Identity Provider Berbasis *Blockchain* untuk *Messaging App*

M Algah Fattah Illahi (13517122)[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517122@std.stei.itb.ac.id

***Abstract*—Perkembangan teknologi informasi memberi dampak yang besar terhadap cara manusia berkomunikasi, terutama dengan orang yang berada jauh dari mereka, baik dengan orang yang akrab dikenal maupun orang yang sama sekali asing. Komunikasi dengan menggunakan media internet relatif lebih cepat dan efisien, namun dibalik kelebihannya ini komunikasi lewat internet memiliki ancaman berupa jaminan kerahasiaan dan keaslian dari pesan dan pengirimnya. Penjaminan kerahasiaan dan keaslian dari pesan dapat dibantu dengan menggunakan kriptografi, namun identitas dari pengirim dan atau penerima pesan menjadi sebuah tantangan tersendiri. Pada saat ini berbagai *messaging app* menyediakan *identity provider* miliknya sendiri yang terletak pada server tersentralisasi milik *messaging app*, yang rentan terhadap kekurangan dari pihak *messaging app*. Makalah ini akan membahas identity provider berbasis blockchain yang dibangun untuk messaging app.**

Keywords—Identity Provider, blockchain, end-to-end encryption.

I. Pendahuluan

Perkembangan teknologi informasi memberi kemudahan dalam komunikasi jarak jauh, terutama komunikasi via internet. Komunikasi jarak jauh via internet dapat dilakukan lewat berbagai media seperti VoIP, email, dan messaging app. Messaging app sangat praktis digunakan untuk berkirim pesan antar penggunanya. Komunikasi via messaging app dapat dilakukan *1 on 1* antar pengguna atau lewat sebuah grup perpesanan. Dibalik kemudahan dari penggunaan messaging app sebagai media komunikasi, terdapat ancaman keamanan berupa ancaman kerahasiaan dan keaslian dari pesan dan pihak-pihak yang terlibat dalam pertukaran pesan. Ancaman yang menyangkut kerahasiaan dan keaslian dari pesan dapat diselesaikan dengan menggunakan kriptografi, baik itu kriptografi simetris dan asimetris. Namun ancaman terkait keaslian dari pengirim dan penerima pesan menjadi sebuah tantangan tersendiri. Untuk mengatasi ancaman tersebut, dibutuhkan sebuah *identity provider* yang menyediakan kunci publik dan identitas dari pihak-pihak yang terlibat dalam pertukaran pesan.

Pada saat ini berbagai messaging app yang sudah menerapkan end-to-end encryption, menggunakan identity provider yang terletak dalam server milik messaging app. Identity provider yang terletak dalam server tersentralisasi tersebut rawan akan ancaman kecurangan dari pihak messaging app. Kurangnya transparansi memungkinkan pihak messaging app untuk memalsukan public key yang diminta oleh pengguna, yang akan berujung bocornya pesan yang seharusnya hanya dapat dibaca oleh pengirim dan penerima pesan.

Untuk mengatasi isu transparansi tersebut, dapat dibangun sebuah identity provider yang terdesentralisasi berbasis blockchain.

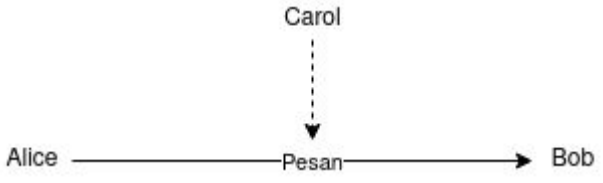
II. Landasan Teori

A. Kriptografi

Kriptografi merupakan cabang ilmu yang mempelajari tentang cara mengubah pesan sehingga pesan tersebut tidak dapat dibaca oleh pihak yang tidak diinginkan tanpa mengetahui algoritma dan kunci yang digunakan. Kriptografi memiliki beberapa aspek yaitu kerahasiaan, integritas pesan, autentikasi dan non repudiation.

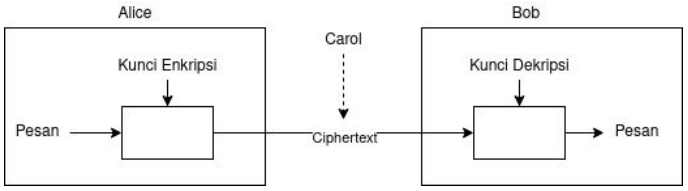
B. Kriptografi Kunci Simetris

Enkripsi merupakan sebuah proses penyandian pesan atau informasi dengan cara tertentu sehingga pesan tersebut hanya dapat dibaca oleh pihak yang berwenang, yang mengetahui algoritma dan kunci yang digunakan dalam penyandian pesan tersebut.



Gambar II.1 Pengiriman pesan tanpa enkripsi

Pada ilustrasi di atas, pesan yang dikirimkan oleh Alice kepada Bob dapat disadap oleh Carol. Karena pesan dikirimkan tanpa adanya enkripsi, Carol tidak punya kesulitan dalam memahami informasi yang ia sadap.



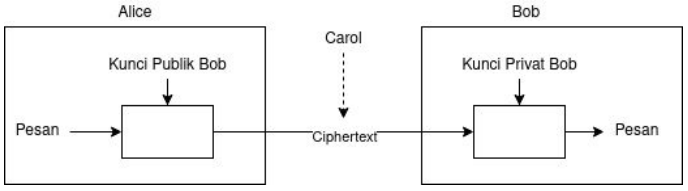
Gambar II.2 Pengiriman pesan dengan enkripsi

Pada gambar di atas, Alice mengirimkan pesan kepada Bob, tapi sebelum pengiriman pesan dilakukan, pesan tersebut dienkripsi terlebih dahulu dengan menggunakan kunci enkripsi (K_e) yang sudah disetujui oleh Alice dan Bob sebelum memulai komunikasi ini. Ciphertext yang dihasilkan dari proses enkripsi kemudian dikirimkan kepada Bob. Untuk mengembalikan pesan dari ciphertext tersebut, Bob melakukan dekripsi terhadap ciphertext dengan menggunakan kunci dekripsi (K_d). Kunci yang digunakan oleh Alice untuk melakukan enkripsi (K_e) dan kunci yang digunakan Bob untuk melakukan dekripsi bernilai sama. Skema enkripsi yang seperti ini disebut dengan enkripsi kunci simetris. Dimana untuk pesan *m*, fungsi enkripsi *E*, fungsi dekripsi *D*, dan kunci *K*, berlaku

$$m = D(K, E(K, m)).$$

C. Kriptografi Kunci Publik

Enkripsi kunci publik merupakan metode enkripsi yang melibatkan dua kunci, kunci publik yang dapat disebarkan secara bebas, dan kunci privat yang hanya boleh diketahui oleh pemilik (Bellare, Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements, 2000). Pada enkripsi kunci publik, proses enkripsi pesan dilakukan dengan menggunakan kunci publik dan dekripsi pesan dilakukan dengan menggunakan kunci privat. Beberapa algoritma yang mengimplementasikan skema kunci publik adalah RSA dan ElGamal.



Gambar II.3 Skema enkripsi dan dekripsi kunci publik

Pada gambar di atas, Alice mengirimkan pesan kepada Bob. Sebelum pengiriman pesan dimulai, Bob membangkitkan pasangan kunci publik dan privat, kemudian membagikan kunci publik miliknya (K_p) kepada Alice. Alice kemudian melakukan enkripsi pesan menggunakan K_p untuk menghasilkan ciphertext dan mengirimkan ciphertext tersebut kepada Bob. Bob yang sudah menerima ciphertext dari Alice kemudian akan melakukan dekripsi dengan menggunakan kunci privat miliknya (K_s) untuk mendapatkan pesan kembali. Carol berhasil menyadap ciphertext yang dikirimkan tidak akan bisa mendapatkan pesan asli sebab ia tidak memiliki kunci privat milik Bob.

Pada skema enkripsi ini, kunci yang digunakan untuk melakukan enkripsi dan dekripsi memiliki nilai yang berbeda. Untuk pesan *m*, fungsi enkripsi *E*, fungsi dekripsi *D*, kunci publik K_p dan kunci privat K_s berlaku aturan

$$m = D(K_s, E(K_p, m))$$

D. Public Key Infrastructure

Public key infrastructure merupakan sebuah infrastruktur yang menyediakan layanan untuk membuat, menyimpan, memverifikasi, dan membuang sertifikat digital. Sertifikat digital merupakan sebuah dokumen digital yang berisi informasi-informasi seperti nama subjek, kunci publik milik subjek, waktu kadaluarsa, dan informasi relevan lain. Sertifikat digital digunakan untuk melakukan pencegahan terhadap impersonation attack, yang rawan terjadi pada enkripsi kunci publik.

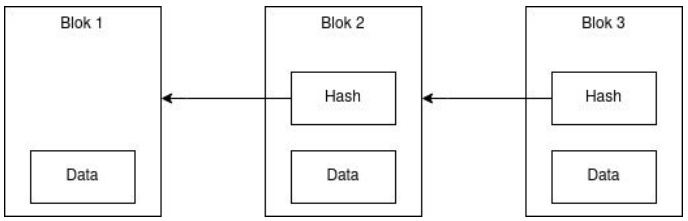
Impersonation attack merupakan serangan dimana seseorang menyamar menjadi pemilik dari kunci publik milik orang lain. Contohnya dalam seorang pelanggan yang ingin mengirimkan informasi kartu kreditnya melalui sebuah *website* toko *online*, informasi tersebut akan dilindungi kerahasiaannya dengan mengenkripsinya dengan menggunakan kunci publik milik *website* toko *online*. Permasalahannya adalah bagaimana cara pelanggan memastikan bahwa kunci publik tersebut memang benar milik *website* toko *online* tersebut.

Certification authority (CA) merupakan pihak yang dipercaya untuk menerbitkan sertifikat digital. CA menandatangani sebuah sertifikat digital dengan cara mengenkripsi nilai hash dari sertifikat dengan kunci privat milik CA.

E. Blockchain

Blockchain merupakan sebuah distributed ledger yang menyimpan data transaksi yang telah terjadi (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016). Blockchain bersifat immutable yang berarti blok yang sudah ditambahkan ke dalam rantai blockchain tidak dapat dihapus atau diubah, yang memastikan data blockchain yang tersebar pada jaringan konsisten. Selain itu blockchain juga bersifat terdesentralisasi yang menyebabkan tidak ada sebuah sistem sentral yang memiliki akses penuh pada catatan transaksi yang ada dalam blok-blok blockchain. Validitas data pada blockchain dipastikan dengan melakukan konsensus pada mayoritas sistem yang ada.

Secara harfiah, blockchain adalah rantai yang terdiri dari blok-blok. Disebut rantai karena setiap blok pada blockchain terhubung dengan blok lainnya dengan menyimpan nilai hash dari blok sebelumnya. (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).



Gambar II.3 Arsitektur umum Blockchain

Pada gambar II.3 dapat dilihat bagaimana blok pada blockchain menyimpan datanya. Blok genesis atau blok pertama tidak menyimpan nilai hash dari blok lain karena tidak ada blok sebelumnya. Blok 2 akan menyimpan nilai hash dari blok 1 sebagai parent hash value, blok 3 menyimpan nilai hash dari blok 2 dan seterusnya. Untuk memverifikasi sebuah blockchain, sistem melakukan traversal dari blok 1 hingga blok terakhir dan membandingkan nilai hash dari blok sebelumnya dengan nilai parent hash value yang disimpan oleh suatu blok. Jika ada pihak yang merubah nilai blok, nilai hash dari blok tersebut akan berubah dan membuat blockchain tersebut menjadi tidak valid karena nilai hashnya tidak sesuai dengan parent hash value yang disimpan pada blok berikutnya.

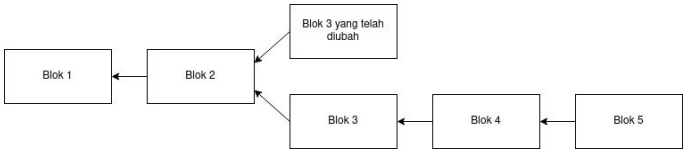
F. Algoritma Konsensus

Algoritma konsensus adalah cara untuk meningkatkan reliabilitas dalam sebuah sistem terdesentralisasi. Proses ini biasanya memerlukan sistem-sistem untuk menyetujui sebuah nilai yang sama. Dalam blockchain, algoritma konsensus digunakan untuk mencapai kesepakatan keadaan sebenarnya dari sebuah rantai blok. Dalam hal ini, algoritma konsensus dalam blockchain memastikan setiap peer dalam blockchain mengacu pada data yang sama (Coulouris, Dollimore, & Kindberg, 2001).

Beberapa algoritma konsensus meliputi, tapi tidak terbatas pada:

- Proof-of-Work

  Proof of Work merupakan salah satu algoritma konsensus pertama untuk blockchain yang digunakan dalam bitcoin blockchain. Protokol bitcoin menentukan bahwa untuk menghasilkan sebuah blok yang valid, seorang pembuat blok harus memberikan bukti bahwa dia telah menggunakan daya pemrosesan yang cukup banyak dalam pembuatan bloknya (Nakamoto, 2008). Proof of Work biasanya berupa jawaban dari persoalan matematika yang hanya dapat ditemukan dengan mencoba bilangan acak satu per satu. Bukti ini diperlukan agar tidak ada komputer yang mampu menambahkan blok ilegal atau mengubah blok ke dalam rantai blok.



Gambar II.4 Ilustrasi peer tidak bertanggung jawab yang berusaha menambahkan blok yang tidak valid

Dalam bitcoin, peer yang berhasil menambahkan blok valid ke dalam rantai terpanjang akan mendapat insentif berupa sejumlah bitcoin, ini memastikan peer yang terdapat dalam jaringan termotivasi untuk mendapatkan coin dengan cara jujur ketimbang dengan cara ilegal, seperti menambahkan transaksi yang tidak valid (Nakamoto, 2008). Jika memang ada peer yang berusaha memalsukan transaksi dalam blok, maka dia harus membuat blok secepat mungkin sehingga rangkaian blok yang dia buat lebih panjang dari rantai blok yang valid. Kasus ini hanya dapat terjadi jika lebih dari setengah kekuatan komputasi yang terdapat pada jaringan dikuasai oleh penyerang (51% attack).

- Proof-of-Stake

  Berbeda dengan Proof-of-Work, algoritma konsensus Proof-of-Stake tidak melibatkan kompetisi dalam pembentukan blok baru. Validator dipilih berdasarkan stake yang dimiliki oleh peer, semakin banyak stake yang dimiliki oleh peer, maka semakin besar kemungkinan perr untuk menjadi validator. Hal ini sangat efektif dalam mengatasi penggunaan energi dan waktu yang besar dalam penambahan blok seperti pada algoritma konsensus Proof-of-Work.

G. Framework Blockchain

Beberapa framework blockchain namun tidak terbatas pada:

- Ethereum

  Ethereum merupakan salah satu penerapan blockchain yang mampu menjalankan smart contract. Smart contract merupakan sebuah mekanisme yang melibatkan aset digital dan dua pihak atau lebih, dimana sebagian atau seluruh pihak memasukkan aset, dan aset secara otomatis didistribusikan kembali di antara pihak-pihak tersebut sesuai dengan formula yang terdapat pada kontrak (Buterin, 2013). Ethereum merupakan blockchain publik yang berarti setiap komputer dapat bergabung dalam jaringan dan terlibat dalam transaksi dan konsensus tanpa perlu melalui proses autentikasi terlebih dahulu.

  Jaringan blockchain Ethereum terbentuk dari peer yang tidak terautentikasi, yang menyebabkan tidak adanya rasa percaya antar peer. Karena hal itu Proof of Work dipilih sebagai algoritma konsensus, yang menggunakan daya komputasi sebagai landasan kepercayaan.

- Hyperledger Fabric

  Hyperledger Fabric merupakan salah satu penerapan blockchain yang mampu menjalankan *smart contracts* yang memiliki arsitektur modular (Cachin, 2016). Dalam implementasinya, Hyperledger membuat sebuah distributed ledger dengan sistem perizinan. Implementasi sistem perizinan pada Hyperledger dibuat dengan membagi sebuah peer dengan izin melakukan validasi dan tanpa izin. Hanya peer dengan izin melakukan validasi yang dapat melakukan transaksi dan menyatakan

konsensus. *Peer* tanpa izin hanya dapat membaca data yang terdapat dalam blockchain.

Sistem validasi yang digunakan oleh Hyperledger membuat setiap komputer yang terdapat dalam jaringan blockchain Hyperledger setidaknya harus dipercaya oleh komputer lain. Hal ini membuat Hyperledger memilih BFT sebagai algoritma konsensusnya (Cachin, 2016). BFT memiliki performa yang jauh lebih baik jika dibandingkan dengan Proof of Work (POW) yang digunakan oleh Bitcoin, yang membuat Hyperledger memiliki performa yang lebih unggul dibandingkan Bitcoin.

H. End-to-End Encryption

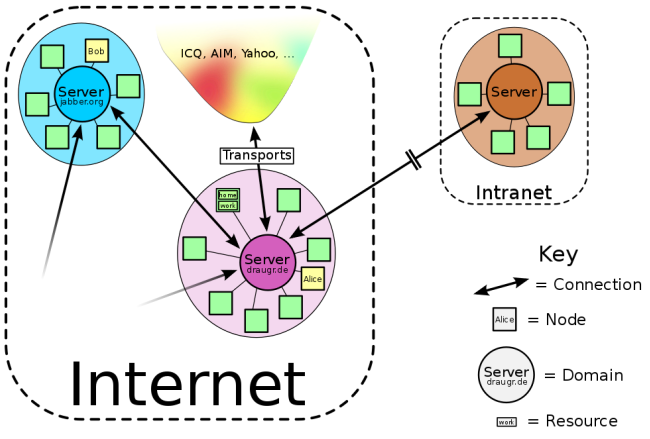
End-to-end encryption merupakan sistem komunikasi dimana hanya pihak-pihak yang berkomunikasi yang dapat membaca pesan. Hal ini dimaksudkan untuk mencegah terjadinya *eavesdropping* dan *man-in-the-middle attack.* Dalam banyak *messaging system*, pesan dikirimkan dengan menggunakan perantara dan disimpan oleh pihak ketiga. Meskipun pesan yang dikirim terenkripsi, tapi jika enkripsi dilakukan dengan menggunakan kunci privat yang diketahui oleh pihak ketiga, maka pihak ketiga dapat membaca pesan tersebut.

End-to-end encryption dimaksudkan untuk mencegah pesan yang dikirimkan dibaca atau diubah dalam proses pengirimannya. Pesan dikirimkan menggunakan perantaraan pihak ketiga, namun pihak ketiga tidak mengetahui kunci yang digunakan untuk dekripsi sehingga hanya penerima yang dimaksud yang mampu mendekripsi pesan tersebut.

Beberapa protokol perpesanan, tetapi tidak terbatas pada:

- Extensible Messaging and Presence Protocol

  Extensible Messaging and Presence Protocol (XMPP) merupakan sebuah protokol komunikasi berbasis XML yang memungkinkan pertukaran data yang terstruktur namun *extensible* antara dua atau lebih entitas dalam jaringan secara *near-real-time.*



Gambar II.5 Jaringan XMPP sederhana

Jaringan XMPP menggunakan arsitektur *client-server* yang berarti *client* tidak berkomunikasi secara langsung satu sama lain. Model dari jaringan ini terdesentralisasi, siapapun dapat menjalankan *server*. Setiap *user* dalam jaringan memiliki XMPP *address* unik yang disebut JID.

- Signal Protocol

Signal Protocol atau sebelumnya dikenal sebagai TextSecure Protocol merupakan sebuah *non-federated cryptographic protocol* yang dapat digunakan untuk menyediakan *end-to-end encryption* untuk panggilan dan pesan. Protokol ini menggunakan algoritma Double Rachet, prekeys, dan 3-DH handshake, serta menggunakan Curve25519, AES-256 dan HMAC-SHA256 sebagai primitifnya.

Layanan yang disediakan oleh protokol ini antara lain adalah *confidentiality, integrity, authentication, participant consistency, destination validation, forward secrecy, post-compromise security, causality preservation, message unlinkability, message repudiation, participant repudiation,* dan *asynchronicity*. Selain itu protokol ini juga mendukung enkripsi *end-to-end* untuk *group chat*.

Pengguna dapat membandingkan *public key fingerprint* lewat saluran luar guna melakukan autentikasi. Hal ini dilakukan guna memverifikasi identitas satu sama lain dan menghindari serangan *man-in-the-middle*.

III. Analisis Permasalahan

Pada Bab I dan II telah dicantumkan keterbatasan dari *messaging app* yang dibangun dengan *identity provider* yang menggunakan arsitektur tersentralisasi, mulai dari kurangnya transparansi hingga single point-of-failure yang mungkin terjadi pada sistem. Selain itu telah dijelaskan pula tentang persoalan yang melekat pada sistem yang dibangun dengan menggunakan arsitektur terdesentralisasi.

Masalah utama yang akan dibahas adalah terkait transparansi sistem, dimana pada *messaging app* dengan *identity provider* yang tersentralisasi, pengguna tidak dapat memastikan bahwa ketika ia ingin menghubungi pengguna lain, *server* tidak berbuat curang dengan mengirimkan public key miliknya sendiri kepada pengguna tersebut, yang menyebabkan pesan yang yang dikirimkan oleh pengguna dapat dibaca oleh *server* terlebih dahulu sebelum diteruskan kepada pengguna yang dituju. Cara yang dapat digunakan pengguna untuk melakukan autentikasi satu sama lain adalah dengan memeriksa *public key fingerprint* masing-masing secara manual lewat saluran yang aman atau dengan bertemu secara langsung.

Dari permasalahan tersebut, kami mengajukan solusi berupa *messaging app* yang mendukung *end-to-end encryption* dengan *identity provider* berbasis blockchain. Dengan menggunakan blockchain sebagai *identity provider*, isu transparansi yang sebelumnya dibahas dapat diselesaikan karena blockchain merupakan sebuah *public ledger* yang isinya dapat dilihat oleh semua orang dalam jaringan.

IV. Rancangan Solusi

A. Analisis

Solusi yang ditawarkan adalah dengan menggunakan *identity provider* berbasis blockchain. *Messaging app* yang digunakan pada sistem yang hendak dibangun merupakan perangkat lunak *open source* yang dimodifikasi. Untuk itu perlu ditinjau teknologi *messaging app* dan blockchain apa yang akan digunakan pada sistem yang hendak dibangun.

Pada Bab II telah dibahas dua framework blockchain, yaitu Ethereum dan Hyperledger Fabric. Kedua framework tersebut memiliki karakteristik masing-masing. Pada subbab ini akan ditinjau framework mana yang paling sesuai dengan kebutuhan dari sistem yang ingin dibangun.

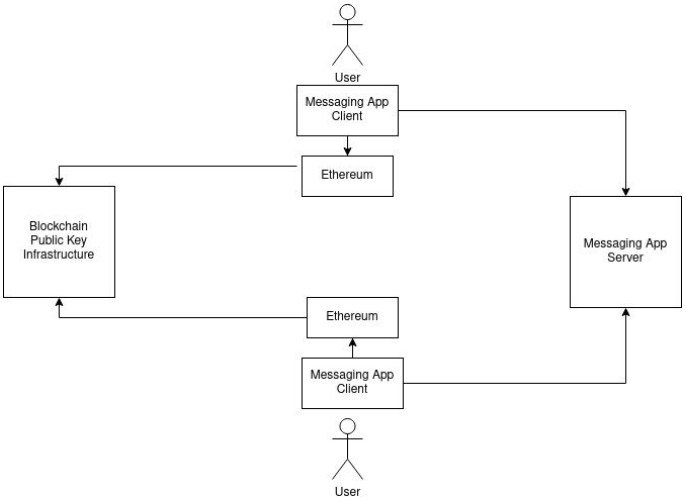
Perbedaan pertama dari kedua framework yang disebutkan diatas adalah hak akses, Ethereum merupakan *public* blockchain yang berarti *node* dapat bergabung dengan jaringan blockchain secara bebas tanpa harus menerima *invitation* dari node yang telah tergabung dalam jaringan. Node yang sudah tergabung dalam jaringan dapat terlibat dalam pencapaian konsensus. Berbeda dengan Ethereum, Hyperledger Fabric merupakan sebuah *private* blockchain, dimana sebuah node harus mendapatkan undangan terlebih dahulu sebelum dapat bergabung ke dalam jaringan, selain itu *peer* yang tergabung dalam jaringan memiliki hak akses yang berbeda, yang menyebabkan tidak semua *peer* dapat terlibat dalam konsensus.

Perbedaan kedua adalah kecepatan *framework* dalam memproses transaksi. Ethereum dengan algoritma konsensus *proof of work* memerlukan 1-2 menit untuk menyelesaikan sebuah transaksi, dengan *throughput* sebesar 10-20 transaksi per detiknya. Sedangkan Hyperledger Fabric memiliki *throughput* sebesar 3500 transaksi per detik.

Dengan menjadikan kedua hal tadi sebagai pertimbangan, Ethereum dirasa lebih cocok untuk sistem yang ingin dikembangkan. Karena transaksi pada blockchain ini akan berisi penerbitan, pencabutan, dan pembaruan pasangan kunci publik yang tidak terlalu intens, karena hanya terjadi ketika pembuatan user baru. Operasi yang akan sering digunakan adalah public key lookup yang tidak membutuhkan konsensus.

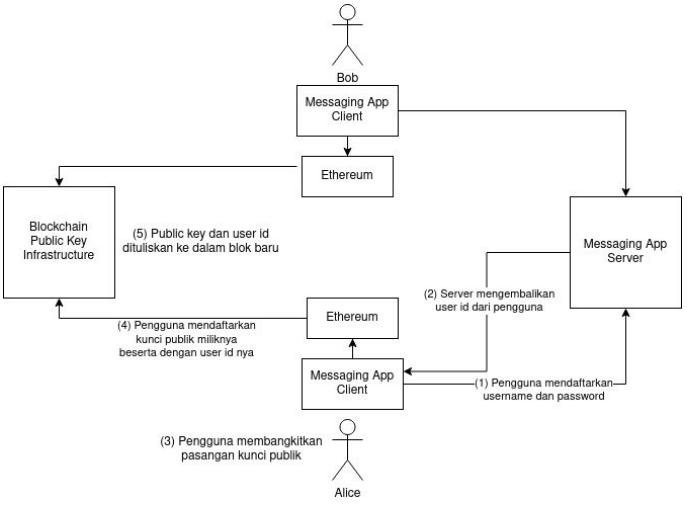
B. Gambaran Umum

Komunikasi antar pengguna dilakukan secara tersentralisasi lewat *server* milik *messaging app*, namun *identity provider* dipisah dari *server* milik *messaging app* dan diimplementasikan dengan menggunakan blockchain. Data yang disimpan pada blockchain adalah *user id* (dari *messaging app*), *public key* milik *user*, dan algoritma *public key* yang digunakan.



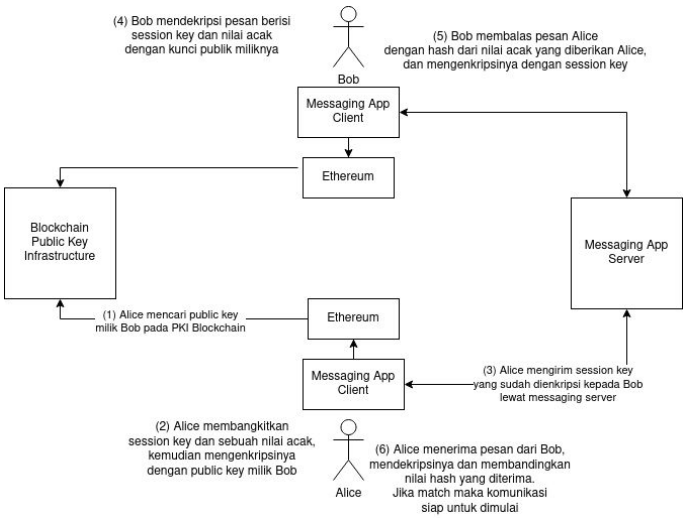
Gambar A.1 Interaksi antar entitas

Alur pendaftaran pengguna dimulai dengan mendaftarkan akun pada messaging app server, kemudian pengguna akan membangkitkan pasangan kunci publik dan privat pada *local machine*, yang kemudian didaftarkan ke dalam *identity provider*.



Gambar A.2 Alur Pendaftaran Pengguna

Alur chatting antar pengguna dimulai dengan Alice melakukan lookup pada *identity provider* untuk mencari public key milik Bob, kemudian Alice mengirimkan pesan berisi session key dan nilai acak yang dienkripsi menggunakan public key milik Bob kepada Bob lewat *messaging app server.* Kemudian Bob mendekripsi pesan tersebut dengan menggunakan kunci privat miliknya. Setelah itu Bob membalas dengan nilai hash dari nilai acak yang diberikan, yang dienkripsi dengan session key. Kemudian Alice membandingkan nilai hash, dan komunikasi dimulai jika nilai hash sesuai.



Gambar A.3 Alur chatting antar pengguna

V. Kesimpulan

Dengan menggunakan *identity provider* berbasis *blockchain* mengatasi isu transparansi yang sebelumnya dimiliki oleh *centralized identity provider*.

VII. Ucapan Terima Kasih

Pertama-tama, penulis berterima kasih kepada Tuhan Yang Maha Esa atas berkat dan rahmatnya makalah tentang *identity provider* berbasis *blockchain* ini dapat diselesaikan. Terima kasih juga kepada Pak Rinaldi selaku pengajar kriptografi yang telah memberikan pengetahuan yang menjadi dasar ilmu pengembangan *identity provider* berbasis *blockchain*. Penulis juga ingin mengucapkan terima kasih kepada seluruh pihak lain yang telah membantu pengerjaan makalah ini.

References

[1] Tanenbaum, A. S., & Steen, M. V. (2002). *Distributed Systems: Principles and Paradigms*. New Jersey/London: Prentice Hall.

[2] Biggs, N. (2008). *Codes: An Introduction to Information Communication and Cryptography.* Springer.

[3] Riverst, R. L., Shamir, A., & Adleman, L. (1977). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*

[4] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin

[5] Buterin, V. (2015). *Ethereum Whitepaper.*

[6] Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers* (DCCL 2016).

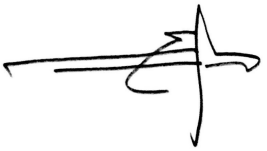
[7] Fromknecht, C., Velicanu, D., Yakoubov, S. (2014). *A NameCoin Based Decentralized Authentication System.*

[8] Axon, L. M., & Goldsmith, M. (2016). *PB-PKI: a privacy-aware blockchain-based PKI. 6.*

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, 21 Desember 2020



M Algah Fattah Illahi (13517122)