

RANCANG BANGUN *WEBSITE* AKADEMIK DENGAN PENYIMPANAN SERTIFIKAT DIGITAL MENGGUNAKAN TEKNOLOGI *BLOCKCHAIN*

Windra Swastika^{1*}, Hermawan Wira Santoso², Oesman Hendra Kelana³

^{1,2,3}Universitas Ma Chung, Malang

Email: ¹ windra.swastika@machung.ac.id, ² 311610009@student.machung.ac.id,

³oesman.hendra@machung.ac.id

*Penulis Korespondensi

(Naskah masuk: 18 Juni 2020, diterima untuk diterbitkan: 27 Februari 2022)

Abstrak

Sertifikat merupakan sebuah bentuk penghargaan yang didapat seseorang setelah menyelesaikan suatu uji kompetensi atau pembelajaran tertentu. Sertifikat harus dibuat dan disimpan dengan metode dan keamanan yang baik untuk mencegah terjadinya perubahan isi atau bahkan pemalsuan. Teknologi *blockchain* merupakan teknologi yang memungkinkan proses penyimpanan yang aman dengan ongkos yang rendah. Keamanan terjamin karena semua orang bisa mengambil bagian untuk menyimpan data dengan *ledger* yang terdistribusi. Berdasarkan hasil penelitian dan perancangan sistem yang dibuat dapat disimpulkan bahwa proses pembuatan teknologi *blockchain* sebagai media penerbitan sertifikat dan validasinya dapat dibuat menggunakan program milik Ethereum yaitu Geth dan penyimpanan data menggunakan *smart contract* yang diterbitkan pada jaringan *blockchain*. Hasil dari pengujian reliabilitas terhadap sistem menunjukkan bahwa sistem berhasil memproses 200 transaksi dalam waktu kurang lebih 8 detik. Untuk pengujian skalabilitas didapatkan estimasi 10 juta blok membutuhkan kapasitas penyimpanan sebesar 22,6 GB untuk menjadi *node* atau *miner* pada jaringan *blockchain* ini.

Kata kunci: belajar online, sertifikat online, blockchain technology

DESIGN OF ACADEMIC WEBSITE USING DIGITAL CERTIFICATE STORAGE USING BLOCKCHAIN TECHNOLOGY

Abstract

A certificate is a form of appreciation that a person receives after completing a certain competency or learning test. Certificates must be created and stored with good methods and security to prevent changes in content or even forgery. Blockchain technology is technology that allows secure storage processes at a low cost. Security is guaranteed because everyone can take part in storing data with a distributed ledger. Based on the results of research and design of the system, it can be concluded that the process of making blockchain technology as a media for issuing certificates and validation can be made using Ethereum's proprietary program Geth and data storage using smart contracts issued on the blockchain network. The results of the reliability testing of the system indicate that the system successfully processed 200 transactions in approximately 8 seconds. For scalability testing, it is estimated that 10 million blocks require a storage capacity of 22.6 GB to become a node or miner on this blockchain network.

Keywords: online learning, online certificate, blockchain technology

1. PENDAHULUAN

Sertifikat menurut Kamus Besar Bahasa Indonesia (KBBI) adalah tanda atau surat keterangan (pernyataan) tertulis atau tercetak dari orang yang berwenang yang dapat digunakan sebagai bukti kepemilikan atau suatu kejadian (KBBI, 2016). Sertifikat sendiri sering dipakai sebagai bukti bahwa seseorang menguasai suatu kemampuan secara profesional atau sebagai bukti kepemilikan suatu benda berharga.

Sertifikat digital saat ini sudah sangat umum digunakan seiring dengan berkembangnya dunia akademik. Saat ini sudah banyak sistem akademik *online* atau platform belajar secara *online* yang menawarkan berbagai kelas baik berbayar maupun gratis. Sertifikat digital akan lebih memudahkan peserta kelas dalam mengakses sertifikat tanpa perlu menyimpannya secara fisik yang berisiko kerusakan kertas dan kehilangan. Sertifikat digital memang memiliki berbagai macam keuntungan, namun juga

tidak terlepas dari berbagai risiko dan tantangan yang perlu dihadapi. Salah satu contoh tantangan yang paling dasar adalah penyimpanan data yang masih menggunakan sistem sentralisasi.

Salah satu teknologi yang telah terbukti bisa membantu menyelesaikan permasalahan seperti akurasi data, keamanan transaksi dan lainnya adalah *blockchain* (Zheng et al., 2018). *Blockchain* adalah merupakan sistem buku besar yang transparan dan tersebar kepada setiap *node* sehingga kebenaran data tidak bisa dipungkiri, sistem ini bisa menambah keamanan dan mengurangi risiko data yang korup (Wijaya, 2016). *Blockchain* merupakan solusi yang tepat untuk mengurangi risiko pemalsuan sertifikat digital dan mengamankan data sertifikat digital, dengan buku besar berisi data sertifikat digital yang tersebar ke semua *node* akan menjadikan data sertifikat digital menjadi lebih aman dan jelas bagi semua orang.

Penerapan teknologi *blockchain* pada awalnya dilakukan oleh Nakamoto (Nakamoto, 2008) dengan mengimplementasikan teknologi *blockchain* pada uang elektronik. Kombinasi uang elektronik dan *blockchain* ini disebut mata uang kripto. Nakamoto membuat mata uang kripto pertama yang disebut dengan Bitcoin. Bitcoin juga yang mempopulerkan teknologi *blockchain* dan semakin banyak bermunculan mata uang kripto lainnya. Implementasi *blockchain* pada mata uang elektronik menggerakkan beberapa penelitian untuk mengimplementasikan teknologi *blockchain* pada berbagai bidang lain seperti biomedis dan kesehatan (Kuo, 2017), pendidikan (Chen, et al., 2018), dan industri perbankan (Guo dan Liang, 2016).

Beberapa jenis penelitian telah dilakukan untuk mengkaji penerapan teknologi *blockchain* pada berbagai bidang. Rifa Hanifatunnisa (Hanifatunnisa, 2017) membuat aplikasi pencatatan e-voting menggunakan teknologi *blockchain*. Hasil penelitian tersebut berupa sistem *blockchain* yang bisa digunakan untuk menyimpan hasil voting dan sistem yang dirancang bisa berjalan dengan tingkat akurasi yang cukup baik. Penyimpanan data hasil voting dengan teknologi *blockchain* bisa meningkatkan keamanan dan transparansi data.

Arief dan Sundara (2017) melakukan penelitian untuk mengkaji bagaimana penerapan teknologi *blockchain* pada *Internet of Thing* (IoT). Berdasarkan hasil penelitian yang dilakukan, teknologi *blockchain* memiliki potensi yang baik untuk diterapkan pada teknologi IoT. Penggunaan *blockchain* pada IoT bisa memudahkan akses dan meningkatkan reliabilitas sistem IoT. Jaringan *peer-to-peer* yang merupakan bagian dari *blockchain* bisa dimanfaatkan untuk menghubungkan perangkat IoT.

Blockchain merupakan teknologi yang menyimpan data ke dalam bentuk ledger yang saling terdistribusi dan memungkinkan terjadinya transaksi secara real-time dengan jaringan *peer-to-peer* (Arief & Sundara, 2017). Teknologi *blockchain* sudah

banyak diterapkan pada beberapa bidang tertentu dan paling banyak diterapkan pada bidang keuangan. Banyak mata uang kripto baru yang bermunculan dan menerapkan teknologi *blockchain* di dalamnya. Terdapat juga beberapa penelitian yang mencoba menerapkan teknologi *blockchain* pada bidang lain selain bidang keuangan. Untuk menguji fungsionalitas dan manfaat *blockchain* pada bidang-bidang baru diperlukan penelitian yang secara khusus menguji penerapan *blockchain* pada bidang tersebut. Penelitian mengenai penerapan *blockchain* pada bidang-bidang seperti pendidikan, kesehatan, asuransi, transportasi dan jual beli masih jarang ditemukan.

Penelitian ini akan berbeda dari penelitian sebelumnya karena pembuatan sistem *blockchain* yang akan diterapkan pada penelitian ini akan menggunakan sistem *blockchain* milik Ethereum. Ethereum merupakan platform *open-source* untuk aplikasi desentralisasi yang bisa digunakan untuk membuat jaringan *blockchain* sendiri lengkap dengan fungsinya (Rosic, 2016). Pembuatan sistem *blockchain* dengan Ethereum dilakukan menggunakan Geth yang merupakan implementasi Ethereum dalam bahasa pemrograman Go. Geth memungkinkan pengguna untuk membuat jaringan *blockchain* tanpa menuliskan kode pemrograman sama sekali. Penyimpanan data pada jaringan *blockchain* dilakukan dengan menggunakan *smart contract*. *Smart contract* merupakan aturan yang bisa diterapkan pada jaringan *blockchain* untuk mengatur penyimpanan data atau proses lainnya (Rey, 2019). *Smart contract* pada jaringan *blockchain* Ethereum ditulis menggunakan bahasa pemrograman Solidity. *Smart contract* yang sudah dituliskan bisa disebarluaskan menggunakan bantuan Truffle. Jaringan *blockchain* yang sudah dibuat dihubungkan menggunakan Metamask.

Penelitian ini akan menguji penerapan teknologi *blockchain* pada bidang pendidikan. Salah satu sektor dalam bidang pendidikan yang akan diteliti adalah platform belajar secara *online*. Tujuan utama penelitian ini adalah menerapkan teknologi *blockchain* untuk penyimpanan sertifikat dalam platform belajar daring. Penelitian ini akan menguji seberapa efektif dan aman teknologi *blockchain* untuk digunakan sebagai media penyimpanan. Penelitian ini juga menguji pemanfaatan teknologi *blockchain* pada bidang selain mata uang digital yang sudah banyak diterapkan saat ini. Penelitian ini bisa membuka peluang baru untuk memanfaatkan teknologi *blockchain* pada berbagai bidang seperti kesehatan, pendidikan, dan lainnya. Berdasarkan pada berbagai tujuan dan manfaat yang ingin dicapai maka penelitian ini akan mengembangkan sebuah *website* akademik untuk proses belajar *online* yang sertifikatnya disimpan menggunakan teknologi *blockchain*.

2. METODE PENELITIAN

2.1. Analisis Masalah

Sertifikasi sering kali dipakai sebagai acuan seberapa dalam kemampuan yang dimiliki oleh seseorang. Sertifikasi bisa ditemukan dalam berbagai bentuk seperti sertifikasi tentang kemampuan khusus, sertifikasi bahasa asing dan berbagai macam jenis sertifikasi lain. Seorang harus berhasil melewati ujian tertentu dalam suatu pembelajaran untuk bisa mendapatkan sebuah sertifikat. Sebuah lembaga bisa membuka kelas akademik dan mengeluarkan sertifikat sebagai tanda kelulusan bagi para siswa atau peserta kelas. Sebuah sertifikat biasanya akan diakui di dalam dunia kerja jika lembaga yang mengeluarkan sertifikat tersebut juga cukup dikenal. Perkembangan teknologi sudah masuk ke dalam bidang pendidikan. Saat ini sudah sangat sering ditemukan berbagai *website* yang menawarkan kelas akademik *online* bersertifikasi yang cukup diakui di dunia kerja.

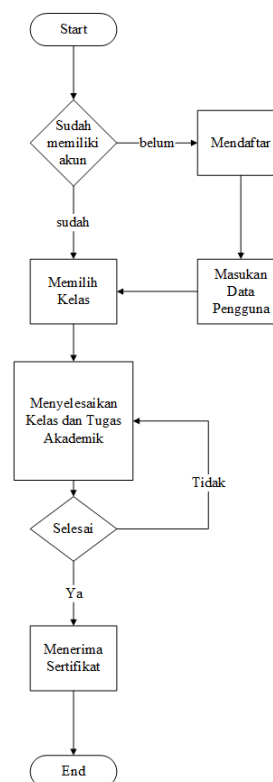
Sertifikat digital yang diterbitkan secara *online* akan disimpan di dalam server milik lembaga penerbit sertifikat atau *website* penyedia kelas *online*. Pengguna memang bisa mengunduh dan mencetak sertifikat tersebut, namun tetap pengguna akan lebih nyaman bila penyedia sertifikat *online* memiliki penyimpanan yang bisa diandalkan sebagai cadangan yang bisa diakses kapan pun. Salah satu faktor lain yang harus dipertimbangkan adalah risiko pemalsuan sertifikat. Sebuah sertifikat akan lebih diakui dan dihargai bila risiko pemalsuan sertifikat sangat kecil atau tidak bisa dipalsukan. Pemalsuan sertifikat akan mempengaruhi kredibilitas lembaga penerbit sertifikat tersebut.

Blockchain merupakan sebuah teknologi yang memungkinkan pengguna menyimpan data secara aman karena data yang disimpan ke dalam *blockchain* akan bersifat permanen dan tidak bisa dihapus. Perubahan data pada rantai blok hampir tidak mungkin terjadi kecuali terdapat aturan yang disematkan pada sistem yang bisa menerima perubahan rantai blok pada suatu kondisi tertentu (Hanifatunnisa, 2017). Metode ini jelas akan cocok bila diterapkan untuk menyimpan kepemilikan surat berharga seperti sertifikat digital. Penelitian ini akan memerlukan sumber daya yang cukup besar karena perangkat komputer akan digunakan sebagai *node* sekaligus *miner* pada *blockchain*. Penelitian juga akan menggunakan sumber daya CPU yang cukup besar karena akan melakukan konsensus *proof of work*. Kapasitas penyimpanan perangkat komputer juga akan dibutuhkan untuk menyimpan *blockchain* dalam bentuk basis data sesuai dengan format Ethereum. Kapasitas yang diperlukan akan terus bertambah sesuai dengan jumlah blok.

2.2. Desain Sistem

Pada penelitian ini akan dibuat sebuah *website* yang dilengkapi dengan teknologi *blockchain* sebagai fitur penyimpanan data kelas dan sertifikat digital

yang dimiliki pengguna. Halaman *website* yang akan dibuat merupakan sebuah kelas *online* yang mana pengguna bisa memilih kelas mana yang akan diikuti. Pengguna yang mendaftar pada suatu kelas harus menyelesaikan rangkaian materi dan pengujian yang ada pada kelas tersebut untuk bisa mendapatkan sertifikat digital. Untuk bisa mengambil sebuah kelas, pengguna harus memiliki akun atau *wallet* Ethereum terlebih dahulu. Diagram alir dari sistem dapat dilihat di gambar 1.



Gambar 1. Diagram alir sistem

Pengguna perlu memiliki *wallet* Ethereum karena sertifikat akan dicatat dalam *smart contract* berdasarkan *public key* milik pengguna dan juga sebagai media pembayaran pengguna. Sebagai peserta kelas, *public key* akan digunakan sebagai alamat pemilik sertifikat sedangkan *private key* akan digunakan untuk pembuatan tanda tangan digital untuk proses penandatanganan transaksi penerbitan sertifikat yang akan dikelola oleh Metamask. Ketika pengguna telah menyelesaikan kelas maka pengguna bisa menerima dan menerbitkan sertifikat pada *blockchain*.

Dalam penelitian ini *node* dan *miner* bisa dijadikan satu, sehingga setiap *node* bisa menjadi *miner* juga. Penelitian ini juga akan menggunakan jaringan *peer-to-peer* dengan menggunakan bantuan Geth sebagai aplikasi pembuat jaringan *blockchain peer-to-peer* sehingga *node* dan *miner* akan terhubung satu sama lain selama dalam satu jaringan. *Miner* dan *node* pada penelitian ini akan bertugas sebagai penyimpan rantai blok dan melakukan

verifikasi rantai blok baru yang akan ditambahkan. *Miner* pada sistem ini akan menggunakan metode konsensus *proof of work* yang mana *miner* akan menebak dan mencari nilai *hash* yang sesuai dengan tingkat kesulitan yang diminta. Setelah konsensus telah selesai dilakukan maka *node* atau *miner* mana pun yang berhasil menyelesaikan terlebih dahulu berhak menambahkan blok baru ke dalam rantai blok. *Node* yang sudah diperbaharui akan melakukan *broadcast* rantai blok terbaru ke seluruh *node* yang ada sehingga semua data pada *node* akan tersinkronisasi dan diperbaharui. *Miner* yang berhasil melakukan konsensus dan menambahkan blok akan mendapatkan hadiah berupa biaya transaksi dan hadiah *mining* dalam bentuk mata uang *kripto*.

Sertifikat digital yang disimpan akan berbentuk sebuah objek sertifikat yang nantinya akan disimpan ke dalam *smart contract* yang ditulis dalam Solidity. *Class* sertifikat akan memiliki beberapa atribut yang akan menunjukkan pemilik sertifikat dan tanggal penerbitan sertifikat. Sertifikat akan disimpan ke dalam sebuah map dengan indeks sebagai nilai untuk identifikasi sertifikat. Proses penyimpanan sertifikat akan dituliskan dalam fungsi Solidity yang nantinya bisa digunakan melalui Javascript dalam aplikasi.

Miner dan *node* pada penelitian ini akan dirancang menggunakan Geth sehingga tidak diperlukan penulisan kode mulai dari nol untuk membuat *node* atau *miner*. Geth juga akan mengatur jaringan *peer-to-peer* yang menampung data *blockchain* dan pengguna hanya perlu mengatur pada jaringan apa Geth akan bekerja juga mengatur genesis *block*. Pada penelitian ini sistem *blockchain* yang dirancang akan menggunakan pola penyimpanan data pada Geth dan pengguna hanya perlu menentukan folder penyimpanan data *blockchain*. *Node* yang terhubung akan melakukan sinkronisasi secara otomatis untuk mengambil data *blockchain* yang paling terbaru. Terdapat proses awal untuk membuat rantai blok sendiri yaitu membuat blok genesis. Blok genesis inilah yang dijadikan acuan antar *node* apakah mereka memegang data yang sama.

2.4. Pembuatan Antarmuka

Pembuatan antarmuka akan dilakukan dengan menggunakan Bootstrap 4. *Website* yang akan dibuat merupakan *website* yang menyediakan beberapa kelas akademik yang diambil dari Cloud Firestore dan bisa dipilih oleh pengguna. Halaman *website* yang bisa diakses oleh peserta atau siswa akan memiliki beberapa halaman dasar seperti halaman *home*, halaman daftar kelas, sertifikat siswa, cek sertifikat dan halaman pembelajaran.

2.5. Pengujian Sistem

Sistem *blockchain* yang akan diterapkan pada kelas *online* akan diuji dengan mempertimbangkan beberapa faktor yaitu keamanan, reliabilitas dan *scalability*. Sistem akan diuji dalam menghadapi

serangan pemalsuan data, pengubahan blok, dan transaksi baru yang tidak valid. Sistem akan diuji menjaga keaslian kontrak sehingga tidak ada kontrak baru yang bisa diterbitkan oleh pihak tidak berwenang. Sistem harus bisa menjaga data agar tetap aman dan asli. Sistem akan diuji dalam menangani transaksi yang cukup besar dalam waktu yang hampir bersamaan. Pengujian akan melihat seberapa cepat respons sistem terhadap aliran data dalam jumlah besar sehingga bisa dilihat seberapa besar kekuatan sistem. Pengujian juga akan melihat seberapa besar sistem bisa menampung data dan tetap menjaga kestabilan sistem. Komponen penting lain yaitu *node* dan *miner* juga akan diuji coba.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Perancangan Sistem

Aplikasi kelas *online* dengan teknologi *blockchain* akan terdiri atas dua jenis sistem yang mengatur *website* tersebut yaitu server untuk tampilan dan konten kelas *online* serta sistem *blockchain* yang digunakan sebagai media penyimpanan data pengguna. Sistem *blockchain* yang akan digunakan dalam penelitian ini dirancang dengan menggunakan program milik Ethereum yaitu Geth. Geth akan membuat jaringan *blockchain* berdasarkan *node* pada jaringan *blockchain* yang sudah dibuat. Pengguna perlu menuliskan beberapa parameter agar Geth mengerti pada jaringan *blockchain* mana *node* akan tersambung. Ketika semua perintah dan parameter telah dituliskan maka Geth akan mengeksekusi perintah tersebut untuk memulai sebuah *node*.

Node yang sudah berjalan bisa melakukan *mining* untuk menambahkan blok baru pada rantai blok. Untuk menghubungkan *node* satu dengan *node* yang lain bisa dilakukan melalui Geth *console* atau dengan membuat berkas *static-nodes.json*. Setelah *node* berhasil terhubung satu sama lain dan siap melakukan *mining*, maka langkah berikutnya adalah menghubungkan Metamask dengan jaringan *blockchain* yang sudah dibuat. Ketika jaringan ditambahkan, Metamask akan otomatis mencoba terhubung dengan jaringan *blockchain* tersebut. Jaringan *blockchain* dan web browser pengguna akan dihubungkan oleh Metamask.

Pada penelitian ini akan digunakan *smart contract* sebagai media penyimpanan data pengguna pada *blockchain*. Data pengguna seperti kelas yang sudah dibeli dan juga sertifikat milik pengguna akan disimpan ke dalam atribut di dalam *smart contract* sehingga akan diperlukan beberapa atribut dan juga fungsi untuk mengakses data yang disimpan. Setelah semua fungsi dan atribut dituliskan pada *smart contract* maka langkah berikutnya adalah menyebar *smart contract* pada jaringan *blockchain* menggunakan Truffle. Perlu diketahui bahwa untuk menyebarkan *smart contract* diperlukan sejumlah Ether untuk membayar *transaction fee*.

Sistem *blockchain* yang sudah dibuat bisa digunakan pada aplikasi web dengan menggunakan Javascript. Firebase Firestore akan diimplementasikan dan digunakan untuk menyimpan data yang tidak krusial. Aplikasi akan berjalan pada server yang dibuat dengan modul milik *Node.js* yaitu *lite-server*. Aplikasi akan berjalan pada *localhost* agar bisa terhubung dengan Metamask. Metamask pada *web browser* akan menghubungkan aplikasi dengan jaringan *blockchain*.

3.2. Hasil Perancangan Antarmuka

Pembuatan antarmuka dilakukan dengan perpaduan CSS dan Bootstrap. Antarmuka bertemakan hitam dan putih juga memiliki tampilan yang bersih dan sederhana. Setiap bagian pokok yang pada aplikasi tersedia melalui navigasi di atas halaman sehingga mudah di akses. Pada bagian paling kanan dalam baris navigasi akan ditampilkan keterangan pengguna yang sedang aktif. Ketika pengguna mengakses *website* maka halaman utama akan secara *default* dimuat. Halaman utama akan menampilkan *carousel* yang menampilkan gambar-gambar kelas yang tersedia pada aplikasi. Gambar di bawah *carousel* dan seterusnya akan menampilkan keunggulan aplikasi seperti penyimpanan yang berbasis *blockchain* dan juga pengenalan aplikasi pada pengguna.

Pada halaman lihat kelas akan ditampilkan semua kelas yang tersedia pada aplikasi. Kelas-kelas yang ditampilkan mengambil data dari Firebase Firestore. Pada masing-masing item kelas akan ditampilkan nama kelas dan juga durasi kelas. Pengguna bisa menekan tombol “lihat” jika tertarik pada kelas tersebut untuk diarahkan pada halaman modul kelas.

Jika pengguna belum membeli kelas maka 3 modul pertama saja yang bisa dilihat oleh pengguna sebagai sampel. Pengguna bisa melanjutkan belajar dengan membeli kelas tersebut. Ketika pengguna mencoba mengakses modul yang terkunci maka akan muncul modal dialog untuk melakukan pembelian kelas. Pengguna bisa menekan tombol beli dan melanjutkan transaksi dengan bantuan Metamask untuk menambahkan kelas pada akun pengguna.

Pada halaman penerbitan sertifikat akan ditampilkan contoh sertifikat dan kelas apa yang sudah dikerjakan pengguna. Pengguna bisa menerbitkan sertifikat mereka dengan menekan tombol terbitkan sertifikat pada bagian bawah halaman. Semua sertifikat pengguna bisa diakses pada halaman sertifikat saya. Pada sertifikat yang ditampilkan akan terdapat data seperti nama kelas, nomor sertifikat untuk mengecek keaslian sertifikat dan juga tanggal sertifikat diterbitkan. Pengguna bisa menunjukkan sertifikat yang dimilikinya kepada orang lain melalui fitur cek sertifikat.

Pada halaman cek sertifikat pengguna bisa memasukkan nomor sertifikat untuk mengecek

keaslian sertifikat. Jika sertifikat terdaftar pada *blockchain* dan nomor yang dimasukkan benar maka sertifikat tersebut akan ditampilkan. Jika nomor sertifikat yang dimasukkan tidak valid dan tidak ada sertifikat dengan nomor tersebut pada *blockchain* maka akan ditampilkan bahwa info bahwa sertifikat tidak valid.

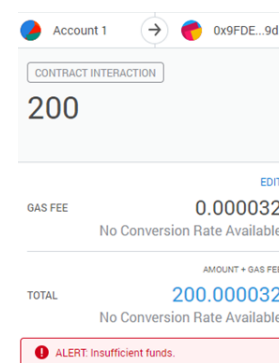
Pengguna yang belum mendaftarkan diri pada aplikasi untuk dicatat nama dan alamat emailnya pada Cloud Firestore akan diberikan dialog untuk mendaftar. Dialog akan muncul ketika pengguna membuka sebuah halaman pada aplikasi.

3.3. Hasil Pengujian Sistem

Keamanan sistem akan diuji berdasarkan seberapa aman data yang disimpan pada jaringan *blockchain* dan juga seberapa aman jaringan menghadapi ancaman pemalsuan data. Sistem *blockchain* dengan keamanan yang baik akan menjaga integritas *smart contract* sehingga tidak bisa diubah oleh pihak yang tidak bertanggung jawab.

Pada pengujian pertama, akan dilakukan penerbitan sertifikat tanpa membeli kelas. Pengujian ini bisa dilakukan dengan menggunakan metode unit testing yang dituliskan dalam bahasa pemrograman Javascript. Pada kode unit testing akan disimulasikan pemanggilan fungsi penerbitan sertifikat yang terdapat pada *smart contract*. Fungsi akan diberikan parameter kode kelas yang belum dimiliki akun yang digunakan sebagai akun uji coba. Ketika dilakukan penerbitan sertifikat tanpa membeli kelas maka akan muncul *error* dan transaksi akan ditolak karena tidak memenuhi syarat yang dituliskan pada *smart contract*.

Pembelian kelas dengan dana kurang atau kosong akan diuji langsung melalui halaman antarmuka untuk memastikan bahwa pengguna memang memiliki dana untuk membeli kelas. Ketika pengguna mencoba membeli kelas atau melakukan transaksi tanpa memiliki dana yang mencukupi maka secara otomatis Metamask akan mendeteksi kekurangan dana.



Gambar 2. Pencegahan kekurangan dana

```

INFO [03-31|18:19:53.517] Submitted transaction           fullhash=0xbbfc7d2fd99t
d51864DB81AC9d52A114C6c51a
INFO [03-31|18:46:47.690] Updated mining threads           threads=8
INFO [03-31|18:46:47.698] Transaction pool price threshold updated price=1000000000
INFO [03-31|18:46:47.713] Commit new mining work          number=5992 sealhash=01
INFO [03-31|18:46:47.754] Commit new mining work          number=5992 sealhash=6c
INFO [03-31|18:46:55.067] Successfully sealed new block    number=5992 sealhash=6c

```

Gambar 3. Waktu yang diperlukan untuk memproses 200 data

Penyebaran *smart contract* baru oleh pihak tidak berwenang perlu diuji untuk memastikan keamanan pengguna. Pengujian akan dilakukan dengan mencoba menyebarkan *smart contract* baru melalui akun pihak yang tidak mempunyai *smart contract* sebelumnya. Berdasarkan hasil pengujian dengan menyebarkan *smart contract* baru melalui perangkat lain didapatkan hasil bahwa *smart contract* yang baru berhasil disebarkan namun tidak menggantikan *smart contract* yang sudah ada. Hasil pengujian menunjukkan bahwa integritas *smart contract* sudah baik karena tidak bisa diubah-ubah oleh pihak yang tidak bertanggung jawab.

Pengujian reliabilitas sistem *blockchain* pada penelitian ini akan dilakukan dengan cara membuat 200 transaksi yang terjadi pada sistem dalam waktu bersamaan. Jumlah transaksi yang dibuat untuk menguji reliabilitas sistem tidak terlalu banyak dikarenakan pengujian dilakukan secara manual sehingga harus membuat transaksi secara satu per satu. Faktor utama yang akan diperhatikan pada pengujian reliabilitas sistem adalah waktu dan stabilitas sistem.

Hasilnya adalah seperti pada Gambar 3 menunjukkan bahwa sistem berhasil memproses 200 transaksi dalam waktu kurang lebih 8 detik. Nilai waktu ini tidak berbeda dengan waktu yang diperlukan untuk memproses jumlah transaksi normal dan sistem masih sangat stabil dalam memproses transaksi tersebut. Berdasarkan hasil pengujian reliabilitas sistem maka bisa diperoleh hasil bahwa sistem sudah cukup baik dalam menangani transaksi dalam jumlah cukup besar.

Pengujian *scalability* sistem dilakukan dengan mengukur seberapa besar jumlah kapasitas penyimpanan yang diperlukan oleh pengguna terutama *node* dan *miner* untuk bisa berperan dalam sistem *blockchain*. Ketika tidak terdapat transaksi untuk divalidasi oleh *miner* maka *miner* tetap akan melakukan *mining* namun menambahkan dengan blok kosong. Blok kosong merupakan blok yang tidak menyimpan transaksi sama sekali. Blok kosong berukuran 539 *byte*, sedangkan untuk blok yang menyimpan 10 transaksi akan berukuran 2265 *byte*.

Jika diambil rata-rata setiap blok menyimpan 10 transaksi maka bisa dilakukan perhitungan untuk memperkirakan sebesar apa kapasitas penyimpanan yang diperlukan untuk menjadi sebuah *node* pada jaringan *blockchain* penelitian ini.

Jika dilakukan perkalian dengan seberapa banyak jumlah blok yang akan ditambahkan maka akan diketahui seberapa perkiraan kapasitas

penyimpanan yang diperlukan. Perkiraan dilakukan dengan mengasumsikan bahwa *miner* akan menambahkan blok hanya ketika terdapat transaksi sehingga tidak ada blok yang kosong. Optimalisasi kinerja *miner* bisa dilakukan dengan membuat kode Javascript yang akan dieksekusi oleh *miner*. Jika menggunakan metode biasa maka estimasi penyimpanan yang diperlukan akan sangat sulit didapatkan karena terlalu banyak perubahan kapasitas tiap blok.



Gambar 4. Estimasi kapasitas penyimpanan yang diperlukan node

Untuk jumlah blok di bawah angka 1 juta diperlukan kapasitas penyimpanan yang relatif kecil. Ketika menyentuh satu juta blok maka akan memerlukan kapasitas penyimpanan sebesar 2,2 *Gigabytes* yang masih relatif kecil untuk teknologi saat ini. Jika mencapai 10 juta blok maka akan diperlukan kapasitas penyimpanan sebesar 22,6 *Gigabytes* untuk menjadi *node* atau *miner* pada jaringan *blockchain* ini. Berdasarkan penelitian dan pengujian maka tingkat *scalability* jaringan *blockchain* yang dibuat dengan menggunakan Geth milik Ethereum masih sangat baik. Kestabilan dan kinerja sistem juga sudah teruji mengingat jaringan Ethereum sudah diterapkan pada dunia nyata.

4. KESIMPULAN DAN SARAN

Hasil penelitian dan pengujian sistem yang dilakukan pada sistem *blockchain* untuk kelas belajar *online* memiliki kesimpulan bahwa jaringan *blockchain* bisa dibuat menggunakan program milik Ethereum yaitu Geth dan penyimpanan data menggunakan *smart contract* yang diterbitkan pada jaringan *blockchain*.

Jaringan *blockchain* lokal yang dibuat pada penelitian ini sudah bisa menjalankan fungsi-fungsi yang diperlukan sebuah platform penerbitan pada sistem belajar *online*. Penggunaan Geth pada jaringan

blockchain yang dibuat memiliki tingkat keamanan, reliabilitas dan juga *scalability* yang cukup baik.

Penelitian ini masih bisa dikembangkan dan diteliti lebih lanjut untuk mendalami berbagai penerapan teknologi *blockchain* untuk berbagai bidang. Misalnya untuk peningkatan reliabilitas dengan menggunakan *boot node* yang di *hosting* pada *web service*. Pengujian sistem juga dapat ditingkatkan dengan melakukan pengujian otomatis sehingga jumlah transaksi dan data yang diuji lebih banyak.

DAFTAR PUSTAKA

- ARIATA. 2019. Apa Itu JavaScript? Pemahaman Dasar Mengenai JavaScript bagi Para Pemula [online]. Tersedia di <https://www.hostinger.co.id>. [Diakses 3 Oktober 2019].
- ARIEF, L. and SUNDARA, T.A., 2017. Studi atas Pemanfaatan Blockchain bagi Internet of Things (IoT). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 1(1), pp.70-75.
- BRAGAGNOLO, S., ROCHA, H., DENKER, M. and DUCASSE, S., 2018, March. SmartInspect: solidity smart contract inspector. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 9-18). IEEE.
- BULKIN, A. 2016. Explaining blockchain—how proof of work enables trustless consensus. [Online]. Tersedia di: <https://keepingstock.net>. [Diakses 24 Februari 2020].
- CHEN, G., XU, B., LU, M. and CHEN, N.S., 2018. Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1), p.1.
- FRANKENFIELD, J. 2019. Proof of Stake (PoS) [Online]. Tersedia di: <https://www.investopedia.com/terms/p/proof-stake-pos.asp>. [Diakses 30 September 2019].
- FURQONI, I.Y., 2017. Pemalsuan Ijazah Di Kalangan Buruh Pabrik (Studi Kualitatif Mengenai Tindakan Sosial dan Stigmatisasi Pelaku Pemalsuan Ijazah Di Kabupaten Bekasi) (Doctoral dissertation, Universitas Airlangga).
- GUO, Y. and LIANG, C., 2016. Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(1), p.24.
- HADI, D. A. 2016. Bootstrap Part 1 : Pengertian Dan Cara Menggunakan Bootstrap [Online]. Tersedia di: <https://www.malasngoding.com>. [Diakses 2 Oktober 2019].
- HANIFATUNNISA, R. 2017. Perancangan dan Implementasi Sistem Pencatatan E-Voting Berbasis Blockchain. Tesis Program Magister Institut Teknologi Bandung.
- KUO, T.T., KIM, H.E. and OHNO-MACHADO, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), pp.1211-1220.
- LUTFI, F. 2017. Mengenal Node.js. [Online]. Tersedia di: <https://www.codepolitan.com>. [Diakses 2 Oktober 2019].
- MUHARDIAN, A. 2017. Belajar Nodejs #2: Mengenal NPM untuk Manajemen Project Javascript. [Online]. Tersedia di: <https://www.petanikode.com>. [Diakses 2 Oktober 2019].
- NAKAMOTO, S., 2019. Bitcoin: A peer-to-peer electronic cash system. Manubot.
- RAMADHAN, H.A. and PUTRI, D.A., 2018. Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia. 1–66.
- ROSIC, A., 2019. What is Ethereum?[The Most Updated Step-by-Step Guide!]. *Blockgeeks*, May.
- SERTIFIKAT. 2016. Pada KBBI Daring. [Online]. Tersedia di: <https://kbbi.kemdikbud.go.id/>. Diakses 2 Oktober 2019.
- WHITTLE, B. 2019. What Is a Nonce? A No-Nonsense Dive into Proof of Work. [Online]. Tersedia di: <https://coincentral.com/what-is-a-nonce-proof-of-work/>. [Diakses 30 September 2019].
- WIJAYA, D. A. 2016. Mengenal Bitcoin dan Cryptocurrency. Puspantara.
- ZHENG, Z., XIE, S., DAI, H.N., CHEN, X. and WANG, H., 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), pp.352-375.

Halaman ini sengaja dikosongkan