BAB 1

PENDAHULUAN

1.1 Latar Belakang

Hyperledger Fabric merupakan sebuah *open-source platform* berbasis *permissioned blockchain* yang dibuat oleh IBM dan Linux Foundation (Hyperledger Fabric 1.4 Documentation, 2020). Hyperledger Fabric merupakan sebuah *permissioned blockchain* di mana tidak semua orang dapat bergabung ke dalam suatu *network* dan hanya orang yang telah menjadi anggota yang dapat mengakses *network* tersebut (Nasir *et al.*, 2018). Setiap transaksi yang terjadi pada *platform* ini dikendalikan oleh sebuah kode program untuk dapat berinteraksi dengan jaringan. Kode program ini dikenal dengan sebutan *chaincode* (Nasir *et al.*, 2018).

Hyperledger Fabric menggunakan algoritma kriptografi asimetrik Rivest-Shamir-Adleman (RSA) atau algoritma kriptografi asimetrik Eliptic Curve Digital Signature Algorithm (ECDSA) pada *digital signature*, dimana *digital signature* ini bertujuan untuk memberikan *signature* pada transkasi yang dibuat (Hyperledger Fabric 1.4 Documentation, 2020). Arsitektur yang digunakan pada platform ini berbentuk *execute-order-validate* yang berhasil mengatasi kekurangan yang dimiliki oleh *permissioned blockchain* pada umumnya yang memiliki bentuk arsitektur *order-execute* (Androulaki *et al.*, 2018). Pada tahap *excecute* akan dilakukan pengecekan diawal pada transaksi yang akan dimasukkan ke dalam *block*, lalu dilanjutkan pengiriman transaksi yang telah dicek ke tahap *order* di mana *orderer* akan membuat transaksi tersebut menjadi sebuah block dan

dilakukan tahap *validate* untuk melakukan validasi transaksi yang sudah berada di dalam *block* (Androulaki *et al.*, 2018).

Pada tahun 1994, ditemukan sebuah algoritma oleh Peter Shor yang menunjukkan bahwa sebuah komputer kuantum dapat menyelesaikan permasalahan faktorisasi bilangan prima besar pada RSA dalam waktu yang lebih singkat dibandingkan dengan komputer klasik saat ini (Gerjuoy, 2004). Jika komputer kuantum memiliki 4099 *qubits* yang stabil berhasil ditemukan, maka enkripsi RSA-2048 dapat dipecahkan hanya dalam 10 detik (Baumhof, 2019). Adanya komputer dan algoritma kuantum menyebabkan algoritma klasik saat ini rentan terhadap serangan kuantum. Oleh karena itu, banyak peneliti mencari cara baru yang lebih sulit untuk dipecahkan oleh algoritma kuantum.

Pada tahun 2016 yang lalu, National Institute of Standards and Technology (NIST) melakukan *call for proposals* untuk *post-quantum cryptosystems* yang bertujuan untuk memilih sejumlah kandidat *cryptosystems* yang dapat diterima sebagai standar dari *post-quantum cryptography* (*Call for Proposals*, 2020). Pada tanggal 22 Juli 2020, NIST mengumumkan finalis yang masuk tahap putaran ketiga dari *call for proposals* ini (*Workshops and timeline*, 2020). Terdapat total tujuh finalis algoritma *post-quantum cryptography*, di mana empat algoritma *public-key encryption and key-establishment* dan tiga algoritma *digital signature* (*PQC Standardization Process: Third Round Candidate Announcement*, 2020). Selain tujuh finalis ini, dipilih juga total delapan kandidat alternatif algoritma *post-quantum cryptography*, di mana lima algoritma *public-key encryption and key-establishment* dan tiga algoritma *digital signature*.

Berdasarkan penjabaran di atas, *blockchain* memerlukan perlindungan tambahan berupa enkripsi data di dalamnya. Penggunaan enkripsi bertujuan untuk melindungi privasi data sehingga pihak lain tidak dapat melihat isi data tersebut. Enkripsi akan dilakukan pada data transaksi menggunakan algoritma enkripsi yang dipercaya tahan dari serangan kuantum. Penelitian ini akan menerapkan skema *hybrid encryption* di mana *public key* dari algoritma *post-quantum* akan digunakan untuk mengenkapsulasi *key random*. *Key random* ini lalu akan digunakan kembali untuk melakukan enkripsi simetrik pada data transaksi. Skema *hybrid encryption* digunakan karena memberikan efektifitas dari skema *symmetric encryption* serta kenyamanan dari skema *asymmetric encryption* (Patil and Bansode, 2020). Pada *symmetric encryption*, enkripsi dan dekripsi data yang besar dapat dilakukan dalam waktu yang lebih cepat daripada *asymmetric encryption.* Pada *asymmetric encryption, keys* yang digunakan untuk berkomunikasi tidak perlu dibagikan lagi karena setiap pihak memiliki *public* dan *private key* masing-masing.

Oleh karena itu, penelitian ini berfokus pada pengimplementasian *hybrid encryption* di mana algoritma *symmetric encryption* yang dipakai adalah AES-256 dan algoritma *asymmetric encryption* yang dipakai adalah algoritma *post-quantum cryptography* yang berhasil masuk menjadi finalis tahap putaran ketiga dari *call for proposals* yang dilakukan oleh NIST. Algoritma *asymmetric encryption* yang dipilih untuk diimplementasikan adalah algoritma *public-key encryption and key-establishment* CRYSTALS-Kyber. CRYSTALS-Kyber memiliki tiga *keysize* yaitu Kyber512, Kyber768, dan Kyber1024 (Avanzi *et al.*, 2020). Algoritma ini akan diterapkan menggunakan *framework* Hyperledger Fabric dan

diimplementasikan pada aplikasi autentikasi produk Oricon. Penelitian ini dilakukan untuk mengukur performa dari segi transaksi sukses, transaksi gagal, *latency* dan *throughput* yang dihasilkan serta waktu yang dibutuhkan untuk melakukan *key generation*, enkripsi, dan dekripsi dari pengimplementasian algoritma *post-quantum cryptography* CRYSTALS-Kyber dengan tiga *keysize* berbeda.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan sebelumnya, maka dirumuskan masalah sebagai berikut.

1. Bagaimana cara pengimplementasian algoritma *post-quantum cryptography* CRYSTALS-Kyber pada aplikasi autentikasi produk Oricon?
2. Bagaimana performa dari implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dinilai dari segi transaksi sukses, transaksi gagal, *latency* dan *throughput* yang dihasilkan?
3. Bagaimana performa dari implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dinilai dari segi waktu yang dibutuhkan untuk melakukan *key generation*, enkripsi, dan dekripsi dengan tiga *keysize* berbeda?

1.3 Batasan Masalah

Berdasarkan penjabaran rumusan masalah sebelumnya dan untuk menjaga penelitian tetap berjalan di jalur seharusnya, maka batasan masalah yang ditentukan pada penelitian ini adalah sebagai berikut.

1. Implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber hanya diterapkan pada *framework* Hyperledger Fabric menggunakan *virtual machine* Ubuntu.
2. Penelitian ini tidak berfokus pada perancangan antarmuka program.
3. Algoritma *post-quantum cryptography* CRYSTALS-Kyber hanya diimplementasikan pada *smart contract* aplikasi autentikasi produk Oricon.
4. Implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dilakukan pada aplikasi autentikasi produk Oricon yang dibuat pada penelitian Wilson Philips (Philips, 2021).

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijabarkan sebelumnya, penelitian ini memiliki 2 tujuan sebagai berikut.

1. Mengimplementaskan algoritma *post-quantum cryptography* CRYSTALS-Kyber pada aplikasi autentikasi produk Oricon.
2. Mengukur performa dari implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dinilai dari segi transaksi sukses, transaksi gagal, *latency* dan *throughput* yang dihasilkan.
3. Mengukur performa dari implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dinilai dari segi waktu yang dibutuhkan untuk melakukan *key generation*, enkripsi, dan dekripsi dengan tiga *keysize* berbeda.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memiliki manfaat sebagai berikut.

1. Menunjukan cara pengimplementasian algoritma *post-quantum cryptography* CRYSTALS-Kyber pada *blockchain*.
2. Mengetahui performa dari implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dinilai dari segi transaksi sukses, transaksi gagal, *latency* dan *throughput* yang dihasilkan.
3. Mengetahui performa dari implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber dinilai dari segi waktu yang dibutuhkan untuk melakukan *key generation*, enkripsi, dan dekripsi dengan tiga *keysize* berbeda.

1.6 Sistematika Penulisan

Sistematika penulisan yang dilakukan dalam laporan skripsi ini adalah sebagai berikut.

BAB 1 PENDAHULUAN

Bab 1 Pendahuluan berisi latar belakang pengambilan skripsi berjudul "Implementasi Algoritma Post-Quantum Cryptography CRYSTALS-Kyber pada Aplikasi Autentikasi Produk Oricon", rumusan masalah yang ditemukan, tujuan dari penelitian yang dilakukan, manfaat yang didapat dari penelitian, serta sistematika penulisan skripsi.

BAB 2 LANDASAN TEORI

Bab 2 Landasan Teori berisi teori-teori yang digunakan pada penelitian. Jurnal ilmiah, *conference proceeding*, serta *website* digunakan sebagai sarana pencarian teori yang dibutuhkan pada penelitian. Teori-teori yang

digunakan pada penelitian ini, yaitu teori mengenai algoritma *post-quantum cryptography* CRYSTALS-Kyber, aplikasi autentikasi produk Oricon, dan Hyperledger Caliper.

BAB 3 METODOLOGI PENELITIAN

Bab 3 Metodologi Penelitian berisi metodologi yang digunakan pada penelitian dan juga perancangan program yang dibuat. Metodogi penelitian yang digunakan yaitu telaah literatur, perancangan dan implementasi, pengujian, evaluasi, dan dokumentasi. Perancangan program dibuat dengan menggunakan *flowchart* untuk mempermudah pemahaman alur jalannya program.

BAB 4 HASIL DAN DISKUSI

Bab 4 Hasil dan Diskusi berisi hasil implementasi algoritma *post-quantum cryptography* CRYSTALS-Kyber menggunakan Bahasa pemrograman Javascript dengan Node.js SDK. Dilakukan juga pengujian implementasi menggunakan metode *blackbox testing* yang bertujuan mengetahui performa dari algoritma *post-quantum cryptography* CRYSTALS-Kyber dengan *key size* berbeda pada *smart contract* aplikasi autentikasi produk Oricon.

BAB 5 SIMPULAN DAN SARAN

Bab 5 Simpulan dan Saran berisi kesimpulan dari pengujian yang telah dilakukan dan dievaluasi serta berisi saran terkait penelitian serupa yang akan dilakukan peneliti lain pada penelitian selanjutnya