Sugandi, H. K., Harahap, N. S., Cynthia, E. P., Yanto, F. and Sanjaya, S. (2022) "Rancang Bangun Aplikasi Simulasi Mining Pada Jaringan Blockchain Bitcoin", Sebatik, 26(1).
Submitted: 2022-05-07 Accepted: 2022-05-29 Published: 2022-06-01

Sebatik Vol. 26 No. 1 Juni 2022
ISSN: 1410-3737(p) 2621-069X(e)

DOI:10.46984/sebatik.v26i1.1875

RANCANG BANGUN APLIKASI SIMULASI *MINING* PADA JARINGAN *BLOCKCHAIN* BITCOIN

Hatami Karsa Sugandi[1)], Nazruddin Safaat Harahap[2)], Eka Pandu Cynthia[3)], Feby Yanto[4)] dan **Suwanto Sanjaya[5)]**

[1,2,3,4,5]Teknik Informatika, Universitas Islam Negeri Sultan Syarif Kasim Riau
[1,2,3,4,5]Jl. H.R. Soebrantas KM 12,5 Simpang Baru, Kec. Tampan, Kota Pekanbaru, Riau 282931
E-mail : 11850114868@students.uin-suska.ac.id[1)], nazruddin.safaat@uin-suska.ac.id[2)], eka.pandu.cynthia@uin-suska.ac.id[3)], febi.yanto@uin-suska.ac.id[4)], suwantosanjaya@uin-suska.ac.id[5)]

ABSTRAK

Bitcoin merupakan salah satu dari mata uang digital yang dalam regulasinya tidak diatur oleh siapa pun seperti lembaga, organisasi maupun pemerintahan. Bitcoin menggunakan teknologi kriptografi atau yang biasa dikenal dengan teknologi *Blockchain*. Teknologi ini merupakan teknologi penyimpanan data atau transaksi kedalam sebuah *block*, dimana setiap proses penambahan *block* baru harus melalui proses validasi oleh sistem sesuai dengan konsensus yang berlaku. Untuk mengamankan jaringan *Blockchain* miliknya, bitcoin menggunakan algoritma konsensus *Proof of Work (PoW).* Proses validasi *block* inilah yang dinamakan dengan proses *mining. Mining* dilakukan untuk menambahkan transaksi kedalam *Block* dengan cara memecahkan teka-teki matematika dari algoritma *PoW* dengan cara memberikan komputasi *power* dari GPU oleh *miner*. Dikarenakan membutuhkan *power* yang besar, para *miner* diberi imbalan berupa bitcoin. Besaran bitcoin yang diterima tergantung dari *hash power miner*. Fenomena *mining* bitcoin menjadi *trend* bisnis pada masa kini karena menjanjikan keuntungan. Fenomena ini membuat banyak orang awam untuk ikut melakukan *mining*, tanpa mengetahui apa yang sebenarnya akan dilakukan. Maka dari itu simulasi ini dibuat dengan tujuan untuk mengedukasi bagaimana proses yang terjadi pada *mining* Bitcoin dengan cara visualisasi melalui Aplikasi web yang nantinya akan dibangun menggunakan bahasa pemrograman *javascript* dan diharapkan dapat menggambarkan proses *mining* pada *blockchain* dengan menerapkan algoritma konsensus *Proof of Work* di dalamnya.

Kata Kunci: *Bitcoin, Cryptocurrency, kriptografi, Algoritma PoW, Mining*

1. PENDAHULUAN

Cryptocurrency adalah sebuah mata uang digital dengan teknologi kriptografi di dalamnya, yang merupakan sebuah aset digital/alat pembayaran elektronik. Tidak sama dengan mata uang fiat pada umumnya yang masih menggunakan bank, mata uang kripto menggunakan *node* (sebuah program khusus yang dijalankan oleh perangkat komputer) dan saling terhubung untuk memproses setiap transaksinya dengan cara P2P (*Peer-to-Peer*). Untuk pencatatan transaksi (menerima dan mengirim coin) *cryptocurrency* memakai sistem buku besar yang terdistribusi (*distributed ledger*), serta menggunakan teknologi kriptografi untuk memverifikasi setiap transaksinya. Teknologi yang dipakai dalam *cryptocurrency* adalah *Blockchain* (Harahap dkk., 2020). *Blockchain* merupakan teknologi yang mana untuk setiap transaksi dan pertukaran data melalui proses validasi oleh sistem sebelum masuk permanen kedalam catatan buku besar/*ledger* berbentuk seperti rantai yang terkait satu sama lain dan untuk penyimpanannya bersifat desentralisasi. Untuk melakukan perubahan data pada *blockchain*, data pada rantai-rantai lainnya ikut berubah karena sifat dari *hashing*. Setiap pengguna yang tergabung dalam jaringan *blockchain* dapat mengecek kebenaran suatu data kapan saja. Hal inilah yang membuat teknologi *blockchain* tidak dapat dipalsukan oleh siapapun. (Yeni & Kumala, 2020).

Bitcoin merupakan salah satu *cryptocurrency* yang dalam regulasinya, tidak dikeluarkan oleh lembaga, organisasi maupun pemerintah. Bitcoin menggunakan jaringan *Peer-to-Peer* sebagai media distribusinya dengan menggunakan protokol kriptografi yaitu fungsi *hash* SHA-256. Pertama kali di cetuskan pada tahun 2008 oleh seorang individu dengan nama samaran Satoshi Nakamoto (Nakamoto, 2009). *Software* bitcoin dibuat dan mulai dijalankan pada tahun 2009. Jumlah peredaran dapat diprediksi dengan nilai yang dibatasi hanya sebesar sekitar 21 juta bitcoin yang dapat ditambang, dan nilai 21 juta bitcoin tesebut akan dicapai sekitar tahun 2140. (Mulyanto & Mulia, 2014). Saat tulisan ini dibuat, sekitar 18,9 juta bitcoin yang telah dihasilkan dan beredar (*Blockchain.com*). Cara paling mudah untuk mendapatkan bitcoin adalah dengan cara membeli bitcoin pada market *Crypto*. Adapun cara lain adalah dengan cara *mining*.

Bitcoin menggunakan konsensus *Proof of Work* untuk mengamankan jaringan *blockchain* miliknya. Cara kerja dari *Proof of Work* adalah dengan cara menvalidasi *blockchain* dengan mengiterasi setiap *block*. Proses

validasi inilah yang disebut dengan *mining.* Proses *mining* dilakukan dengan cara memecahkan teka teki dari *Proof of Work* untuk bisa menghasilkan *block* baru di jaringan *blockchain*. Pada setiap *block* di jaringan *blockchain* memiliki *hash* number dari *block* sebelumnya, menyebabkan setiap *block* saling terkait satu sama lainnya. Pada dasarnya, proses *mining* berfungsi untuk menemukan susunan *block* baru menggunakan super komputer yang memiliki kemampuan ALU yang besar. Seseorang yang melakukan *mining* disebut dengan *miner*.

Para *miner* bekerja dengan cara memberikan kekuatan *hashing* yang biasa disebut dengan *hash power* atau *hash* rate. *Hash power* ini didapatkan dari prangkat keras yang memiliki unit ALU (*Arithmetic and Logic Unit*). ALU adalah unit pada mesin komputer untuk melakukan perhitungan aritmatika dan logika. Umumnya perangkat keras yang digunakan untuk *mining* adalah CPU, GPU, FPGA, dan ASIC. GPU atau lebih dikenal dengan graphic card (VGA) menjadi yang terbanyak digunakan, serta yang paling efisien dari segi harga dan performa (Pathirana dkk., 2019). Pada penelitian sebelumnya (Gupta & Mahajan, 2020) hanya membahas bagaimana penerapan dari algoritma konsensus bitcoin dengan bahasa pemrograman python, tujuan mereka untuk mengukur waktu yang dihasilkan dalam menyelesaikan teka-teki dari algoritma PoW. Pada penelitian kali ini didasarkan oleh fenomena mining yang menjadi *trend* baru dalam bisnis digital.

Fenomena *mining* bitcoin menjadi *trend* bisnis pada masa kini karena menjanjikan keuntungan. Fenomena ini membuat banyak orang awam untuk ikut *mining*, tanpa mengetahui apa yang sebenarnya dilakukan. Berdasarkan fenomena ini maka penulis akan membuat sebuah aplikasi simulasi *mining* pada *Cryptocurrency* Bitcoin yang bertujuan untuk memvisualisasikan proses *mining.* simulasi ini berbentuk web yang dibangun menggunakan bahasa pemrograman *javascript.*.

2. RUANG LINGKUP

Dalam penelitian ini permasalahan mencakup:

1. Cakupan permasalahan.
   Mining bitcoin merupakan kegiatan untuk memvalidasi setiap transaksi yang terjadi kedalam jaringan *block*chain bitcoin. Kegiatan validasi (*mining*) inilah yang nantinya akan di simulasikan secara sederhana berbentuk aplikasi web. Tujuan dari simulasi ini adalah sebagai bentuk edukasi tentang pemahaman teknik *mining.*
2. Batasan-batasan penelitian.
   Jaringan *blockchain* yang dibangun hanya bisa di akses di *local* komputer. Untuk transaksi yang akan dimasukkan ke dalam jaringan *block*chain tidak berupa transaksi secara *real*, melainkan hanya untuk mendapatkan nilai *hash*.

3. BAHAN DAN METODE

Pada bagian ini menjelaskan bahan-bahan dan metode yang akan digunakan pada penelitian nantinya. Untuk pengujian aplikasi nantinya akan menggunakan metode *black box* Beberapa bahan dan metode diantaranya adalah:

3.1 *Blockchain*

Blockchain adalah sebuah teknologi buku besar yang terdistribusi (*Distributed Ledger* Technology). Teknologi ini hampir sama dengan database pada umumnya, berfungsi untuk menyimpan data. Bedanya, teknologi *blockchain* menggunakan proses *hashing* dan setiap data yang telah masuk kedalam *blockchain* tidak dapat diubah. Konsep dari teknologi *blockchain* mulai timbul bersamaan dengan hadirnya bitcoin yang menjadi jawaban dari permasalahan tidak adanya campur tangan pihak ketiga (lembaga finansial atau pemerintah) untuk menyambung kepercayaan antara pihak-pihak yang akan melakukan transaksi pada lingkungan yang tidak aman (Noorsanti dkk., 2018).

Sifat *append only* menjadi properti utama dalam teknologi *blockchain*, dimana data pada *blockchain* tidak bisa dihapus dan hanya bisa ditambah dengan data baru, dan untuk data sudah masuk kedalam *blockchain* tidak akan bisa diubah selamanya. Dengan adanya properti ini, teknologi *blockchain* akan menjamin keamanan sebagai database yang terdistribusi dan terdesentralisasi, yakni jika *block* baru berhasil dibuat dan data telah masuk kedalam *block*, data tersebut akan selamanya selalu berada di dalam sebuah jaringan *blockchain* tersebut. Pada tahap selanjutnya akan dijelaskan properti append-only ini dengan menggunakan algoritma PoW (*Proof of Work*) (Alvaro dkk., 2018).

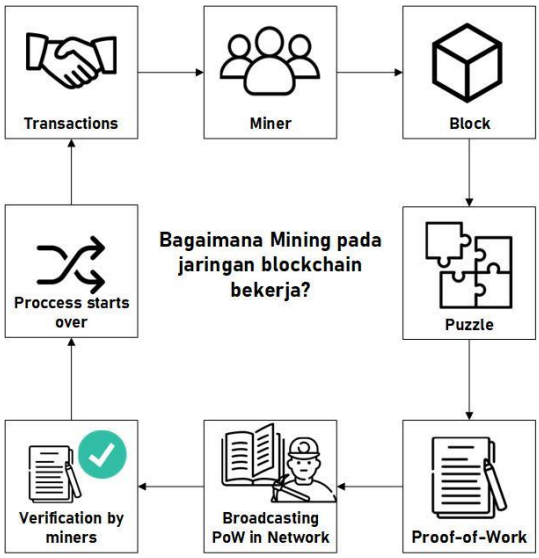
3.2 Bitcoin *Mining*

Bitcoin *mining* adalah proses menghasilkan Bitcoin dengan memecahkan teka-teki matematika yang kompleks menggunakan perangkat keras. Individu yang disebut miner bertugas mengamankan jaringan Bitcoin. Perangkat keras diperlukan untuk menambang Bitcoin, Berbagai jenis perangkat keras digunakan oleh penambang dari waktu ke waktu untuk menambang blok Bitcoin. Awalnya Bitcoin ditambang hanya menggunakan CPU, dan kemudian berkembang menggunakan GPU, FPGA, dan ASIC (Ghimire, 2019). Sistem kepercayaan bitcoin didasarkan pada perhitungan. Transaksi digabungkan menjadi blok, yang membutuhkan sejumlah besar perhitungan untuk membuktikan, tetapi hanya sedikit jumlah perhitungan untuk memverifikasi sebagai terbukti. Proses penambangan memiliki dua tujuan dalam bitcoin:

1. *Node* penambangan memvalidasi semua transaksi dengan mengacu pada aturan konsensus bitcoin. Oleh karena itu, penambangan memberikan keamanan untuk transaksi bitcoin dengan menolak yang tidak valid atau transaksi yang salah.

2. Penambangan menciptakan bitcoin baru di setiap blok, hampir seperti bank sentral yang mencetak baru uang. Jumlah bitcoin yang dibuat per blok terbatas dan berkurang dengan waktu, mengikuti jadwal yang telah ditentukan.

Setiap 10 menit atau lebih, Komputer para penambang bersaing dengan ribuan sistem serupa di dunia berlomba untuk menemukan solusi untuk blok transaksi (Andrea, 2017). Menemukan solusi seperti itu, disebut *Proof of Work* (PoW), membutuhkan kuadriliun operasi *hashing* per detik di seluruh jaringan bitcoin. Algoritma untuk *Proof of Work* melibatkan pengulangan *hashing* header blok dan nomor acak dengan algoritma kripto SHA256 sampai solusi yang cocok dengan pola yang telah ditentukan muncul. Penambang pertama yang menemukan solusi seperti itu memenangkan putaran kompetisi dan menerbitkannya blok ke dalam *blockchain* lalu mendapatkan bitcoin. Untuk proses dari mining bitcoin dapat dilihat pada gambar 1.



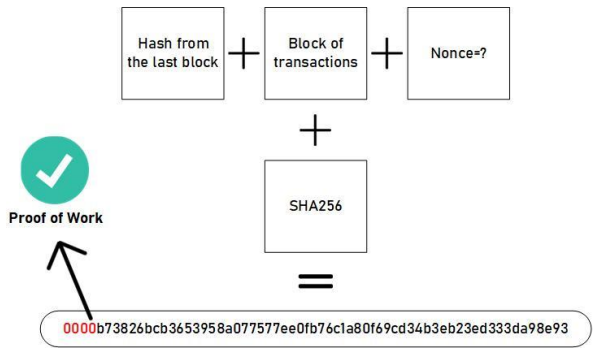
Gambar 1. Proses *mining* bitcoin

3.3 *Consensus*

Sebuah algoritma konsensus, menjamin bahwa setiap informasi yang berada di buku besar bernilai sama untuk semua *node* di sistem, juga dengan demikian, membatasi orang tidak bertanggung jawab dalam memanipulasi informasi. Karena konsensus, simpul-simpul dari jaringan cenderung memiliki data, yang sama di seluruh jaringan. Protokol konsensus beragam dengan perbedaan implementasi *blockchain* (Xu dkk., 2019).

3.4 *Proof of Work*

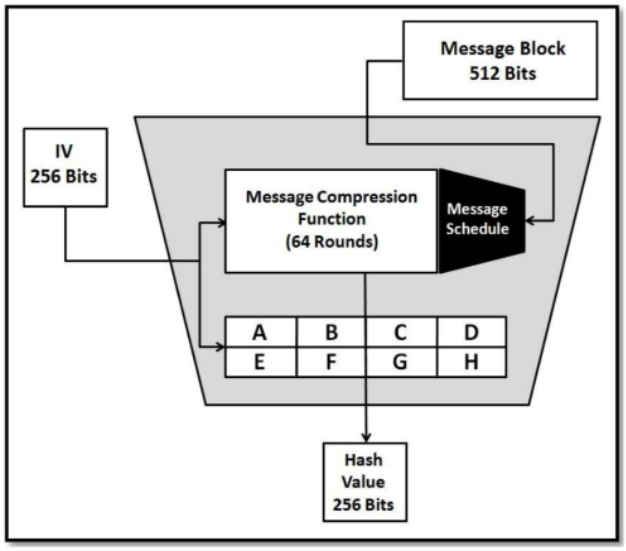
Proof of Work atau disingkat dengan PoW, adalah algoritma konsensus asli dalam jaringan *blockchain*, dimana pengguna melakukan transaksi token digital satu sama lain, memverivikasi transaksi dan membuat blok baru ke dalam *blockchain*. Dalam algoritma ini, semua penambang atau validator berpartisipasi untuk memvalidasi dan mengkonfirmasi transaksi pada jaringan *blockchain* untuk mendapatkan imbalan berupa coin yang ditambang. Semua transaksi terverifikasi di jaringan lalu dikumpulkan ke dalam blok oleh buku besar yang didistribusikan dan sesuai aturan. Proses ini lah yang disebut dengan penambangan. Ketika ingin menambahkan blok baru ke dalam *blockchain*, ada syarat yang harus dipenuhi dari setiap *hash* number, yaitu karakter n pertama dari *hash* number merupakan karakter yang telah ditentukan oleh sistem. Contohnya *hash* "0000b73826bcb3653958a……", dimana 4 karakter pertama pada *hash* tersebut adalah angka 0. Panjangnya nilai n ditentukan oleh tingkat diffilcuty pada *blockchain*. Semakin banyak nilai n, maka semakin sulit *hash* untuk dicari. Dikarenakan untuk sebuah *block* berisi data spesifik, tidak mungkin *hash* langsung memenuhi syarat yang berlaku. Nonce ditambahkan untuk bisa memenuhi syarat itu, yaitu sebuah angka *text* yang bisa membuat *hash* dari *block* memenuhi syarat yang dijelaskan diatas. Pada *hash* diatas, 4 karakter pertamanya adalah angka 0. Inilah yang dinamakan puzzle yang harus dipecahkan oleh miner. *Proof of Work* berfungsi sebagai protokol keamanan yang mencegah serangan seperti (DDoS) yang bermaksud menguras sumber daya komputer dengan mengirimkan banyak permintaan palsu. Dengan cara ini, untuk *node* yang bisa menambahkan transaksi ke dalam jaringan *blockchain* adalah *node* yang mampu untuk memecahkan teka-teki matematika yang diberikan. Protokol *blockchain* akan mengeluarkan teka teki baru secara otomatis ketika sebuah *node* berhasil memecahkan teka teki matematika yang diberikan, demikian seterusnya. Metode yang dipakai ini dikenal juga dengan *mining*. pada metode ini, memiliki masalah utama yang muncul yaitu tingkat kesulitan teka-teki matematika yang harus dipecahkan akan menyesuaikan kemampuan komputasi pada seluruh *node* yang ada. sehingga apabila semakin banyak *node* yang bergabung pada jaringan, maka semakin besar daya ALU yang dibutuhkan setiap *node* dan membutuhkan energi (daya listrik) yang sangat besar untuk menjalankan perangkat *node* tersebut (Alvaro dkk., 2018). Untuk ilustrasi persyaratan dari algoritma *Proof 0f Work* bisa dilihat pada gambar 2.



Gambar 2. Syarat dari *Proof of Work*

3.5 Fungsi *hash* SHA256

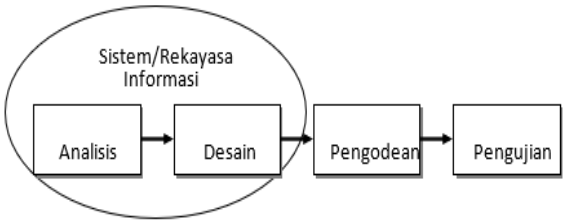
Fungsi *hash* merupakan sebuah fungsi yang digunakan untuk menghasilkan "sidik jari" digital dari semua jenis data. Fungsi ini mencampur serta memecahkan data untuk mendapatkan sidik jari, yang biasanya diwakilkan dengan string pendek huruf dan angka heksadesimal, disebut juga dengan nilai *hash*. Fungsi *hash* dikatakan baik jika fungsi yang tidak mempuyai output nilai *hash* yang sama untuk input yang berbeda. Fungsi satu arah merupakan sebutan lain dari fungsi *hash*, intisari pesan, sidik jari, kompresi, dan kode verifikasi pesan (Ghimire, 2019). Fungsi ini biasanya digunakan untuk mendapatkan sidik jari dari sebuah pesan. Fungsi *hash* adalah fungsi yang menerima string input dengan panjang berapa pun dan mengubahnya menjadi string output dengan panjang tetap. Bitcoin menggunakan fungsi *hash* SHA-256 (Secure *Hash* Algorithm 256), fungsi *hash* ini paling umum digunakan dan hingga saat ini belum ada yang bisa memecahkan algoritma fungsi *hash* SHA-256. Bentuk dari *block* diagram fungsi *hash* SHA-256 bisa dilihat pada gambar 3.



Gambar 3. SHA 256 *Block* diagram (Ghimire, 2019)

3.6 Model pengembangan aplikasi *Waterfall*

Model pengembangan aplikasi *waterfall* menyediakan pendekatan alur hidup perangkat lunak secara sekuensial dan terurut dimulai dari analisis, desain, pengkodean dan pengujian (Sukamto & Shalahuddin, 2018). Model pengembangan sistem *waterfall* bisa dilihat pada gambar 4.



Gambar 4. Model Pengembangan aplikasi *Waterfall*

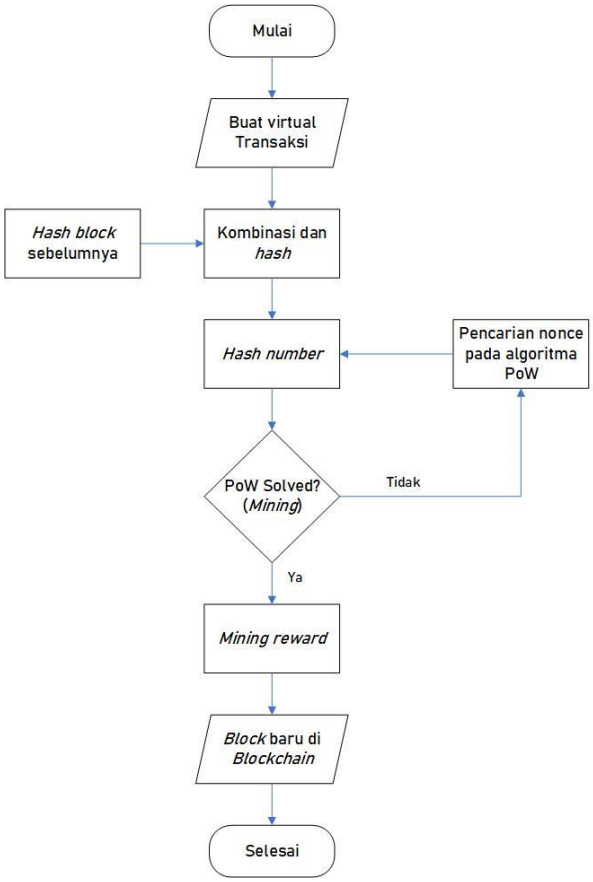
1. Analisis, analisis dilakukan untuk memenuhi kebutuhan sistem, yang akan digunakan untuk melakukan perancangan pada sistem nantinya. Untuk metode analisis yang akan dipakai diantaranya adalah Analisis proses, yang digunakan untuk mengetahui Langkah dalam sistem yang terjadi.
2. Desain, desain dilakukan untuk merancang alur kerja sistem dan struktur yang ada pada sistem yang berdasarkan kebutuhan untuk dapat mensimulasikan *mining* pada jaringan *blockchain* bitcoin.
3. Pengkodean, pengkodean merupakan tahapan yang dilakukan para peneliti sesudah Analisis dan desain. Pengkodean adalah tahapan yang dilakukan untuk membuat dan menyusun perangkat lunak dengan Bahasa pemrograman yang telah dipilih. Bahasa pemrograman yang digunakan adalah *javascript.*
4. Pengujian, pengujian dilakukan untuk memastikan apakah aplikasi yang telah dibangun berjalan lancar dan sesuai dengan yang diharapkan, pengujian nantinya akan menggunakan metode *black box.*

3.7 Rancangan aplikasi

Alur dari aplikasi dimulai dari membuat sebuah transaksi virtual yang akan dimasukkan kedalam *blockchain*. Transaksi ini kemudian di kombinasikan dengan *hash* dari *block* sebelumnya dan di konversi ke dalam bentuk kriptografi dengan menggunakan algoritma SHA256. Setelah menjadi *hash* number, proses berikutnya adalah mencari nonce untuk mendapatkan hasi *hash* yang sesuai dengan algoritma PoW yaitu angka ‘0’ dibelakang *hash* number ‘0000…….’. proses inilah yang dinamakan dengan *mining*. Jika nilai *hash* sudah sesuai dengan algoritma PoW maka *block* pun berhasil ditambahkan. Jika belum sesuai maka hanya perlu menunggu waktu lebih lama untuk akhirnya diselesaikan dengan komputer. Setelah *block* bertambah, miner akan mendapatkan *mining reward* yang akan dikirim ke wallet address miner. Pada aplikasi juga disematkan fitur untuk mengatur tingkat diffilcuty dari pencarian nonce yaitu berapa panjang angka ‘0’ yang akan dicari pada *hash* number.

1. Flowchart algoritma *mining Proof of Work*

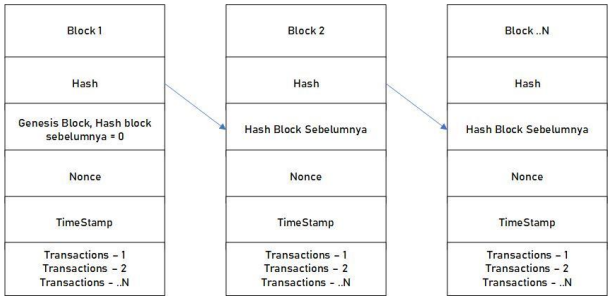
Flowchart dari algoritma *mining* pada jaringan *blockchain* bitcoin menggunakan algoritma *Proof of Work*, bisa dilihat pada gambar 5.



Gambar 5. Flowchart algoritma *mining Proof of Work*

2. Struktur *blockchain*

Fokus utama pada simulasi kali ini ialah pada bagian *blockchain* yang akan dibangun. Pada setiap *block* di jaringan *blockchain* yang dibuat berisi nilai *hashing* dari algoritma PoW, *hash* dari *block* sebelumnya (efek *chain* di jaringan *blockchain*), nonce, timestamp serta berisi transaksi. Struktur dari *blockchain* yang telah dirancang bisa dilihat pada gambar 6.



Gambar 6. Struktur *Blockchain* aplikasi

4. PEMBAHASAN

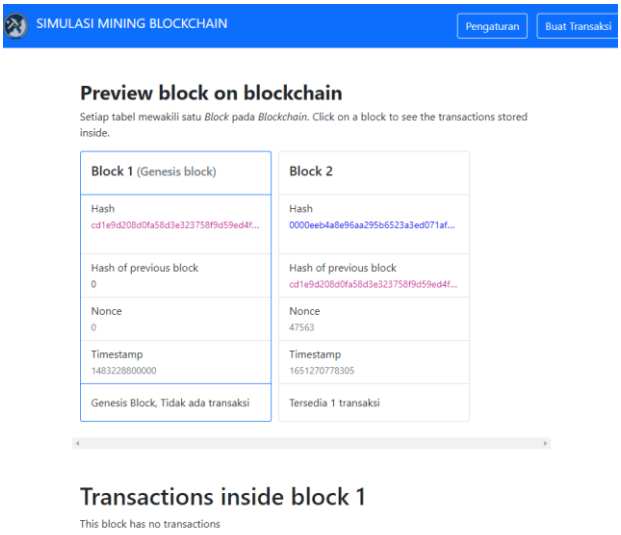
Aplikasi simulasi proses *mining* akan memvisualisasikan bagaimana proses penambahan *block* baru ke dalam *Blockchain* dengan menerapkan konsensus orisisnil dari *cryptocurrency* Bitcoin yaitu algoritma konsensus *Proof of Work*. Aplikasi ini dibangun menggunakan bahasa pemrograman javascrypt dengan menggunakan library *node* js. Untuk pengujian akan menggunakan metode *black box.*

4.1 Implementasi Aplikasi

Simulasi *mining* ini dimulai dengan menampilkan *block* yang ada pada jaringan *blockchain* yang telah dibuat. Selanjutnya adalah dengan menciptakan virtual transaksi sebagai contoh data yang akan dimasukkan kedalam jaringan *blockchain*. Kemudian dilakukan proses *mining* untuk memvalidasi *block*. Proses validasi inilah yang menjadi fokus utama dalam simulasi ini. Berikut adalah rincian tampilan yang telah dihasilkan:

1. Tampilan halaman utama aplikasi simulasi

Halaman utama dari aplikasi simulasi ini berisi data tentang *block* pada jaringan *blockchain* yang sudah diverifikasi atau ditambang. Dimulai dengan Genesis *block* atau juga disebut *block* awal, tidak ada transaksi yang terjadi pada *block* ini. Nantinya akan dilanjutkan oleh *block* yang selesai ditambang. Pada bagian bawah tabel terdapat detail transaksi yang masuk ke dalam *block* pada *blockchain*. Tampilan dari halaman utama aplikasi simulasi bisa dilihat pada gambar 7.



Gambar 7. Tampilan halaman utama aplikasi

2. Tampilan halaman Buat transaksi

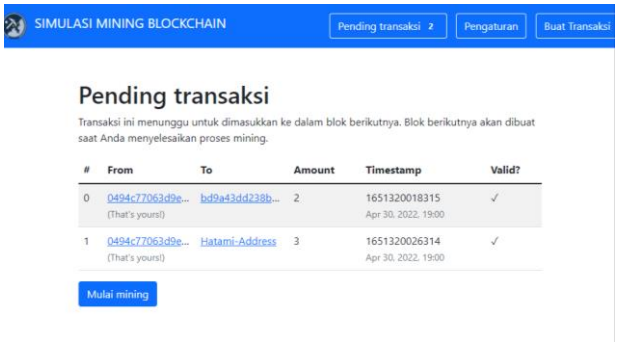
Halaman buat transaksi, berfungsi untuk membuat sebuah virtual transaksi yang nanti nya akan dimasukkan kedalam *block* pada jaringan bock*chain*. Transasksi yang dibuat bisa lebih dari 1 transaksi. Form *from address* berisi detail wallet kita yang di ciptakan menggunakan elliptic secp256k1. Dan *to address* berisi alamat tujuan

serta jumlah coin yang akan ditransfer. Pengguna tidak harus memasukkan *real* alamat wallet, cukup menginputkan *random text* saja. Simulasi ini tidak melakukan transaksi secara *real* seperti pada umumnya, hanya untuk mendapatkan nilai *hash* dari transaksi yang sedang berlangsung. Tampilan dari halaman buat transaksi bisa dilihat pada gambar 8.

Gambar 8. Tampilan halaman buat transaksi

3. Tampilan halaman pending transaksi

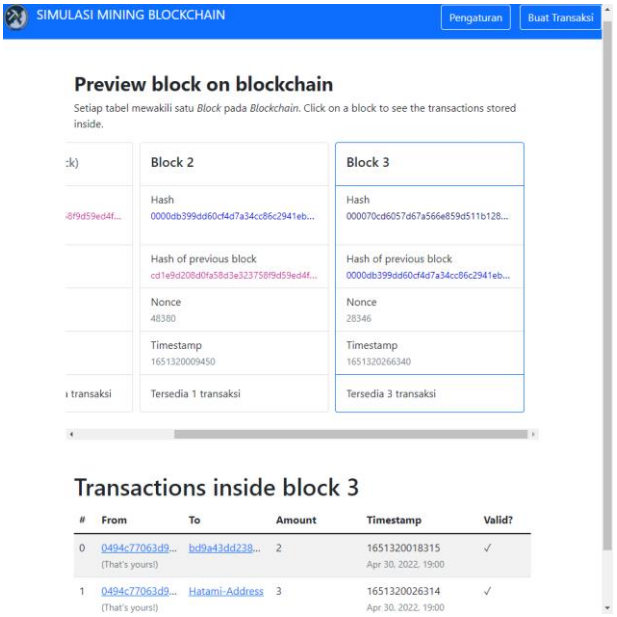
Halaman pending transaksi adalah keadaan dimana transaksi berhasil dibuat dan menunggu proses validasi atau *mining*. Pada halaman ini menampilkan asal alamat wallet ke alamat alamat wallet tujuan serta kapan waktu terjadinya transaksi. Proses *mining* di mulai pada halaman ini. Setelah pengguna klik tombol mulai *mining* maka proses akan berlangsung. Lamanya proses *mining* tergantung pada tingkat kesulitan yang telah di atur pada menu pengaturan. Tampilan dari halaman pending transaksi bisa dilihat pada gambar 9.



Gambar 9. Tampilan Halaman pending transaksi

4. Tampilan halaman hasil *block* baru

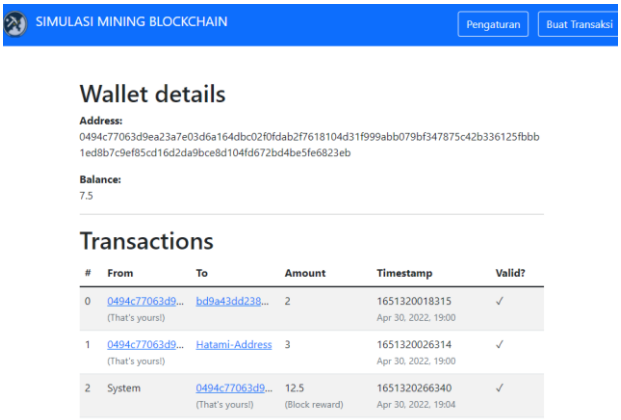
Kembali ke halaman awal, *block* baru sudah berhasil ditambahkan. Rincian transaksi yang masuk bisa dilihat pada bagian bawah tabel. pada *block* harus berisikan hasil *hash* dari *block* sebelumnya, bagian inilah yang membuat efek *chain* pada *blockchain*. Pada bagian *hash* juga harus memenuhi dari algoritma Pow, yaitu bagian awal *hash* harus diawali dengan angka '0' dan panjangnya diatur, sehingga harus menghasilkan '0000.....'. Hasil *block* baru yang telah ditambahkan bisa dilihat pada gambar 10.



Gambar 10. Tampilan halaman hasil *block* baru

5. Tampilan detail wallet

Halaman detail wallet berisi informasi tentang wallet kita. Mulai dari history pengiriman dan *block reward* yang didapat dari hasil *mining*. Tampilan detail wallet bisa dilihat pada gambar 11.



Gambar 11. Tampilan halaman detail *wallet*

6. Tampilan halaman pengaturan

Pada menu pengaturan ini pengguna dapat mengatur tingkat kesulitan yaitu dengan cara menyesuaikan tingkat *block* puzzle dari algoritma *Proof of Work*. Hasil *hash* '0000.....' berarti tingkat kesulitan nya 4. Pada menu ini juga mengatur *block reward* yang akan didapatkan

oleh miner. Tampilan halaman pengaturan bisa dilihat pada gambar 12.

Gambar 12. Tampilan halaman pengaturan

4.2 Pengujian *black box*

Penelitian ini menggunakan metode pengujian *black box* untuk mengetahui apakah sistem yang telah dibuat bisa berfungsi dengan baik. pengujian yang telah dilakukan dapat dilihat pada tabel 1.

Tabel 1. Pengujian *black box*

Skenario pengujian	Hasil yang diharapkan	Hasil pengujian	Ket.
Menampilkan data pada jaringan *block*chain	Data tampil berdasarkan *block* yang telah ditambah	Data *block*chain berhasil ditampilkan	[x]Berhasil []Gagal
Buat transaksi virtual	Transaksi virtual dibuat	Transaksi dibuat, Masuk ke halaman pending transaksi	[x]Berhasil []Gagal
Validasi transaksi kedalam *block*chain	*Block* baru ditambahkan	*mining*, *block* baru berhasil ditambah	[x]Berhasil []Gagal
Mengubah pengaturan *mining*	Aturan baru diterapkan	Berhasil menerapkan aturan baru	[x]Berhasil []Gagal

berdasarkan hasil pengujian menggunakan metode *black box* yang telah di lakukan, hasil yang didapatkan sesuai dengan yang diharapkan.

5. KESIMPULAN

Aplikasi ini dibangun untuk dapat mensimulasikan bagaimana proses mining yang terjadi pada *cryptocurrency* bitcoin, yaitu dengan cara memvalidasi setiap transaksi "buatan" kedalam jaringan *blockchain* yang sudah dirancang. adapun syarat validasi kedalam *block*chain menggunakan algoritma dari *proof of work*. proses validasi ini membutuhkan *hash power* komputer, dimana jika semakin tinggi tingkat kesulitan *nonce* maka semakin lama proses validasi yang dilakukan. Untuk mengatasi waktu yang lama ini, solusinya adalah dengan cara menambah kekuatan *hash power* yang bisa didapatkan dengan menambahkan GPU komputer.

6. SARAN

Mining menjadi *trend* bisnis baru pada masa kini dalam mendapatkan *cryptocurrency*. Dalam melakukan *mining* membutuhkan energi listrik semakin banyak dari waktu ke waktu. Selain *mining* adapun cara lain untuk mendapatkan *cryptocurrency* adalah dengan cara staking. Saran dari penulis adalah peneliti berikutnya bisa mensimulasikan bagaimana proses staking pada *cryptocurrency*.

7. DAFTAR PUSTAKA

Alvaro, D., Teknik, S., & Key, I. P. (2018). *Implementasi Blockchain untuk Distribusi Kunci Publik Terdesentralisasi*.

Andrea, A. (2017). Mastering BitCoin. In *Journal of World Trade* (Vol. 50, Issue 4). https://www.bitcoinbook.info/

Blockchain. (n.d.). Retrieved November 20, 2021, from https://www.*block*chain.com/charts/total-bitcoins

Ghimire, S. (2019). *Analysis of Bitcoin Cryptocurrency and Its Mining Techniques*. *May*, 66. http://dx.doi.org/10.34917/15778438

Gupta, C., & Mahajan, A. (2020). Evaluation of Proof-of-Work Consensus Algorithm for *Block*chain Networks. *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*. https://doi.org/10.1109/ICCCNT49239.2020.9225676

Harahap, A. khoirunnisa, Oktari, N. M. D. S., Agung, A. A. G., & K, R. B. (2020). Perbandingan ROI Metode Konsensus Proof of Work, Proof of Stake, dan Proof of Service (Masternode). *Jurnal Teknologi Informasi Dan Manajemen*, *volume 2*.

Mulyanto, F., & Mulia, M. T. (2014). Analisis Mining System Pada Bitcoin. *KNSI 2014*.

Mustaqbal, M. S., Firdaus, R. F. & Rahmadi, H., 2015. Pengujian Aplikasi Menggunakan Black Box Testing Boundary Value Analysis. Jurnal Ilmiah Teknologi Informasi Terapan, Volume I.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Noorsanti, R. C., Yulianton, H., Hadiono, K., Studi, P., Informatika, T., Informasi, F. T., & Stikubank, U. (2018). *Block*chain - Teknologi Mata Uang Cryptocurrency. *Prosiding SENDI_U 2018*, 978–979.

Pathirana, A., Halgamuge, M. N., & Syed, A. (2019). Energy Efficient Bitcoin Mining to Maximize the Mining Profit : Using Data from 119 Bitcoin Mining Hardware Setups Energy Efficient Bitcoin Mining to Maximize The Mining Profit : Using

Data From 119 Bitcoin Mining. *Proceedings of 262nd The IIER International Conference, Istanbul, Turkey, November*, 12.

Sukamto, R. A., & Shalahuddin, M. (2018). Rekayasa Perangkat Lunak. Informatika

Xu, X., Weber, I., & Staples, M. (2019). Introduction. In *Architecture for Blockchain Applications*. https://doi.org/10.1007/978-3-030-03035-3_1

Yeni, M., & Kumala, D. (2020). *Teknologi Blockchain untuk Transparansi dan Keamanan pada Era Digital*. 6. http://repository.unmuha.ac.id/xmlui/handle/123456789/579