LAPORAN PENELITIAN
PROGRAM STUDI

ANALISIS ALGORITMA SHA-256 PADA PROSES MINING TEKNOLOGI BLOCKCHAIN BITCOIN

PENELITI :

Ilka Zufria, M.Kom (Ketua)

Yusuf Ramadhan Nasution, M.Kom (Anggota)

Raja Alfiansyah (Anggota)

FAKULTAS SAINS DAN TEKNOLOGI

UINIVERSITAS ISLAM NEGERI (UIN)

SUMATERA UTARA

MEDAN

2022

LEMBAR PENGESAHAN

1.	a. Judul Penelitian	Analisis Algoritma SHA-256 Pada Proses Mining Teknologi Blockchain Bitcoin
	b. Kluster Penelitian	Penelitian Program Studi
	c. Bidang Ilmu	Ilmu Komputer
	d. Kategori	Kelompok
2.	Peneliti	a. Ilka Zufria, M.Kom (Ketua) b. Yusuf Ramadhan Nasution, M.Kom (Anggota) c. Raja Alfiansyah-Mahasiswa (Anggota)
3.	Unit Kerja	Fakultas Sains dan Teknologi
4.	Waktu Penelitian	3 bulan, Agustus s.d Oktober 2022
5.	Biaya Penelitian	Rp. 5.000.000,- (Lima Juta Rupiah)

Medan, Oktober 2022

Dekan FST UIN SU

Penanggung Jawab

Prof. Dr. Mhd. Syahnan, MA
NIP. 196609051991031

Ilka Zufria, M.Kom
NIP. 198503162015031003

SURAT PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan dibawah ini :

Nama	:	Ilka Zufria, M.Kom
Jabatan	:	Dosen/ Lektor/Gol. III.d
Unit Kerja	:	FST UIN Sumatera Utara Medan
Alamat	:	Jalan Lapangan Golf No. 120, Deli Serdang Sumut

dengan ini menyatakan bahwa :

1. Judul penelitian "Analisis Algoritma SHA-256 Pada Proses Mining Teknologi Blockchain Bitcoin" merupakan karya orisinal saya.
2. Jika dikemudian hari ditemukan fakta bahwa judul , hasil atau bagian dari pelaporan penelitian saya merupakan karya orang lain dan/atau plagiasi, maka saya akan bertanggung jawab untuk mengembalikan 100% dana hibah penelitian yang telah saya terima, dan siap mendapatkan sanksi sesuai ketentuan yang berlaku.

Demikian pernyataan ini dibuat untuk digunakan sebagaimana mestinya.

Medan, Oktober 2022

Yang menyatakan

Ilka Zufria, M.Kom

ABSTRAK

Mata uang kripto (Cryptocurrency) atau sering disebut dengan mata uang virtual/digital merupakan hasil dari sebuah perkembangan teknologi keuangan (financial technology). Tujuan mata uang ini dibuat adalah untuk memberikan kemudahan dan keamanan dalam pembayaran. Dengan adanya teknologi Blockchain didalamnya, menjadikan membuat biaya transaksi menjadi lebih murah. Kehadiran bitcoin sebagai salah satu tonggak penting naiknya popularitas mata uang kripto (cryptocurrency). Hadirnya bitcoin tidak lepas dari munculnya masalah atas peran institusi finansial dalam sebuah transaksi. Dalam proses mining pada bitcoin proses hashing pada sistem blockchain yang digunakan oleh Bitcoin menggunakan algoritma SHA-256. SHA256 (Secure Hash Algorithm 256) adalah algoritma tertua dan terpopuler, di atas mana protokol Proof of-Work (PoW) Bitcoin dibangun, serta banyak cryptocurrency lainnya.

Kata Kunci : Cryptocurrency, Blockchain, Bitcoin, SHA256, Mining

ABSTRACT

Cryptocurrency or often called virtual/digital currency is the result of a development of financial technology (financial technology). The purpose of this currency is to provide convenience and security in payments. With the Blockchain technology in it, it makes transaction costs cheaper. The presence of bitcoin as one of the important milestones in the rising popularity of cryptocurrencies. The presence of bitcoin can not be separated from the emergence of problems over the role of financial institutions in a transaction. In the hashing process on the blockchain system used by Bitcoin using the SHA-256 algorithm. SHA256 (Secure Hash Algorithm 256) is the oldest and most popular algorithm, on which the Bitcoin Proof of-Work (PoW) protocol is built, as well as many other cryptocurrencies.

Keywords: Cryptocurrency, Bitcoin, SHA256, Mining

KATA PENGANTAR

Alhamdulillahirobbil Alamiin, segala puji bagi Allah SWT. Atas berkat rahmat dan karuniaNya, saya dan tim penelitian dapat menyelesaikan penelitian ini dengan judul **"Analisis Algoritma SHA-256 Pada Proses Mining Teknologi Blockchain Bitcoin"**. Sholawat dan salam senantiasa dipanjatkan kepada baginda Muhammad SAW beserta kerabat, sahabat, para pengikutnya sampai akhir zaman, adalah sosok yang telah membawa manusia dan seisi alam dari kegelapan ke cahaya sehingga kita menjadi manusia beriman, berilmu, dan tetap beramal shaleh agar menjadi manusia yang berakhlak mulia.

Penulisan laporan ini bertujuan untuk melengkapi persyaratan luaran penelitian. Laporan ini juga diharapkan dapat menambah wawasan ilmu pengetahuan, khususnya bidang ilmu komputer dalam instalasi nilai-nilai Islam yang terpadu dalam proses pembelajaran di lingkungan Universitas Islam Negeri Sumatera Utara.

Dalam penulisan laporan ini, saya sangat menyadari bahwa masih banyak kekurangan yang perlu perbaikan dan penyempurnaan, sumbangan pemikiran yang membangun sangat kami harapkan dari rekan-rekan sejawat terutama dari dosen-dosen senior. Semoga laporan penelitian ini dapat diperkaya melalui evaluasi terus menerus. Terimakasih kepada anggota peneliti dan tim penelitian yang sudah fokus dalam penyelesaian laporan ini dan pastinya sangat berperan dalam proses penelitian dari tahap awal higga akhir.

Medan, Oktober 2022

Penulis

Ilka Zufria, M.Kom

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan perekonomian dunia khususnya di Indonesia tidak dapat dilepaskan dari unsur teknologi informasi. Perkembangan teknologi informasi akan berhubungan dengan seluruh bidang termasuk bidang keuangan. Mata uang kripto (*Cryptocurrency*) atau sering disebut dengan mata uang virtual/digital merupakan hasil dari sebuah perkembangan teknologi keuangan (financial technology). Mata uang digital mulai banyak digunakan sebagai alat pembayaran pada internet. Tujuan mata uang ini dibuat adalah untuk memberikan kemudahan dan keamanan dalam pembayaran. Dengan adanya teknologi Blockchain didalamnya, menjadikan membuat biaya transaksi menjadi lebih murah. Namun, Pemerintah dalam hal ini Bank Indonesia melarang transaksi dengan menggunakan uang digital/virtual karena memiliki dampak berbahaya terhadap Sistem Keuangan, Stabilitas Moneter dan Sistem Pembayaran di Indonesia.

Dari sisi teknologi yang ditawarkan, *cryptocurrency* merupakan perkembangan dari teknologi keuangan yang memungkinkan akan mengganti uang kertas menjadi uang digital dalam transaksi keuangan dimasa depan. Diharapkan pemerintah dapat mengkaji teknologi yang terdapat pada *cryptocurrency* dengan lebih mendalam sehingga kebijakan yang dibuat nantinya tidak melarang teknologi yang terdapat pada *cryptocurrency* serta memberikan pengetahuan kepada masyarakat agar lebih memahami tentang *cryptocurrency*.

Kehadiran bitcoin sebagai salah satu tonggak penting naiknya popularitas mata uang kripto (cryptocurrency). Hadirnya bitcoin tidak lepas dari munculnya masalah atas peran institusi finansial dalam sebuah transaksi. Peran institusi

finansial merupakan bentuk sistem/model kepercayaan (*trust model/system*) dari dua pihak yang sepakat untuk melakukan transaksi jual beli. Meskipun begitu, sistem/model kepercayaan yang sudah ada dapat membuat proses transaksi menjadi tidak mudah dan cepat bila antara institusi finansial memiliki perbedaan, terutama dalam hal memproses transaksi. Hilangnya peran institusi finansial/pemerintah merupakan kelebihan dari mata uang kripto/bitcoin. Hal inilah yang membuat bitcoin tidak serta merta diakui oleh banyak negara di dunia sebagai alat tukar layaknya mata uang yang sudah kita kenal.

Setiap *cryptocurrency* menggunakan algoritma hashing tertentu yang menerapkan fungsi hash kriptografi dan mempertahankan fungsi blockchain dan pemrosesan transaksi, setelah itu penambang menerima imbalan mereka dalam bentuk koin dari *cryptocurrency* tertentu yang dikirim ke dompet mereka. Dalam proses hashing pada sistem blockchain yang digunakan oleh Bitcoin menggunakan algoritma SHA-256. SHA256 (*Secure Hash Algorithm 256*) adalah algoritma tertua dan terpopuler, di atas mana protokol Proof of-Work (PoW) Bitcoin dibangun, serta banyak cryptocurrency lainnya.

Bitcoin menggunakan protocol blockchain untuk membuat serial transaksi mata uang Bitcoin di antara penggunanya. Mesin negara direplikasi mempertahankan saldo dari pengguna yang berbeda, dan transisinya adalah transaksi yang memindahkan dana di antara mereka. Mesin negara ini dikelola oleh node-node sistem, yang disebut penambang.Dengan latar belakang diatas penulis mencoba untuk menganalisis cara kerja algoritma SHA-256 dalam proses mining bitcoin dengan judul **"Analisis Algoritma SHA-256 Pada Proses Mining Teknologi Blockchain Bitcoin"**

1.2. Rumusan Masalah

Berdasarkan latar belakang dan identifikasi masalah tersebut, maka masalah pada penelitian ini, yaitu:

1. Bagaimana proses mining pada bitcoin?

2. Bagaimana cara kerja algoritma SHA-256 pada proses mining pada bitocin ?

1.3. Tujuan Penelitian

Sesuai dengan rumusan masalah di atas, maka tujuan penelitian ini adalah sebagai berikut:

1. Menganalisis proses mining pada bitcoin
2. Menganalisis cara kerja algoritma SHA-256 pada proses mining pada bitocin

BAB II
KAJIAN PUSTAKA

1.4. Mata Uang Kripto (*Cryptocurrency*)

Sebagai bagian dari perkembangan teknologi informasi, instrumen keuangan jenis baru, cryptocurrency telah lahir dan berkembang. Mata uang virtual ini dapat dijadikan sebagai alat transaksi elektronik. Selain itu para pemiliknya juga menggunakan cryptocurrency untuk berinvestasi maupun trading. Kini bertransaksi bisnis dapat dilakukan secara daring tanpa melibatkan pihak penengah seperti bank. Transaksi dilakukan seketika, lintas negara, lintas benua, lebih cepat, lebih mudah, lebih murah, dan lebih terjamin kerahasiaannya[1].

Mata uang kripto merupakan mata uang digital tetapi bukan uang elektronik karena pengertian uang elektronik yang berlaku di negara Indonesia merupakan bentuk lain dari mata uang rupiah yang mekanisme pengelolaannya berbeda. Uang elektronik, berdasarkan Peraturan Bank Indonesia no. 11/PBI/2009 pasal 3 ayat 3 butir a dan d, disebutkan bahwa uang elektronik merupakan uang rupiah yang harus disetorkan terlebih dahulu oleh pemegang kepada penerbit dan nilai uang yang disetor oleh pemegang dan dikelola oleh penerbit bukan merupakan simpanan seperti yang dimaksud dalam undang-undang perbankan. Secara garis besar dapat disimpulkan bahwa mata uang kripto merupakan mata uang yang bukan mata uang dan nilai tukar yang sah menurut peraturan yang berlaku serta bukan termasuk dalam golongan uang elektronik[2]. Penggunaan mata uang kripto seperti bitcoin tidak dilarang oleh Bank Indonesia, meskipun tidak dilarang, resiko yang timbul dari penggunaan mata uang kripto merupakan tanggung jawab pribadi yang bersangkutan.

Mata uang kripto terdesentralisasi pertama, bitcoin, dibuat dan diadakan pada 2009 oleh pengembang Satoshi Nakamoto. ini menggunakan SHA-256, fungsi hash kriptografi, sebagai skema pembuktian kerjanya. Pada April 2011,

Namecoin dibentuk sebagai upaya untuk membentuk DNS terdesentralisasi, yang akan membuat sensor internet sangat sulit. Segera setelah itu, pada Oktober 2011, Litecoin dibebaskan. itu adalah mata uang kripto yang sukses pertama yang menggunakan scrypt sebagai fungsi hash SHA-256. Mata uang kripto terkenal lainnya, Peercoin adalah yang pertama menggunakan hybrid proof-of-work / proof-of-stake[3].

1.5. Teknologi Blockchain

Secara sederhana, teknologi blockchain dapat digambarkan sebagai sebuah basis data yang terdistribusi yang mencatat transaksi yang dibagikan kepada orang-orang yang tergabung di dalam sebuah jaringan basis data terdistribusi tersebut. Setiap transaksi yang terjadi selalu harus sesuai dengan konsensus yang telah disepakati di dalam jaringan basis data terdistribusi tersebut yang akhirnya membuat kemungkinan terjadi kecurangan terminimalisir.

Dari awal munculnya blockchain sampai sekarang, blockchain mengalami evolusi yang cukup berarti meskipun secara harafiah, blockchain adalah sebuah kumpulan block yang saling berhubungan (ter-rantai) dan berisi informasi mengenai transaksi yang terjadi. Yang menjadi kunci di dalam teknologi blockchain adalah kemampuan untuk melacak kembali di dalam jaringan basis data terdistribusi. Secara sederhana, perkembangan teknologi blockchain sudah mencapai 3 fase, yaitu blockchain 1.0 yang awalnya muncul sebagai tonggak mata uang digital, kemudian berkembang menjadi blockchain 2.0 sebagai bentuk perkembangan selanjutnya pada bidang ekonomi digital, dan yang terakhir adalah blockchain 3.0 sebagai bentuk evolusi dari ekonomi digital ke dalam bentuk perhimpunan atau masyarakat digital[4].

Selain menjadi dasar pengembangan aset kripto, teknologi blockchain juga sudah banyak diimplementasikan dalam beberapa bidang kehidupan seperti berikut :

1. Sektor Pemerintahan

Teknologi blockchainmenjadi terobosan bagi pengembangan layanan publik dan sebagai bentuk layanan untuk semua kalangan berinteraksi dengan mudah dan transparan. Terdapat beberapa contoh penggunaan blockchain dalam sektor pemerintahan, yaitu:

a. Berbagi data antar instansi pemerintahan.

   Penggunaan teknologi blockchain memungkinkan penyimpanan data antar-departemen terjadi dalam jaringan pribadi, memberikan autentifikasi pada masing-masing jaringan sehingga dapat bermanfaat dalam membangun kepercayaan dan kerahasiaan.

b. Pemungutan Suara

   Pemungutan suara dapat menggunakan fungsi smart contract yang berada dalam fitur blockchain. Pemilih akan menerima ID pemungutan suara yang memiliki fungsi sebagai media verifikasi bahwa suaranya terdaftar di blockchain dan terhitung sebagai suara yang sah.

c. Kontrak Proyek Pemerintah

   Teknologi blockchain membantu pemantauan secara real-time dari layanan e-government. Ia juga berguna untuk pelaksanaan kontrak pemerintah. Nantinya, akan ada empat langkah untuk melaksanakan lelang kontrak proyek, yaitu persiapan dan penyerahan, penawaran dan seleksi, pemantauan pelaksanaan, dan audit.

d. Rekrutmen Sumber Daya Manusia

Ketika organisasi membutuhkan seseorang untuk mengisi suatu posisi pekerjaan, maka mereka akan menerbitkan smart contract pada sistem blockchain. Hal ini dapat membantu pelamar kerja untuk melihat lebih banyak informasi pada setiap posisi pekerjaan.

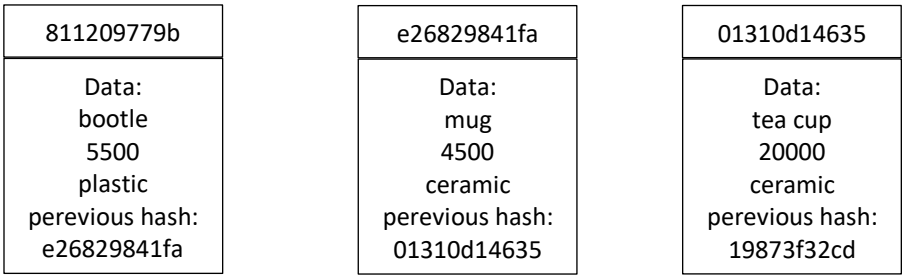
2. Sektor Kesehatan

Penggunaan blockchain dalam sektor kesehatan mencakup penelitian biomedis, asuransi kesehatan, catatan kesehatan elektronik, pendidikan kedokteran, proses penyediaan dan pengadaan obat, serta kebutuhan pelayanan pasien lainnya.

3. Sektor Keuangan

Pada sektor keuangan, blockchain banyak menjadi utilitas karena bermanfaat menyederhanakan layanan perbankan dan kredit, mengurangi risiko, dan mengurangi waktu memproses. Selain itu, blockchain juga memungkinkan untuk melacak dan melakukan tracking dalam transaksi akuntansi.

Ilustrasi blockchain sebagai sebuah kumpulan block yang terhubung dengan mencatat tanda digital / hash dari block sebelumnya dapat digambarkan seperti berikut :



Gambar 2.1. Ilustrasi dari Blockchain

Dari gambar 2.1 dapat dikatakan bahwa block dalam blockchain memiliki 3 komponen penting, yaitu data, previous hash dari block sebelumnya, dan hash beserta waktu saat block dibuat untuk block yang bersangkutan.

Teknologi berbasis Blockchain memberikan transparansi kepada semua orang di jaringan, dengan transaksi yang terlihat oleh semua komputer yang terhubung. Mayoritas komputer yang terhubung ke blockchain harus menyetujui transaksi atau perubahan pada blockchain yang mencegah transaksi agar tidak disembunyikan atau dimanipulasi. Semua perubahan hampir real-time; proses ini terjadi saat transaksi disetujui dan ditambahkan ke
blockchain. Skenario seseorang dalam organisasi yang mencuri uang atau menyembunyikan kerugian perusahaan dengan memanipulasi entri dalam buku besar sangat kecil kemungkinannya terjadi pada buku besar terdistribusi berbasis blockchain[5].

1.6. Mengenal Bitcoin

Teknologi blockchain banyak dipercaya berasal dari white paper Satosi Nakamoto yang berjudul bitcoin blockchain yang muncul di tahun 2019. Namun demikian, sejarah teknologi blockchain tidak dapat dilepaskan juga dari karya Stuart Haber dan Scott Stornetta yang mengembangkan struktur time stamping yang telah dilakukannya dua puluh tahun sebelum karya dari Nakamoto. Karya dari Haber dan Sornetta ini memfokuskan perhatian pada kepercayaan informasi bada abad digital, khususnya aplikasi blockchain dalam bidang seni[6].

Bitcoin dibuat dengan tujuan untuk menjadi alternatif mata uang fiat yang sudah menyalahi aturan-aturan alat transaksi seharusnya. Ini dikarenakan, secara konspirasi, mata uang fiat dipercaya telah dikuasai dan dipermainkan oleh sebagian elit global. Bitcoin di desain dengan cara memperbolehkan orang-orang untuk memiliki identitas anonim dalam kepemilikan dan pemindahan harta kekayaan, dari satu wallet (dompet elektronik) ke wallet lainnya. Lalu dikarenakan Bitcoin tidak melalui perantara, fee dalam bertransaksi pun jauh lebih rendah daripada menggunakan jasa institusi keuangan konvensional[7].

Ketua Komisi Dakwah MUI Soal Hukum Bitcoin" menerangkan, bahwa

KH. Cholil Nafi berpendapat, eksistensi Bitcoin sebagai mata uang baru yakni uang virtual tidak jadi masalah, karena dahulu pun khalifah Umar ibn Khattab bermaksud membuat uang jenis baru dari kulit unta. Adapun penggunaan Bitcoin dalam transaksi Bisnis, cenderung haram karena eksistensi Bitcoin belum diakui negara (Hidayat, 2018)[8].

Sebagai pengguna baru, kita dapat mulai menggunakan dengan Bitcoin tanpa harus memahami detil teknisnya. Setelah menginstal wallet Bitcoin di komputer atau ponsel, secara otomatis akan membuat alamat Bitcoin pertama dan bisa membuat lebih banyak alamat bitcoin lagi kapanpun kita membutuhkannya. Kita bisa memberitahukan alamat Bitcoin itu kepada teman-teman kita sehingga mereka bisa membayar kita ataupun sebaliknya. Sangat mirip dengan cara kerja email, kecuali bahwa alamat Bitcoin sebaiknya hanya digunakan sekali saja. Rantai-blok (blockchain) adalah sebuah catatan transaksi publik di mana jaringan Bitcoin bersandar. Semua transaksi yang telah dikonfirmasi tersimpan di dalam rantai-blok. Sehingga, wallet Bitcoin dapat menghitung sisa uang yang dapat dibelanjakan serta transaksi-transaksi baru dapat diverifikasi untuk memastikan bahwa memang dimiliki oleh pengguna itu. Integritas dan urutan kronologis rantai-blok diterapkan menggunakan kriptografi[9].

Bitcoin, dalam banyak hal, hampir identik dengan mata uang kripto, yang berarti kita dapat membeli atau menjualnya di hampir setiap bursa kripto baik untuk uang fiat dan mata uang kripto lainnya. Beberapa pasar utama tempat tersedianya perdagangan BTC adalah:

1. Binance
2. Coinbase Pro
3. OKEx
4. Kraken
5. Huobi Global
6. Bitfinex

Bitcoin (BTC) merupakan sistem uang elektronik peer-to-peer yang tidak memerlukan perantara, memungkinkan pengguna untuk bertransaksi langsung lintas batas. Untuk mengirim Bitcoin, pengguna harus merasa nyaman dengan infrastruktur dasar yang diperlukan untuk transaksi Bitcoin. Untuk mengirim Bitcoin (BTC), pengguna memerlukan dompet Bitcoin, alat untuk berinteraksi dengan blockchain Bitcoin.

Meskipun umum untuk berbicara secara metaforis tentang dompet BTC yang "menyimpan" cryptocurrency pengguna, lebih akurat untuk memahami bahwa dompet Bitcoin digunakan untuk menghasilkan informasi yang diperlukan untuk mengirim dan menerima cryptocurrency via transaksi blockchain.

Seorang pengguna mungkin ingin mengirim Bitcoin ke pengguna lain sebagai bentuk pembayaran atau perdagangan, atau mereka mungkin ingin mengirim BTC di antara dompet Bitcoin yang berbeda yang mereka gunakan sendiri untuk berbagai tujuan (yaitu untuk perdagangan mata uang kripto atau untuk HODLing).

Dompet apa pun dapat digunakan untuk mengirim Bitcoin ke alamat dompet lain — perangkat lunak, perangkat keras, atau kertas — asalkan alamat tersebut secara khusus merupakan dompet Bitcoin dan bukan dompet yang dirancang untuk mata uang kripto yang berbeda, misalnya. Ethereum (ETH), Bitcoin Cash (BCH), atau XRP. Bitcoin diamankan dengan algoritme SHA-256, yang termasuk dalam kelompok algoritme hashing SHA-2, yang juga digunakan oleh fork Bitcoin Cash (BCH), serta beberapa mata uang kripto lainnya.

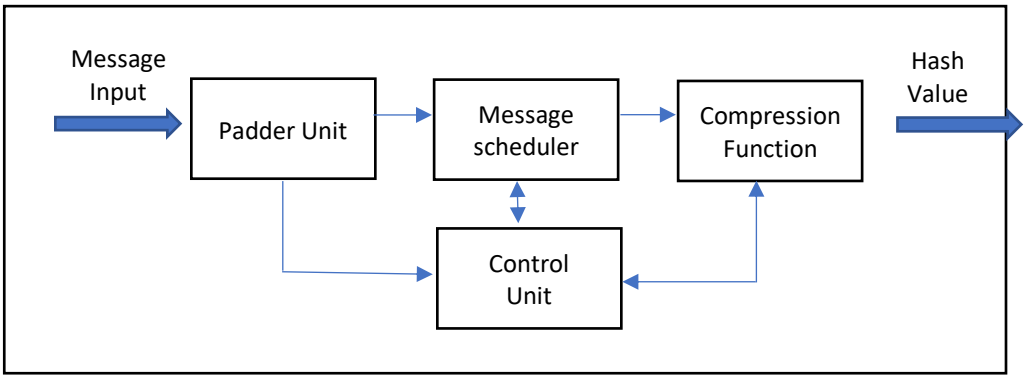
1.7. Algoritma SHA-256

SHA-2 adalah sebuah kriptografi fungsi hash yang dirancang oleh National Security Agency (NSA) dan dipublikasikan oleh National Institute of Standart and Technology (NIST) sebagai sebuah Federal Information Processing Standart

(FIPS) oleh U.S. Ada empat algoritma untuk keamanan fungsi hash yaitu SHA-0, SHA-1, SHA-2, dan SHA-3. NIST memperbaharui SHA-2, dengan panjang output (256 atau 512- bit di atas 160-bit pada SHA-1) dan perbedaan-perbedaan pada SHA ini merupakan besar pesan yang ada pada
proses komputasi[10].

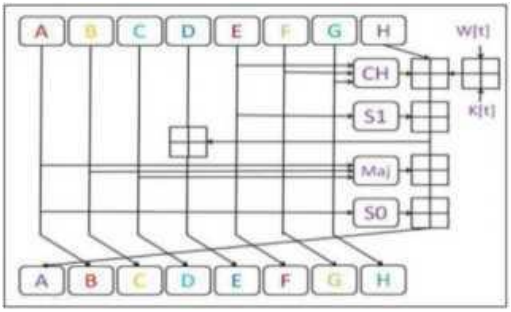
SHA (Algoritma keamanan fungsi hash) merupakan algoritma enkripsi fungsi hash yang dapat digunakan untuk menghasilkan penggambaran konsolidasi dari sebuah data teks yang disebut sebuah proses pesan. SHA-256 dan SHA-512 adalah fungsi hash dengan kapasitas terbaru dengan panjang 32-bit dan 64-bit kata secara terpisah. Kedua fungsi hash ini dalam proses matematisnya menggunakan penjumlahan karakter yang berbeda dan ditambah dengan konstanta substansi. Meski demikian, struktur keduanya pada dasarnya tidak jauh berbeda, perbedaannya hanya terletak pada jumlah putaran saja[10].

Arsitektur sederhana dari algoritma SHA-256 ditunjukkan oleh gambar berikut:



Gambar 2.2 Arsitektur Sederhana SHA-256

Berikut merupakan jalur komputasi SHA-256:



Gambar 2.3. Jalur Komputasi SHA-256

Adapun proses atau tahapan pada algoritma SHA-256 adalah sebagai berikut :

1. Message Padding

Pada tahap pertama ini, pesan berupa binary disisipkan dengan angka 1 dan ditambahkan bit-bit pengganjal, yakni angka 0 hingga panjang pesan kongruen dengan 448 modulo 512. Panjang pesan asli ditambah sebagai angka biner 64 bit. Maka panjang pesan sekarang menjadi kelipatan 512 bit.

2. Parsing

Pada proses ini, pesan yang telah dipadding kemudian dibagi menjadi N buah blok 512 bit : $M^{(1)}$, $M^{(2)}$, … $M^{(n)}$

3. Message Expansion

Masing-masing blok 512 bit tadi dipecah menjadi 16 word 32 bit : $M_0^{(i)}$, $M_1^{(i)}$, … $M_{15}^{(i)}$

Kemudian akan diperluas menjadi 64 word yang diberli label W0, W1,...W63.

4. Message Compression

Masing-masing dari 64 word yang diberi label W0, W1,...W64 tadi diproses denga algoritma fungsi hash SHA-256. Dalam proses tersebut, inti utama dari algoritma SHA-256 adalah membuat 8 variabel yang diberikan nilai awal L0-L7. Nilai awal tersebut adalah sebagai berikut :

Tabel 2.1. Nilai Awal Variabel SHA-256

Lo	a	6A09E667	L4	e	510E527F
L1	b	BB67AE85	L5	f	9B05688C
L2	c	3C6EF372	L6	g	IF83D9AB
L3	d	A54FF53A	L7	h	5BE0CD19

5. Kemudian dilakukan perhitungan sebanyak 64 kali putaran untuk setiap blok. Delapan variabel yang diberikan pada nilai awal berupa L0 sampai dengan L7 asumsikan menjadi nilai A,B,C,D,E,F,G, dan H nilainya terus berganti selama perputaran dengan rumus sebagai berikut :

   T1 = h + s1 + CH + K[t] + W[t]

   T2 = s0 + MAJ

   h = g

   g= f

   f = e

   e = d + T1

   d = c

   c = b

   b = a

   a = T1 + T2

   Keterangan:

   s0 = (a>>> 2) $\oplus$(a>>>13) $\oplus$(a>>>22)

   s1 = (e>>>6) $\oplus(e \ggg 11)(e \ggg 25)$

   CH = (e &f) $\oplus$((¬ e) & g))

   MAJ = (a & b) $\oplus(a \,\&c)\oplus(b \,\&c)$

   Nilai akhir hash adalah sebagai berikut :

   L0 = L0 + a

L1 = L1 + b

L2 = L2 + c

L3 = L3 + d

L4 = L4 + e

L5 = L5 + f

L6 = L6 + g

L7 = L7 + h

Maka, MD yang didapatkan adalah hasil akhir penjumlahan yang disusun secara memanjang.

1.8. Menambang (mining) pada bitcoin

Bitcoin miner adalah salah satu cara agar bisa mendapatkan bitcoin. Kita dapat melihat bitcoin sebagai suatu sistem keuangan global secara virtual dan digital yang menyimpan berbagai riwayat transaksi (atau proses pergerakan uang). Saat transaksi bitcoin sedang diproses oleh jaringan bitcoin, pastikan bahwa semua transaksi telah direkam dengan benar. Sederhananya, bitcoin diproses bukan oles perseorangan atau perusahaan, melainkan oleh ribuan komputer di seluruh dunia yang terhubung dengan internet. Kegiatan tersebut dikenal dengan istilah minner atau miner yang berarti penambangan[11].

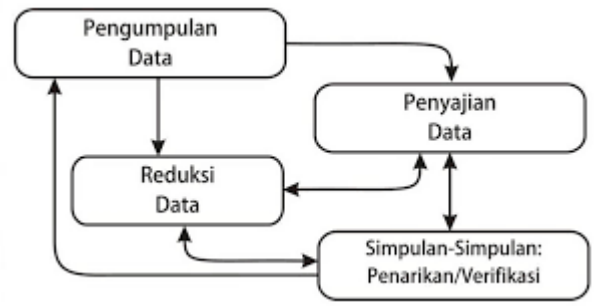
BAB III
METODE PENELITIAN

Metodologi yang digunakan dalam penulisan ini adalah metode analisis data kualitatif dengan pendekatan normatif yang dilakukan dengan cara mengkaji blockchain dari beberapa perspektif. Menurut Sugiyono (2016) metode penelitian kualitatif adalah metode yang digunakan untuk meneliti kondisi objek yang alamiah dimana peneliti sebagai instrumen kunci[12].

Menurut Meleong (2005:6), penelitian kualitatif adalah penelitian yang bermaksud untuk mengetahui kejadian yang di alami oleh subjek penelitian, yang kemudian menghasilkan data yang bersifat deskriptif [13].

Penulis mereduksi data-data yang telah diperoleh selama penelitian dengan cara mengkelompokan serta memilih data yang relevan dengan kajian penelitian. Tahapan selanjutnya penulis melakukan penyusunan data-data yang telah dikelompokan sebelumnya dan yang terakhir penulis melakukan verifikasi atau penarikan kesimpulan. Data penelitian berupa data sekunder yang diperoleh dari artikel jurnal, makalah konferensi, kertas kerja, dan beberapa sumber dari website terpercaya yang membahas blockchain maupun algoritma SHA-256.

Berikut langkah-langkah penelitian analisis data kualitatif yang digambarkan dengan diagram ilmiah, seperti gambar berikut :



Gambar 3.1. Langkah-langkah menggunakan Teknik Analisis Data Kualitatif

BAB IV
HASIL DAN PEMBAHASAN

4.1. Implementasi Blockchain

Blockchain pada dasarnya adalah buku besar transaksi dalam bentuk digital yang diperbanyak atau diduplikasi kemudian disebarluaskan ke seluruh jaringan sistem komputer yang ada pada jaringan blockchain tersebut. Salah satu perbedaan utama antara database biasa dan blockchain adalah terstruktur datanya. Basis data biasanya menyusun datanya ke dalam tabel, sedangkan blockchain, seperti namanya, menyusun datanya menjadi potongan (blok) yang dirangkai.

Ketika sebuah blok diisi dan ditautkan, blok diberi penanda atau stempel waktu. Blok tersebut kemudian dihubungkan bersama dengan kriptografi (hash). Maka terbentuklah rantai yang hampir mustahil diubah. Fungsi Hash banyak sekali digunakan untuk mempercepat pencarian dalam tabel data atau pembandingan data seperti di dalam basis data, mencari duplikasi atau kesamaan (rekaman) di sebuah arsip komputer yang besar, menemukan sesuatu di sebuah DNA, dan sebagainya.

Ada banyak sekali tipe atau jenis dari fungsi hash, berikut ini beberapa diantaranya MD2, MD3, MD4, MD5, MD6, SHA-1, SHA-224,SHA-256, SHA-384, SHA-512, SHA-3.

1. Bitcoin menggunakan SHA-256
2. Ethereum menggunakan Keccak-256

Berikut merupakan contoh manual hasil perhitungan SHA-256 untuk tulisan “tes”[14]:

1. Langkah pertama yaitu input plain teks

Plain teks adalah sebuah kata atau karakter yang akan kita enkrip dengan SHA256 dan Bcrypt, Plain teks yang akan di buat oleh penulis yaitu : tes

2. Pada tahap ini pesan yang dimasukan oleh penulis tadi akan di ubah ke dalam bentuk angka biner agar bisa ke tahap selanjutnya.

   t= 01110100 e=01100101 s= 01110011

   Setelah di ubah ke angka biner maka pesan "tes" tadi menjadi M=011101000110010101110011 Diketahui panjang pesan = 24 bit

3. *Message Padding*

   Padding pesan yang telah di ubah ke angka biner tadi dengan cara menambahkan bit 1 dan sisanya bit nol hingga pesan sepanjang 512 bit. Untuk menemukan berapa bit nol yang akan ditambahkan maka laukan dengan rumus :

   I + 1+k = 448 mod 512 k = 448-25 mod 512

   24+1+k = 448 mod 512 k = 423

   Karena K = 423 maka banyaknya bit 0 yang akan ditambahkan adalah sebanyak 423 bit.

4. *Parsing*

   Pesan yang telah dipadding menghasilkan blok pesan 512 bit selanjutnya adalah melakukan pembagian setiap blok 512 bit menjadi 16 buah word 32 bit.

5. *Message Schadule*

   Tahap ini adalah memperluas memperluas masing-masing 16 buah word yang telah diparsing menjadi 64 buah 32 bit word.

6. Inisialisasi Variabel dan Konstanta

Tahap kita hanya perlu menuliskan variabel awal pada fungsi SHA- 256 kemudian kita inisialisasikan, yaitu sebagai berikut: a = H0(0) = 6A09E667, b = H0(1) = BB67AE85 c = H0(2) = 3C6EF372, d = H0(3) = A54FF53A e = H0(4) = 510E527F, f = H0(5) = 9B05688C g = H0(6) = 1F83D9AB

7. *Hash Computation*

   Dalam proses ini dilakukan perhitungan nilai a sampai h sebanyak 64 kali putaran.

8. *Computer intermediate Hash Value + Initial Hash Value*

   Setelah didapat hasil ke 64 dalam proses Hash Computation kemudian dilakuan proses penjumlahan hasil ke-64 dengan nilai hash value.

9. Penggabungan H0 - H7

   Tahap ini kita hanya perlu melakukan penggabungan hasil dari penjumlahan ke-64 dan hash value.

10. Nilai Hash

Dengan seluruh proses yang telah dilalui didapatlah nilai hash SHA- 256 dari pesan tes:

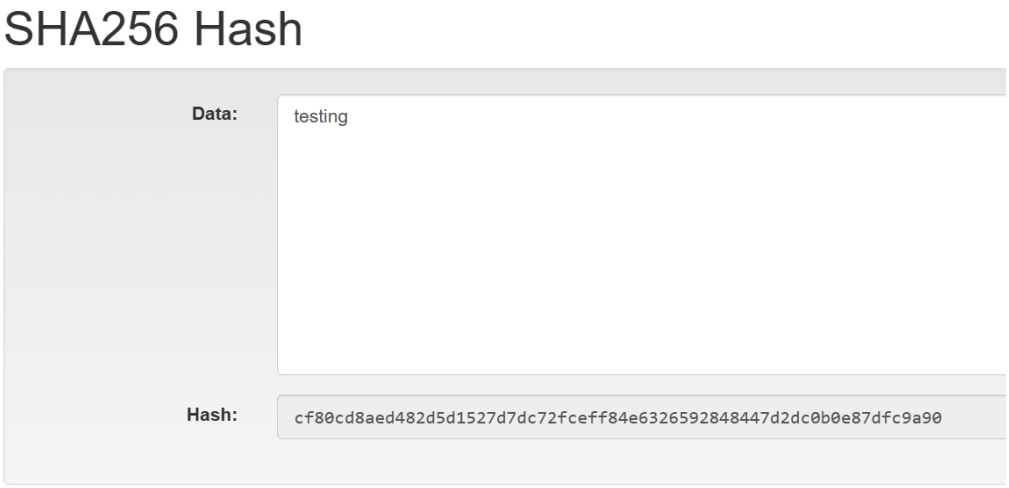
ce0f6c28b5869ff166714da5fe08554c70c731a335ff9702e38b00f81ad348c6

4.2. Implementasi Hash SHA-256 dan Cara Kerja Blockchain kedalam Sistem

Berikut ini merupakan contoh kode hash yang dihasilkan oleh SHA-256 untuk tulisan “test” sesuai dengan contoh manual diatas dengan menggunakan tools[15] blockchain hash SHA-256 :

Gambar 4.1. Proses Hash SHA-256 pada sistem

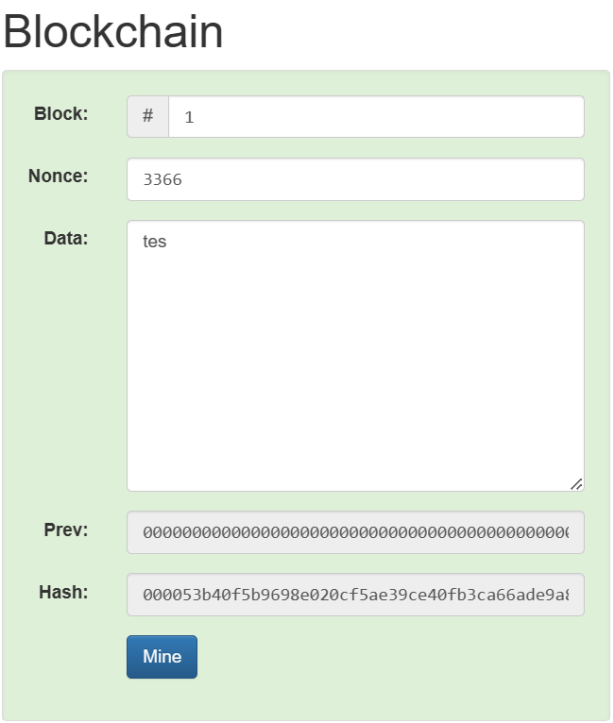
Setiap perubahan apapun yang terjadi pada teks “tes” pasti akan mengubah has yang dihasilkan. Misalkan menambah teks menjadi “testing”. Maka akan menghasilkan hash berikut ini :



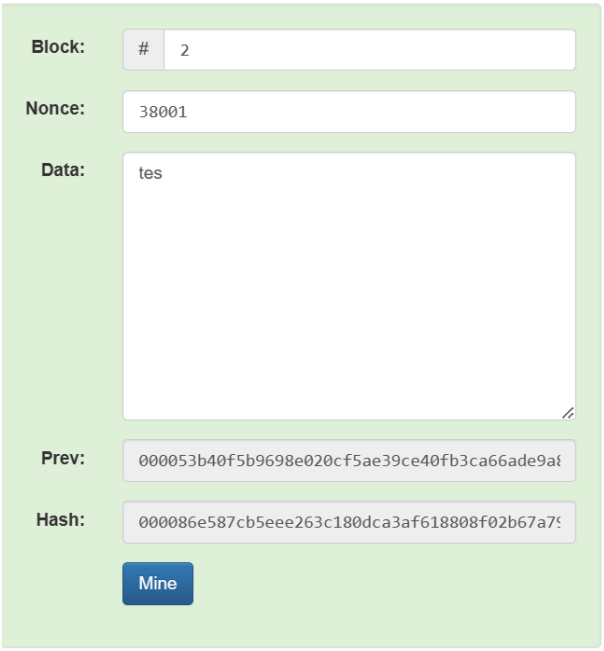
Gambar 4.1. Proses Hash SHA-256 pada sistem saat dirubah

Hasil dari HASH-256 tidak lebih dari 64 karakter yang terdiri dari huruf maupun angka yang acak.

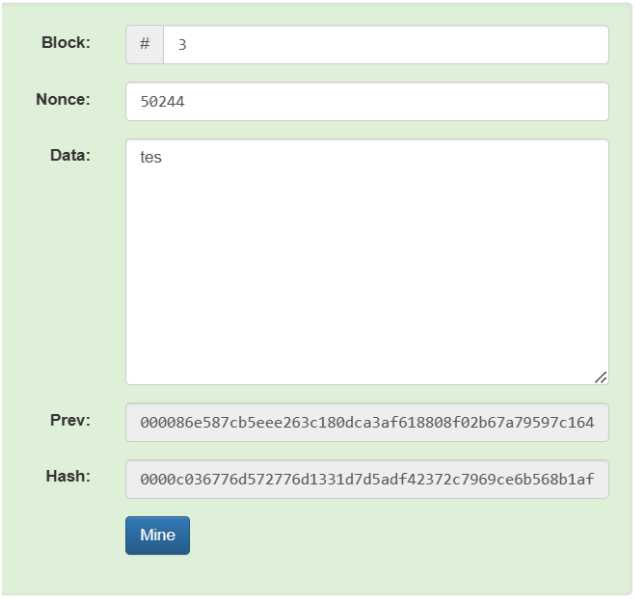
Selanjutnya proses mining dengan blockchain dengan data hash sebelumnya:



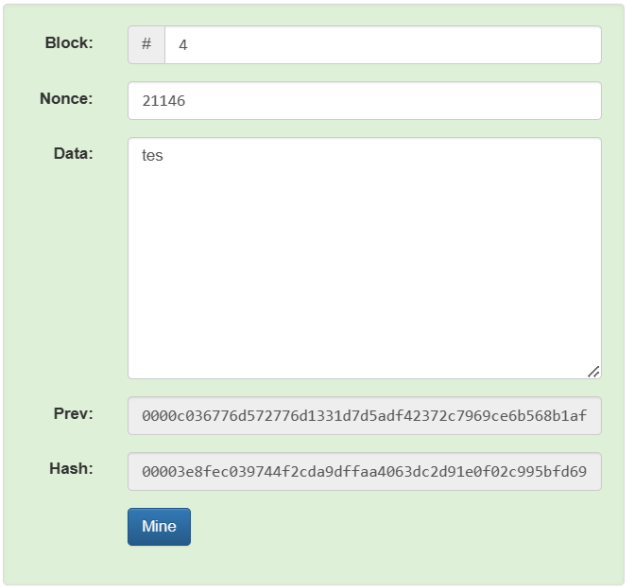
Gambar 4.3. Proses Mining Blockchain Block 1



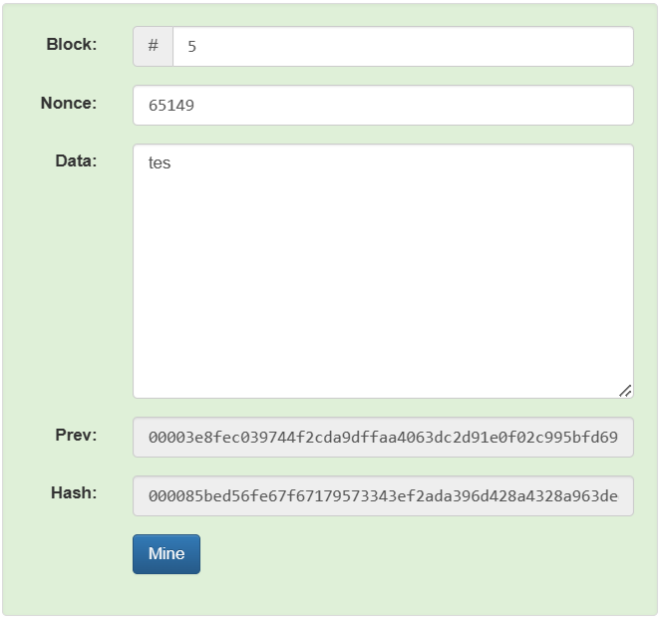
Gambar 4.4. Proses Mining Blockchain Block 2



Gambar 4.5. Proses Mining Blockchain Block 3

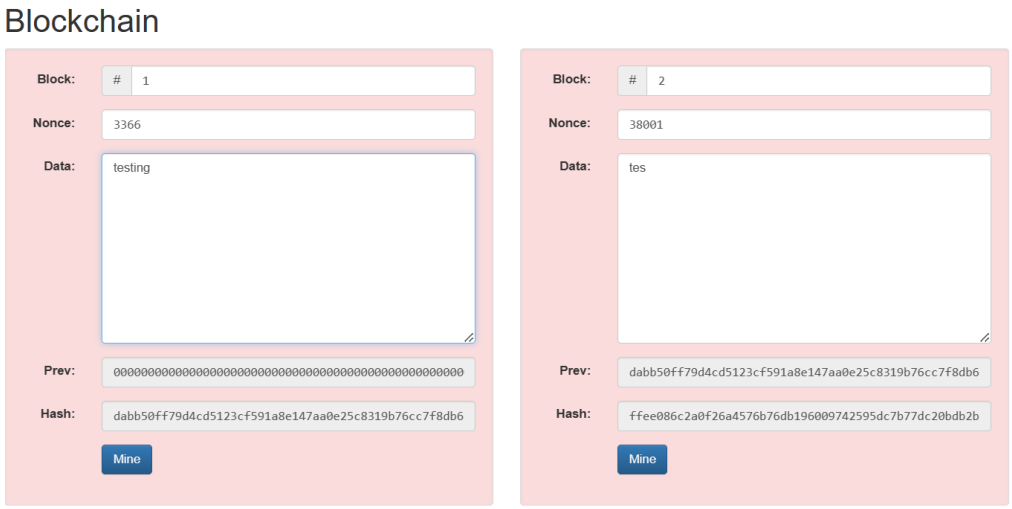


Gambar 4.6. Proses Mining Blockchain Block 4

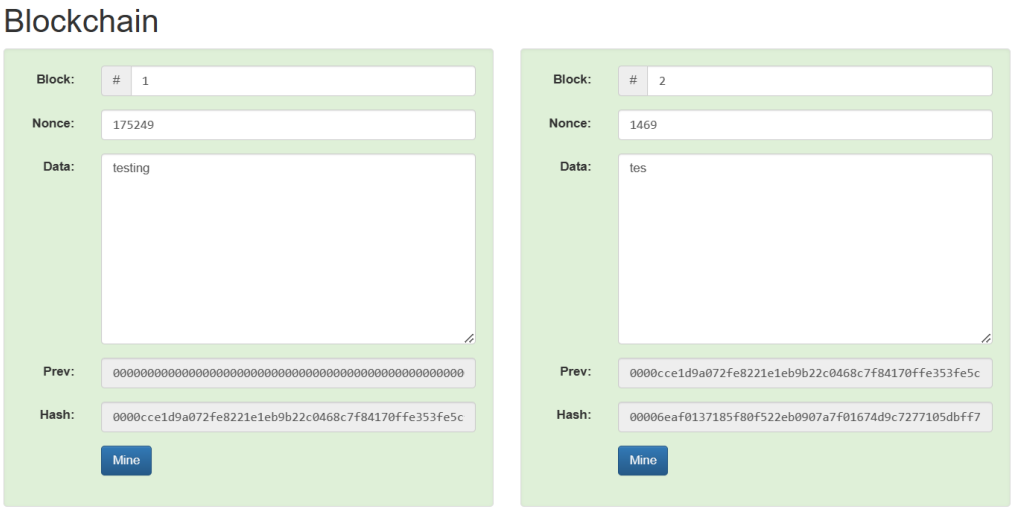


Gambar 4.7. Proses Mining Blockchain Block 5

Selanjutnya akan dicoba merubah data pada salah satu block seperti pada gambar berikut:



Gambar 4.8. Proses Perubahan Data Pada Salah Satu Block



Gambar 4.8. Proses Mining Kembali Data Yang Dirubah

Pada gambar diatas terlihat bahwa jika terjadi perubahan data pada salah satu block maka block yang lain juga akan berpengaruh dengan di tandai dengan warna orange di sistem. Artinya jika ada perubahan pada salah satu block maka harus di lakukan mining Kembali untuk memecahkan kode hash sesuai dengan nilai nonce blockchain.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian disimpulkan bahwa Algoritma SHA-256 digunakan dalam proses mining teknologi blockchain bitcoin. Hasil perhitungan manual menunjukan beberapa tahapan yang menghasilkan suatu nilai hash yang selanjutnya akan digunakan dalam proses pengaman teknologi blockchain pada bitcoin. Percobaan yang dilakukan melalui aplikasi sesuai dengan perhitungan manual algoritma SHA-256 dan terlihat adanya perubahan data pada setiap block jika salah satu block dirubah datanya. Dengan demikian harus dilakukan proses mining Kembali untuk menciptakan nilai hash yang baru.

5.2. Saran

Saran pada penelitian selanjutnya diharapkan dapat menganalisis algoritma yang digunakan pada mata uang kripto lainnya dan dapat menjadi referensi kelimuan dalam bidang kriptografi dan keamanan jaringan.

DAFTAR PUSTAKA

[1] A. Afrizal, M. Marliyah, and F. Fuadi, "Analisis Terhadap Cryptocurrency (Perspektif Mata Uang, Hukum, Ekonomi Dan Syariah)," *E-Mabis J. Ekon. Manaj. dan Bisnis*, vol. 22, no. 2, pp. 13–41, 2021, doi: 10.29103/e-mabis.v22i2.689.

[2] R. C. Noorsanti, H. Yulianton, and K. Hadiono, "Blockchain - Teknologi Mata Uang Cryptocurrency," *Pros. SENDI_U 2018*, pp. 978–979, 2018.

[3] Wikipedia, "Mata uang kripto." https://id.wikipedia.org/wiki/Mata_uang_kripto

[4] H. Yulianton, U. S. Semarang, S. Mulyani, and U. S. Semarang, "Implementasi sederhana blockchain," no. December, pp. 0–4, 2018.

[5] B. U. Indonesia, "presents Blockchain Untuk Indonesia Pencapaian Industri".

[6] Q. Jurnal, E. Dan, B. Islam, M. Faozi, and E. S. Gustanto, "Blockchain , bitcoin ," vol. 1, pp. 127–151, 2022.

[7] M. N. Hasani, "Analisis Cryptocurrency Sebagai Alat Alternatif Dalam Berinvestasi Di Indonesia Pada Mata Uang Digital Bitcoin," *J. Ilm. Ekon. Bisnis*, vol. 8, no. 2, pp. 21–36, 2022.

[8] A. Z. Ausop and E. S. N. Aulia, "Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam," *J. Sosioteknologi*, vol. 17, no. 1, pp. 74–92, 2018, doi: 10.5614/sostek.itbj.2018.17.1.8.

[9] B. P. 2009-2022 D. di bawah lisensi MIT, "Bagaimana cara kerja Bitcoin?" https://bitcoin.org/id/cara-kerja

[10] Z. Panjaitan, E. F. Ginting, and Y. Yusnidah, "Modifikasi SHA-256 dengan Algoritma Hill Cipher untuk Pengamanan Fungsi Hash dari Upaya Decode Hash," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 19, no. 1, p. 53, 2020, doi: 10.53513/jis.v19i1.225.

[11] R. M. Vekelita, “Apa Itu Bitcoin Miner? Bagaimana Cara Kerja Mining Bitcoin?,” 2021.

[12] Subandi, “Qualitative Description as one Method in Performing Arts Study,” *Harmonia*, no. 19, pp. 173–179, 2011.

[13] R. S. Giffary and E. Ramadhani, “Implementasi Bcrypt dengan SHA-256 pada Password Pengguna Aplikasi Golek Kost,” *J. Sist. Komput. dan Inform. Hal 543−*, vol. 546, no. 4, pp. 543–546, 2022, doi: 10.30865/json.v3i4.4285.

[14] A. Funnatiq, P. S. Matematika, F. Sains, D. A. N. Teknologi, U. Islam, and N. Syarif, “Implementasi Algoritma Sha -256 Menggunakan Implementasi Algoritma Sha -256 Menggunakan,” 2013.

[15] A. Brownworth, “Blockchain Demo.” https://andersbrownworth.com/blockchain/

Biodata Peneliti

a. Ketua

1. Nama lengkap : Ilka Zufria, M.Kom
2. NIP : 19850604 201503 1 006
3. Pangkat/ Gol / Jabfung : Penata Tk.I / III.d / Lektor
4. Tempat/Tanggal Lahir : Medan, 04 Juni 1985
5. Jenis Kelamin : Laki-laki
6. Bidang Keahlian : Sistem Informasi
7. Kantor/Unit Kerja : UINSU Medan/ Fak Saintek
8. Alamat Kantor : Jln. Lapangan Golf No 120, Durin Jangak, Kec. P.Batu, Deli Serdang
   Kabupaten : Deli Serdang
   Kode Pos : 20353
   Telepon : (+6261) 6615683; 6622925
   Faksimile : (+6261) 6615683
   Email : ilkazufria@uinsu.ac.id
9. Alamat Rumah : Jln. Sederhana Gg. Raya 34, No. 04 Sambirejo Timur, Pasar 7 Tembung Kec. Percut Sei Tuan
10. Kabupaten : Deli Serdang Kode Pos:20371
    Telepon : -
    Faksimile : -
    No. HP. : +6281397238909
11. Pendidikan (S1 ke atas)

No	Perguruan Tinggi	Kota & Negara	Jenjang Pendidikan	Tahun Lulus	Bidang Studi
1.	UPI "YPTK" Padang	Padang, Indonesia	S2	2009	Ilmu Komputer (Sistem Informasi
2.	UPI "YPTK" Padang	Padang, Indonesia	S1	2006	Sistem Informasi

b. Anggota 1

Nama Lengkap dan gelar : Yusuf Ramadhan Nasution, M.Kom

NIP : 1100000075

Pangkat/Jabatan : III-c/lektor

Jenis Kelamin : Laki-laki

Tempat dan tanggal lahir : Medan, 25 Mei 1985

Alamat : Jalan Datuk Kabu Gg. Pisang 2

No. Telephone/HP : 081375158900

Email : ramadhannst@uinsu.ac.id

Riwayat Pendidikan :

1. SD Negeri 060913 Medan Tamat Tahun 1997
2. SMP Budisatrya Medan Tamat Tahun 2000
3. SMU Josua Medan Tamat Tahun 2003
4. STMIK Budidarma Medan Tamat Tahun 2009
5. UPI YPTK Padang Tamat Tahun 2014

c. Anggota 2

1. Nama Lengkap : Raja Alfiansyah
2. NIM : 0701172060
3. Status : Mahasiswa Semester VII
4. Program Studi : Ilmu Komputer
5. Jenis Kelamin : Laki-laki
6. Tempat dan tanggal lahir : Kota Tanjungbalai, 29-06-2001
7. Alamat : JL.PUNGGUK PERUMAHAN CALISTA CITY NO.11 Kelurahan Sei Sikambing B Kecamatan MEDAN SUNGGAL
8. No. Telephone/HP : 0853 6002 2268