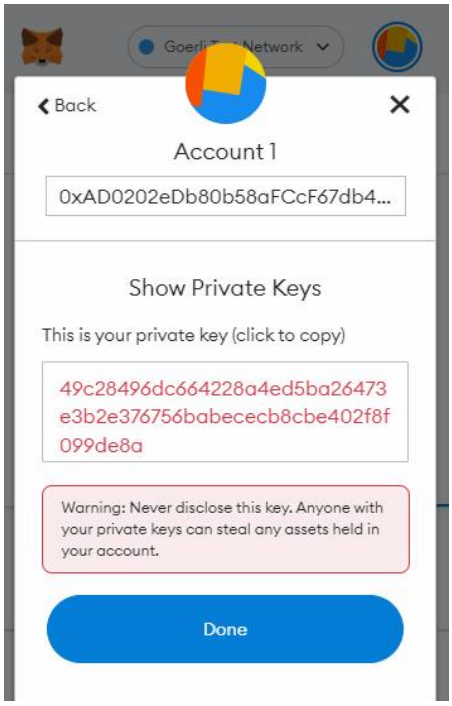
Gambar 8 Balance Stealing Gagal Ke Contract Yang Digunakan Pada Sistem

3.1.3 Keamanan pada *Asymmetric Cryptography* Pada dunia kriptografi, ada dua jenis kriptografi yang sering ditemui yakni *asymmetric cryptography* dan *symmetric cryptography*. *Symmetric cryptography* adalah Teknik kriptografi yang paling umum digunakan dan contoh penggunaannya adalah enkripsi, enkripsi mengubah sebuah objek atau teks menjadi sebuah objek lain yang berbeda dari sebelumnya dan akan menutupi isi asli dari objek yang dienskripsi tersebut. Namun *symmetric cryptography* dinilai masih tergolong mudah untuk dipecahkan selama mengetahui kunci apa yang digunakan untuk melakukan enkripsi tersebut.

Asymmetric cryptography memiliki tingkat keamanan yang lebih tinggi daripada *symmetric cryptography* karena dalam prosesnya melibatkan dua buah (satu pasang) kunci yang berbeda yakni *cryptography* dan *private key*. Pada sistem yang dikerjakan pada penelitian ini menggunakan *Ethereum network* yang memanfaatkan *cryptography* dan *private key*, *cryptography key* merupakan sebuah key yang dapat secara global diketahui oleh semua orang dan dapat menjadi identitas dari pemilik akun tersebut, oleh karena itu *Ethereum address* yang didapatkan dari *metamask* adalah sama dengan *cryptography key* dari akun tersebut. Sementara *private key* merupakan sebuah *key* yang bersifat rahasia dimana setiap pemilik akun wajib untuk menjaga *private key* mereka dari kehilangan dan kebocoran. Pada Gambar 9 ditunjukkan *Public Key* yang diakses melalui *metamask* dapat dengan mudah diketahui oleh pemilik maupun oleh orang lain melalui *etherscan* secara publik



Gambar 9 Public Key Pada Metamask



Gambar 10 Private Key Pada Metamask

Sementara untuk mengetahui *private key*, bahkan pemilik akun harus memasukkan *password* terlebih dahulu untuk mendapatkan akses kepada *private key*-nya sendiri. *Metamask* juga menggarisbawahi hal terkait kerahasiaan dan vitalitas dari *private key* dengan menyatakan informasi tambahan dibawah *private key* yang telah ditampilkan seperti yang ditunjukkan pada Gambar 10. *Private key* digunakan pada transaksi untuk membuat *digital signature* yang menjadi penanda bahwa transaksi adalah valid dan benar dibuat oleh pengirim yang bersangkutan, untuk kemudian dipasangkan dengan *cryptography key* pengirim yang sebelumnya sang penerima sudah mengetahuinya karena notabene mudah didapatkan. Karena tidak mudah diketahui seperti *cryptography key*, orang-orang yang hendak melakukan penyerangan tidak akan dapat melakukan tindakan apabila hanya memiliki *public key*. Tidak seperti aplikasi tersentralisasi lainnya, kehilangan *private key* pada akun akan berdampak fatal karena sistem terdesentralisasi tidak memiliki otoritas utama untuk menawarkan pemulihan atau mengelola kata kunci. Selain itu bila disalahgunakan oleh orang tidak bertanggung jawab, *private key* dapat digunakan untuk melakukan transaksi illegal diluar sepengetahuan pemilik *wallet* asli.

3.2 Analisis

Pada penelitian yang telah dibuat, sistem terlebih dahulu dijalankan dengan melakukan simulasi *supply chain management* pada lingkungan kerja dengan sensor RFID untuk mendapatkan data transaksi dan perjalanan barang, setelah data didapat kemudian data dimasukkan oleh masing-masing *node* yang bersangkutan untuk di-*input*kan kedalam jaringan *blockchain* melalui sebuah *website*. Data yang telah dimasukkan kedalam *blockchain* tidak dapat diubah dan juga tidak dapat dipantau oleh pihak bertanggung jawab melalui *tool* seperti *burpsuite* yang melihat informasi melalui *traffic* yang dikirimkan dari satu lokasi ke lokasi yang lainnya, hal ini dibuktikan dengan informasi pada *traffic* yang terenkripsi dan tidak dapat dibaca oleh manusia. Sistem yang dibuat mudah dioperasikan dan menampilkan informasi yang mudah

dilihat oleh pengguna legal, sistem juga dinilai sudah cukup aman untuk menyimpan data dari *supply chain management* yang dijalankan karena tersimpan didalam jaringan *blockchain*. Didalam tingkat keamanan pada *smart contract* dan *private key* juga sistem dinilai penulis sudah aman, dibuktikan dengan pengujian keamanan sistem yang sudah dilakukan dan menghasilkan *output* yang positif dan aman dari beberapa jenis *threat.*

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan penulis, didapatkan kesimpulan diantaranya adalah implementasi *RFID* untuk proses pembacaan dan *input* data pada *supply chain management* berhasil dilakukan dengan menyusun *RFID Antenna* sesuai tujuan, melakukan skenario perjalanan barang mulai dari Produsen menuju ke Distributor, diteruskan ke Toko dan dijual kepada konsumen, serta menjalankan pembacaan data melalui *RFID Reader, yang* mampu diintegrasikan dengan teknologi *Blockchain* untuk mendapatkan transparansi kualitas produk serta ketertelusuran perjalanan produk yang berjalan melalui *system supply chain management*, hal ini dibuktikan dengan tampilan *web* yang berhasil dibuat.

Penelitian mampu menghasilkan sistem yang memiliki sifat *traceability* yang baik, data terbukti *immutable,* dan aman dari *threat*. Hal ini dibuktikan dengan pengujian sistem yang mampu menampilkan informasi *supply chain management* dan pengujian keamanan sistem yang menunjukkan bahwa data sudah terenkripsi sehingga data tidak diketahui oleh pihak yang tidak bertanggung jawab serta aman dari tindak kecurangan lainnya seperti pencurian.

5. SARAN

Penelitian mendatang berikutnya dapat dilanjutkan dengan pembuatan *blockchain* secara *realtime* dengan melibatkan *node-node* yang berpartisipasi secara langsung untuk mencapai desentralisasi, *traceability*, transparansi, dan sifat *immutable* yang lebih baik lagi. Kemudian sistem dapat ditingkatkan dengan perancangan sistem *blockchain* yang lebih baik lagi kedepan. Penelitian juga dapat dilanjutkan dengan menggunakan algoritma dan metode lainnya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Laboratorium Elektronika dan Sistem Digital yang telah memberikan dukungan berupa fasilitas dan peralatan selama penelitian ini berlangsung.

DAFTAR PUSTAKA

[1] X. Zhang *et al.*, “Blockchain-based safety management system for the grain supply chain,” *IEEE Access*, vol. 8, pp. 36398–36410, 2020, doi: 10.1109/ACCESS.2020.2975415.

[2] S. E. Chang and Y. Chen, “When blockchain meets supply chain: A systematic literature review on current development and potential applications,” *IEEE Access*, vol. 8, pp. 62478–62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[3] K. Wang, J. Dong, Y. Wang, and H. Yin, “Securing Data with Blockchain and AI,”

IEEE Access, vol. 7, pp. 77981–77989, 2019, doi: 10.1109/ACCESS.2019.2921555.

[4] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Comput. Ind. Eng.*, vol. 135, no. June, pp. 582–592, 2019, doi: 10.1016/j.cie.2019.06.042.

[5] S. Köhler and M. Pizzol, "Technology assessment of blockchain-based technologies in the food supply chain," *J. Clean. Prod.*, vol. 269, 2020, doi: 10.1016/j.jclepro.2020.122193.

[6] D. Bumblauskas, A. Mann, B. Dugan, and J. Rittmer, "A blockchain use case in food distribution: Do you know where your food has been?," *Int. J. Inf. Manage.*, vol. 52, no. September 2019, p. 102008, 2020, doi: 10.1016/j.ijinfomgt.2019.09.004.

[7] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains," *IEEE Access*, vol. 7, pp. 7273–7285, 2019, doi: 10.1109/ACCESS.2018.2890389.

[8] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

[9] G. Perboli, S. Musso, and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018, doi: 10.1109/ACCESS.2018.2875782.

[10] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?," *Futur. Internet*, vol. 10, no. 2, pp. 8–13, 2018, doi: 10.3390/fi10020020.

[11] A. Tumpal, L. Sianturi, and A. F. Oklilas, "Penerapan Teknologi Blockchain pada Sistem Supply Chain Management yang Terintegrasi dengan Sensor RFID (Paper Review)," *J. Sist. Inf.*, vol. 14, no. 1, 2022, [Online]. Available: http://ejournal.unsri.ac.id/index.php/jsi/index