Penerapan *Smart Contract Ethereum* pada Aplikasi *Crowdfunding* dengan Keamanan *Keccak-256*

1st M. Naufal Faqih
Universitas Buana Perjuangan Karawang
Karawang, Indonesia
if21.m.faqih@mhs.ubpkarawang.ac.id

2rd Deden Wahiddin
Universitas Buana Perjuangan Karawang
Karawang, Indonesia
deden.wahiddin@ubpkarawang.ac.id

3rd Kiki Ahmad Baihaqi
Universitas Buana Perjuangan Karawang
Karawang, Indonesia
kikiahmad@ubpkarawang.ac.id

4th Yana Cahyana
Universitas Buana Perjuangan Karawang
Karawang, Indonesia
yana.cahyana@ubpkarawang.ac.id

Abstract*— Crowdfunding telah muncul sebagai metode yang populer untuk mengumpulkan dana secara online, namun masalah seperti salah urus dana dan kurangnya transparansi masih tetap ada. Penelitian ini bertujuan untuk mengatasi masalah ini dengan mengembangkan platform crowdfunding berdasarkan teknologi blockchain menggunakan smart contract di Ethereum. Sistem ini memastikan transparansi, integritas, dan ketertelusuran transaksi dengan mencatatnya secara permanen di blockchain. Setiap kampanye penggalangan dana diidentifikasi menggunakan ID unik yang dihasilkan melalui algoritma hashing Keccak-256, yang mencegah duplikasi data dan memastikan pengindeksan yang aman. Proses pengembangan termasuk merancang smart contract, mengimplementasikan antarmuka berbasis web, dan menerapkan server backend untuk penyimpanan gambar menggunakan Express.js. Fungsionalitas sistem diuji menggunakan pengujian blackbox di beberapa skenario, termasuk pembuatan kampanye, pemrosesan donasi, dan validasi penarikan. Hasilnya menunjukkan bahwa sistem bekerja dengan baik, dengan setiap fitur inti beroperasi seperti yang diharapkan dan integritas data terjaga. Transparansi dicapai melalui transaksi yang dapat diverifikasi secara publik, sementara penggunaan Keccak-256 memberikan perlindungan yang efektif terhadap gangguan. Analisis biaya gas menunjukkan bahwa transaksi tetap berada dalam kisaran biaya yang wajar untuk implementasi skala kecil. Studi ini menunjukkan bagaimana sistem berbasis blockchain dapat meningkatkan kepercayaan pada platform crowdfunding dan menawarkan referensi untuk pengembangan sistem penggalangan dana yang transparan dan aman di masa depan.

Kata kunci — Crowdfunding, Blockchain, Ethereum, Smart Contract, Keccak-256, Blackbox Testing

I. PENDAHULUAN

Crowdfunding telah menjadi salah satu komponen penting dalam dunia filantropi dan bisnis digital [1]. Crowdfunding adalah proses di mana individu atau organisasi berupaya mengumpulkan dana dari sejumlah besar orang, sering kali melalui internet [2]. Tujuan crowdfunding adalah untuk mendukung proyek, kegiatan sosial, atau usaha tertentu. Dengan berkembangnya kebutuhan akan penggalangan dana untuk berbagai keperluan, seperti bantuan sosial, kegiatan kreatif, dan pendanaan proyek bisnis, kini individu maupun organisasi dapat dengan mudah melakukannya melalui platform-platform seperti Kitabisa, Trakteer, dan Saweria [3]. Konsep ini menghilangkan batasan jarak dan waktu, memungkinkan masyarakat luas untuk berkontribusi secara finansial melalui internet.

Namun, meningkatnya popularitas Crowdfunding menimbulkan risiko penggelapan dan penyalahgunaan dana yang merugikan donatur maupun penerima dana. Salah satu isu utama adalah risiko penggelapan dana atau penyalahgunaan dana yang terkumpul [4]. Dalam beberapa kasus, dana yang telah dikumpulkan tidak digunakan sesuai dengan tujuan kampanye awal yang disepakati. Hal ini tidak hanya merugikan para donatur, tetapi juga berdampak buruk pada kepercayaan masyarakat terhadap platform crowdfunding secara keseluruhan [5]. Transparansi dan akuntabilitas pengelolaan dana menjadi tantangan utama dalam ekosistem crowdfunding, terutama ketika pengawasan terhadap penggunaan dana masih terbatas [1].

Untuk mengatasi tantangan ini, teknologi blockchain dapat menjadi solusi. Blockchain adalah teknologi yang memungkinkan pencatatan transaksi secara terdesentralisasi, transparan, dan tidak dapat diubah (immutable) [6]. Ethereum, salah satu blockchain populer, menyediakan fitur smart contract untuk mengotomatiskan eksekusi transaksi sesuai dengan ketentuan yang telah ditetapkan [7]. Smart contract pada platform crowdfunding memastikan dana digunakan sesuai tujuan dan meminimalkan risiko penggelapan.

Salah satu komponen kunci dalam menjaga keamanan dan integritas data pada blockchain adalah algoritma Keccak-256. Algoritma ini digunakan untuk menghasilkan hash yang unik dan aman, memastikan bahwa data transaksi tidak dapat diubah atau dipalsukan [8]. Dalam smart contract, Keccak-256 berperan penting dalam memverifikasi integritas data dan memastikan bahwa setiap transaksi tercatat secara akurat dan konsisten.

Penelitian terkait pada penggunaan teknologi blockchain dalam ekosistem crowdfunding telah mendapatkan perhatian dari berbagai pihak. Misalnya, penelitian F. Aprialim menunjukkan bahwa integrasi blockchain pada platform Crowdfunding menyediakan catatan transaksi yang transparan dan tidak dapat diubah [9]. Penelitian H. Kartiko dengan integrasi teknologi InterPlanetary File System (IPFS) pada smart contract ethereum untuk meningkatkan efisiensi sistem crowdfunding dengan menurunkan gas fee rata-rata hingga 94,39% dan meningkatkan kecepatan transaksi hingga 13,55%, khususnya dalam hal pengurangan biaya transaksi dan kompleksitas penyimpanan data [10]. Selain itu, Penelitian A. Mubroh dengan algoritma Proof of Authority pada smart contract menghasilkan waktu delay rata-rata stabil sekitar 6 detik untuk sistem smart meter, sementara proses

pengiriman data melalui MQTT memiliki delay maksimal 30,07 detik, lalu sistem ini efektif untuk penyimpanan data daya listrik dengan interval waktu 30 detik, sehingga tetap dapat memperkuat keamanan dan akurasi data [11].

Penelitian ini bertujuan untuk mengimplementasikan smart contract ethereum pada aplikasi crowdfunding berbasis website, dengan memanfaatkan algoritma Keccak-256 untuk memastikan integritas data. Dengan demikian, penelitian ini diharapkan dapat meningkatkan transparansi, keamanan, dan kepercayaan publik terhadap platform crowdfunding.

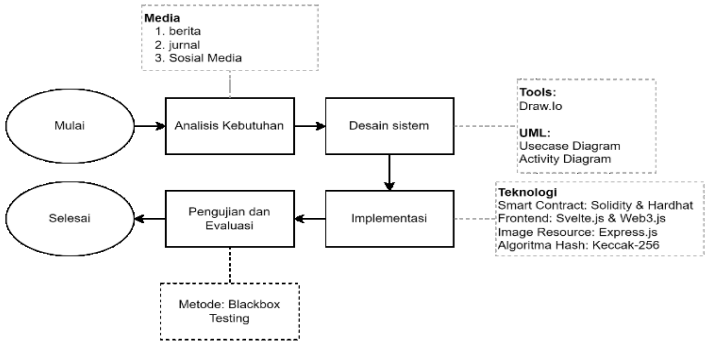
II. METODE PENELITIAN

A. Objek Penelitian

Objek penelitian ini berfokus pada penerapan blockchain dalam platform crowdfunding dengan ethereum, yang memanfaatkan smart contract untuk penggalangan dana secara transparan. Setiap penggalangan dana diidentifikasi dengan ID unik yang dihasilkan menggunakan hash dari kombinasi nama, deskripsi, gambar, target dana, dan deadline. Hash ini digunakan sebagai key dalam data index mapping untuk memastikan setiap penggalangan dana memiliki identifikasi yang unik.

B. Prosedur Penelitian

Prosedur penelitian ini disusun untuk merancang, mengimplementasikan, dan menguji platform crowdfunding berbasis blockchain ethereum.



Gambar 1 Flowchart Prosedur Penelitian

Tahapan penelitian meliputi analisis kebutuhan, pengembangan, implementasi dan evaluasi sistem. Diagram alur proses utama digambarkan untuk memvisualisasikan setiap langkah secara jelas.

C. Analisis Kebutuhan

Crowdfunding telah menjadi solusi populer untuk penggalangan dana secara online [12]. Namun, berita menunjukkan bahwa masih sering terjadi penyalahgunaan dana, kurangnya transparansi dalam pengelolaan, hingga kasus penipuan pada platform crowdfunding [13]. Hal ini menurunkan kepercayaan masyarakat terhadap platform yang ada. Sistem ini dirancang untuk mengatasi permasalahan tersebut menggunakan teknologi blockchain.

D. Identifikasi Masalah

Berdasarkan penelitan menurut [4], platform crowdfunding menghadapi beberapa tantangan utama yang memengaruhi kepercayaan pengguna dan efektivitas sistem. Tantangan-tantangan tersebut meliputi kasus penipuan dan penyalahgunaan, kurangnya transparansi penggunaan dana, dan tidak adanya mekanisme efektif untuk mencegah penyalahgunaan Dana.

E. Kebutuhan Fungsional

Kebutuhan fungsional merujuk pada fungsi inti yang harus dimiliki oleh sistem Crowdfunding berbasis blockchain. kebutuhan fungsional umum pada platform seperti ini meliputi:

1) Pembuatan Penggalangan Dana

Sistem harus memungkinkan pengguna untuk membuat kampanye penggalangan dana dengan memasukkan data seperti nama kampanye, deskripsi, target dana, dan batas waktu. Hal ini sesuai dengan penelitian oleh [14], yang menekankan pentingnya fleksibilitas dalam pembuatan kampanye untuk meningkatkan partisipasi pengguna.

2) Transaksi Donasi yang Aman dan Transparan

Setiap transaksi harus dicatat di blockchain untuk menjamin keamanan dan transparansi, seperti yang diungkapkan oleh [15]. Penggunaan hashing Keccak-256 juga memberikan tingkat keamanan tambahan pada integrasi data untuk memastikan data dapat diaudit jika terjadi manipulasi. Pengguna juga harus dapat memantau status kampanye secara real-time, termasuk dana terkumpul dan total donatur. Berdasarkan [4] menekankan bahwa transparansi dalam laporan meningkatkan kepercayaan pengguna terhadap platform.

F. Kebutuhan Non-Fungsional

Kebutuhan non-fungsional sangat penting untuk memastikan efektivitas dan keamanan sistem. Berdasarkan hal tersebut, kebutuhan non-fungsional sistem ini meliputi:

1) Keamanan

Sistem menggunakan hashing Keccak-256 untuk menjaga integritas data, sesuai rekomendasi standar keamanan data dalam pengembangan blockchain [8], [16].

2) Efesiensi

Sistem dirancang tanpa menggunakan database tradisional seperti NoSQL, dan data dicatat langsung di blockchain untuk mengurangi kompleksitas serta meningkatkan efisiensi pencatatan [17].

3) Antarmuka Pengguna (UI)

Antarmuka yang ramah pengguna dirancang menggunakan framework frontend Svelte.js, yang terkenal karena kecepatan rendering dan efisiensinya dalam aplikasi web [18].

G. Teknologi yang digunakan

Menurut berbagai penelitian Teknologi yang cocok digunakan dalam sistem ini meliputi:

1) Solidity & Hardhat

Solidity digunakan untuk pengembangan smart contract, sementara Hardhat digunakan sebagai framework untuk pengujian dan *debugging* smart contract. Kombinasi ini sering direkomendasikan dalam pengembangan berbasis Ethereum karena kemudahan penggunaannya [19], [20], [21].

2) Express.js

Framework ini digunakan untuk menangani penyimpanan gambar secara tanpa memanfaatkan layanan IPFS. Penggunaan Express.js efektif untuk kebutuhan penyimpanan sederhana karena umum dan mudah saat proses pengembangan [22].

3) Svelte.js & Web3.js

Svelte.js digunakan sebagai framework frontend karena kemampuannya yang efisien dalam rendering UI, sementara Web3.js memfasilitasi interaksi dengan smart contract di blockchain Ethereum [23].

4) Keccak-256

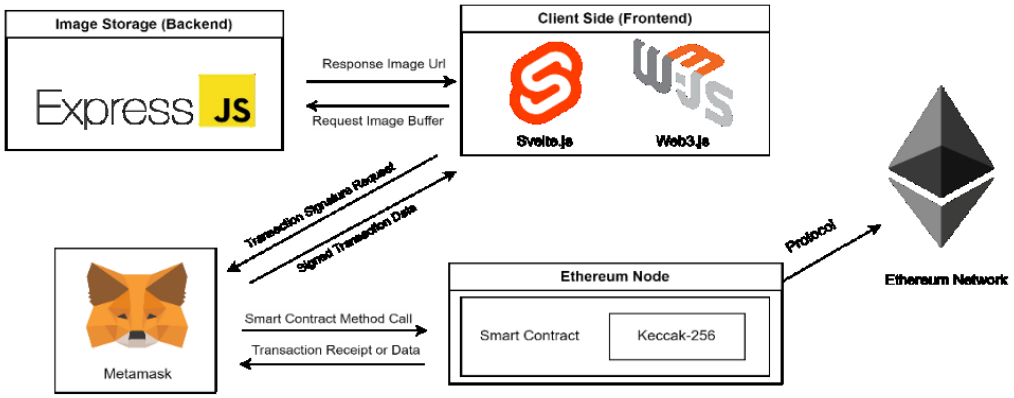
Algoritma ini digunakan untuk hashing, yang berfungsi menjaga integritas dan keamanan data. Hal ini sejalan dengan praktik terbaik dalam pengelolaan data berbasis blockchain [16], [24].

H. Desain Sistem

Desain sistem menggambarkan alur dan struktur sistem sebelum implementasi. Tahap ini mencakup gambaran umum sistem, use case diagram untuk menunjukkan interaksi pengguna, serta activity diagram untuk memodelkan alur aktivitas. Ketiganya menjadi dasar dalam proses pengembangan dan pengujian sistem.

1) Gambaran Umum Sistem

Gambaran umum sistem ini dirancang untuk memastikan setiap komponen memiliki peran yang jelas dalam pengelolaan crowdfunding berbasis blockchain.



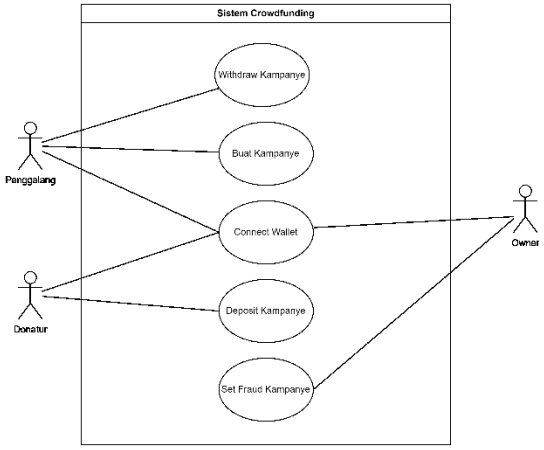
Gambar 2 Gambaran Umum Sistem

Arsitektur sistem crowdfunding berbasis blockchain ini dirancang dengan peran terpisah untuk setiap komponennya. Backend menggunakan Express.js untuk menangani penyimpanan gambar, di mana frontend yang dikembangkan dengan Svelte dan Web3.js mengirimkan gambar sebagai request buffer dan menerima URL gambar sebagai respons. Interaksi dengan blockchain difasilitasi melalui Metamask, yang menghubungkan frontend ke Ethereum Node. Di dalam Ethereum Node, smart contract bertanggung jawab memproses transaksi, sementara algoritma Keccak-256 digunakan untuk melakukan hashing ID

penggalangan dana guna memastikan setiap ID bersifat unit, kemudian hasil pemrosesan ini kemudian dikirim kembali ke frontend melalui Metamask.

2) Usecase Diagram

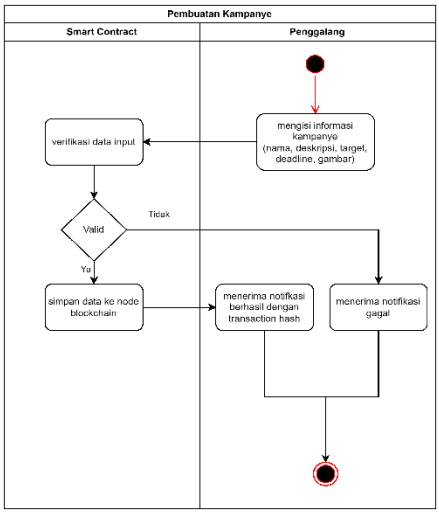
Usecase diagram ini memvisualisasikan interaksi antara aktor dan sistem pada platform Crowdfunding berbasis blockchain, mencakup alur kerja yang mendukung keamanan serta transparansi.



Gambar 3 Usecase Diagram Sistem Crowdfunding

3) Activity Diagram

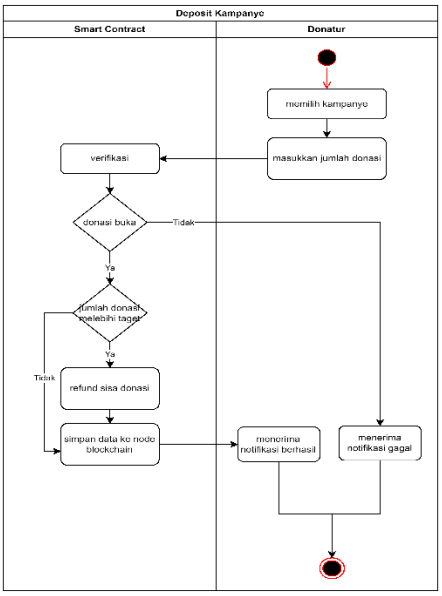
Sistem Crowdfunding mencakup beberapa aktivitas utama yang dirancang untuk mendukung transparansi, keamanan, dan efisiensi pengelolaan penggalangan dana.



Gambar 4 Activity Diagram Pembuatan Kampanye

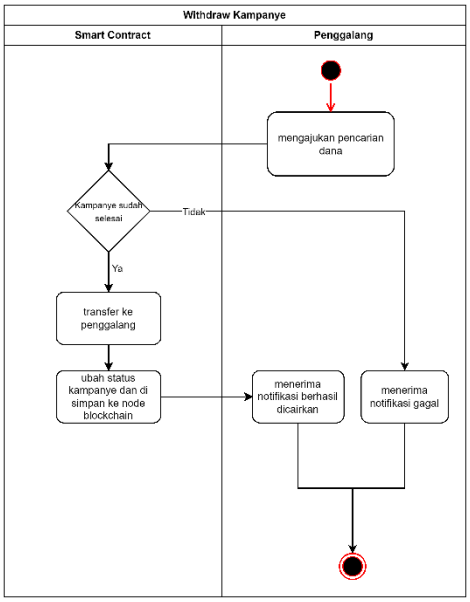
Pada Gambar 4, ditampilkan activity diagram proses pembuatan kampanye. Diagram ini menggambarkan alur mulai dari pengisian data oleh pengguna, proses validasi data, hingga penyimpanan ke sistem. Terdapat percabangan kondisi yang menunjukkan apakah data yang diinput sesuai atau tidak, dan sistem akan merespons sesuai dengan hasil validasi tersebut.

ISSN: 2715-2766
Vol. 7 No. 1, Januari 2026



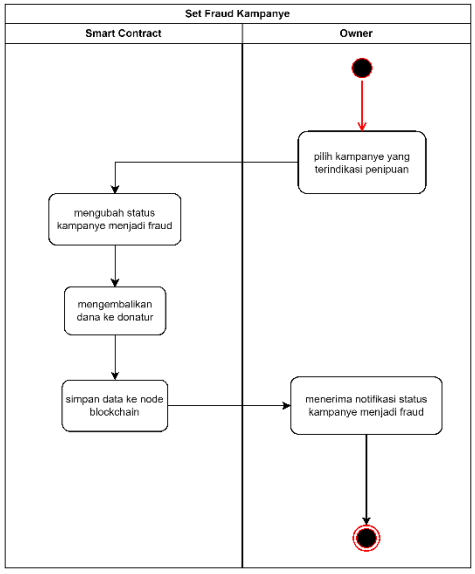
Gambar 5 Activity Diagram Deposit Kampanye

Pada Gambar 5, ditampilkan activity diagram proses donasi pada kampanye. Alur dimulai dari pemilihan kampanye oleh pengguna, kemudian dilanjutkan dengan pengisian nominal donasi. Sistem akan melakukan validasi terhadap saldo pengguna; jika saldo tidak mencukupi, transaksi akan ditolak. Namun, jika saldo mencukupi, donasi akan diproses. Dalam kondisi di mana jumlah donasi melebihi target kampanye, kelebihan dana akan secara otomatis dikembalikan kepada pengguna.



Gambar 6 Activity Diagram Withdraw Kampanye

Pada Gambar 6, ditampilkan activity diagram proses penarikan dana (withdraw) oleh pembuat kampanye. Proses ini hanya dapat dilakukan jika memenuhi ketentuan yang berlaku, seperti batas waktu kampanye telah berakhir atau target dana telah tercapai. Jika syarat tidak terpenuhi, sistem akan menolak permintaan. Sebaliknya, jika semua ketentuan terpenuhi, dana akan ditransfer ke saldo pembuat kampanye.



Gambar 7 Activity Diagram Set Fraud Kampanye

Pada Gambar 7, ditampilkan activity diagram proses penandaan kampanye sebagai penipuan (set fraud). Proses ini hanya dapat dilakukan oleh akun pemilik (owner). Jika sebuah kampanye terindikasi sebagai penipuan, owner dapat mengubah status kampanye menjadi fraud. Setelah status diubah, kampanye tersebut tidak dapat lagi diakses atau digunakan oleh pengguna.

I. Implementasi

Pada tahap implementasi, sistem ini dikembangkan menggunakan teknologi dan metode yang telah direncanakan sebelumnya. Proses implementasi melibatkan pengembangan frontend, backend, dan smart contract, yang saling berintegrasi untuk menyediakan layanan penggalangan dana. Pada integrasi sistem, bagian ini menjelaskan bagaimana komponen sistem terhubung untuk mendukung fungsionalitas utama:

1) Otentikasi dan Transaksi

Pengguna dapat menghubungkan akun Ethereum mereka menggunakan MetaMask, yang berfungsi sebagai perantara antara aplikasi frontend dan blockchain. MetaMask digunakan untuk mengotorisasi transaksi seperti donasi atau pembuatan kampanye.

2) Komunikasi dengan Blockchain

Aplikasi frontend yang dibuat dengan Svelte.js menggunakan library Web3.js untuk mengirim dan menerima data dari blockchain. Proses ini mencakup transaksi dan pengambilan informasi kampanye.

3) Keamanan Data

Sistem memanfaatkan hashing Keccak-256 untuk memastikan integritas data. Hash ini digunakan sebagai indeks unik untuk setiap penggalangan.

J. Pengujian Sistem

Pengujian sistem bertujuan untuk memastikan bahwa sistem berfungsi dengan baik sesuai dengan tujuan yang telah ditentukan. Pengujian dilakukan menggunakan metode blackbox testing, yang berfokus pada pengujian fungsionalitas sistem tanpa mempertimbangkan struktur internal atau kode sumbernya [25]. Berdasarkan penelitian [26], pengujian blackbox sangat efektif untuk mengevaluasi apakah sistem memenuhi persyaratan yang telah ditetapkan, terutama dalam pengujian fungsionalitas antarmuka pengguna. Dalam penelitian ini, pengujian dilakukan untuk mengevaluasi beberapa aspek utama sebagai berikut:

1) Verifikasi Smart Contract

menguji apakah smart contract yang diterapkan dapat berfungsi sesuai ketentuan, seperti pembuatan penggalangan dana, pengumpulan dana, hingga penarikan dana oleh penggalang dana.

2) Keamanan dan Keaslian Data

memastikan bahwa data transaksi yang disimpan di blockchain tidak dapat dimanipulasi serta menguji penerapan algoritma Keccak-256 untuk memvalidasi integritas data.

3) *Transparansi*

menguji kemampuan sistem untuk memberikan informasi yang jelas terkait status penggalangan dana, jumlah donasi yang diterima, dan proses penarikan dana. Transparansi ini bertujuan untuk meningkatkan kepercayaan pengguna terhadap platform.

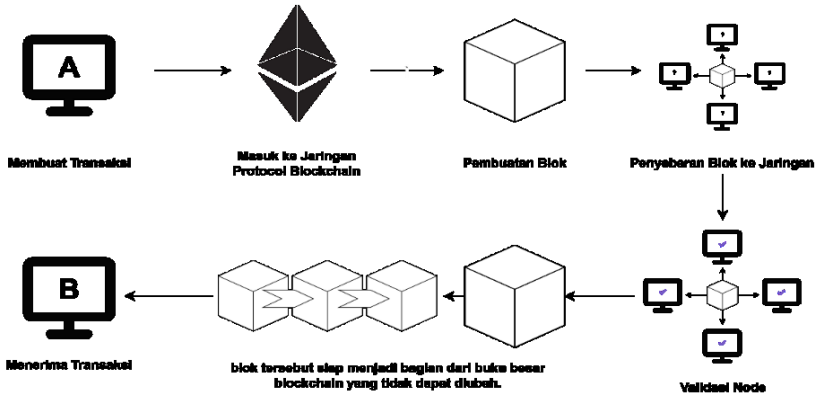
Setiap pengujian dilakukan dengan skenario berbeda untuk mengidentifikasi potensi masalah dan memastikan semua fitur berfungsi dengan baik. Hasil pengujian ini digunakan sebagai dasar untuk evaluasi sistem sebelum deployment.

Selain itu, dilakukan juga pengamatan terhadap gas fee pada setiap jenis transaksi sebagai bagian dari analisis efisiensi sistem. Estimasi biaya transaksi ini diperoleh menggunakan Hardhat Gas Reporter pada jaringan lokal, dan tetap diuji melalui pendekatan blackbox untuk mengetahui seberapa besar beban biaya yang ditanggung pengguna dalam menjalankan fitur-fitur utama sistem.

III. HASIL DAN PEMBAHASAN

A. Cryptocurrency

Sistem crowdfunding dalam penelitian ini dibangun menggunakan teknologi blockchain, di mana seluruh aktivitas penggalangan dana dilakukan dengan mata uang kripto. Blockchain yang digunakan berbasis Ethereum, sehingga transaksi menggunakan Ether (ETH). Karena bersifat desentralisasi, transaksi berlangsung secara peer-to-peer tanpa memerlukan perantara seperti bank, berbeda dengan mata uang fiat yang membutuhkan pihak ketiga dalam proses transaksi.



Gambar 8 Alur Diagram Cryptocurrency

B. Smart Contract

Smart contract digunakan sebagai logika inti dalam sistem crowdfunding berbasis blockchain ini. Semua proses utama, seperti pembuatan kampanye, donasi, dan penarikan dana, dijalankan secara otomatis tanpa pihak ketiga. Detail implementasi dijelaskan pada subbab berikut.

1) Desain Smart Contract

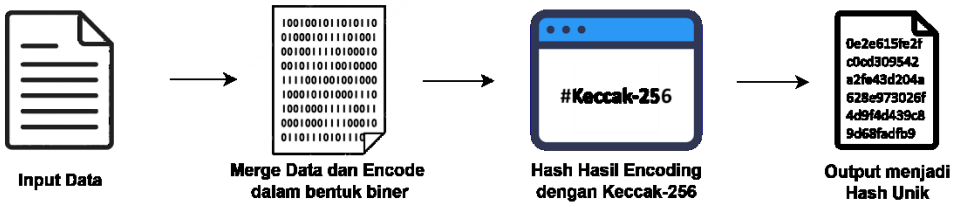
Smart Contract dikembangkan menggunakan Solidity dan berfungsi untuk mengatur seluruh proses crowdfunding, termasuk pembuatan kampanye, penyumbangan dana, dan penarikan dana. Smart Contract memastikan bahwa setiap transaksi mengikuti aturan yang telah ditentukan tanpa perlu perantara. Tabel berikut merinci fungsi-fungsi utama dalam smart contract yang diimplementasikan.

Tabel 1 Desain Smart Contract

Komponen	Tipe Data	Deskripsi
Penggalang	Struct	menyimpan informasi penggalangan dana, seperti nama, deskripsi, target, dan status.
IDonatur	Struct	menyimpan informasi donatur, seperti alamat donatur dan jumlah donasi.
owner	address	Alamat pemilik kontrak
GalangData	mapping(bytes32 => Penggalang)	Menyimpan data penggalangan dana berdasarkan ID unik (hash Keccak-256)
galangIds	bytes32[]	Array untuk menyimpan ID penggalangan dana yang telah dibuat.
GalangDatalength	uint256	Menghitung jumlah total penggalangan dana yang telah dibuat.
donatur	mapping(bytes32 => IDonatur[])	Menyimpan daftar donatur untuk setiap penggalangan dana berdasarkan ID unik.
createGalang	public function, payable	Membuat penggalangan dana baru dengan parameter seperti nama, deskripsi, target, dan deadline.
deposit	public function, payable	Menyumbang dana ke penggalangan yang ditentukan berdasarkan ID, dengan validasi target dan pengembalian jika melampaui target
withdraw	public function	Penarikan dana oleh penggalang setelah tenggat waktu berakhir.

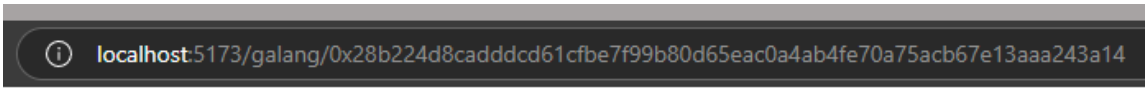
FraudDonation	public function, onlyOwner	Menandai penggalangan dana sebagai penipuan dan mengembalikan semua dana ke donatur (hanya dapat dilakukan oleh pemilik kontrak).
getGalangData	public function, view	Mengembalikan semua data penggalangan dana yang telah dibuat.
getDonatur	public function, view	Mengembalikan daftar donatur untuk penggalangan dana tertentu berdasarkan ID.
GalangCreated	event	log emit saat penggalangan baru dibuat
Deposited	event	log emit saat ada donasi masuk
Withdrawn	event	log emit saat dana berhasil ditarik

2) Peran Keccak-256 untuk Integrasi Data



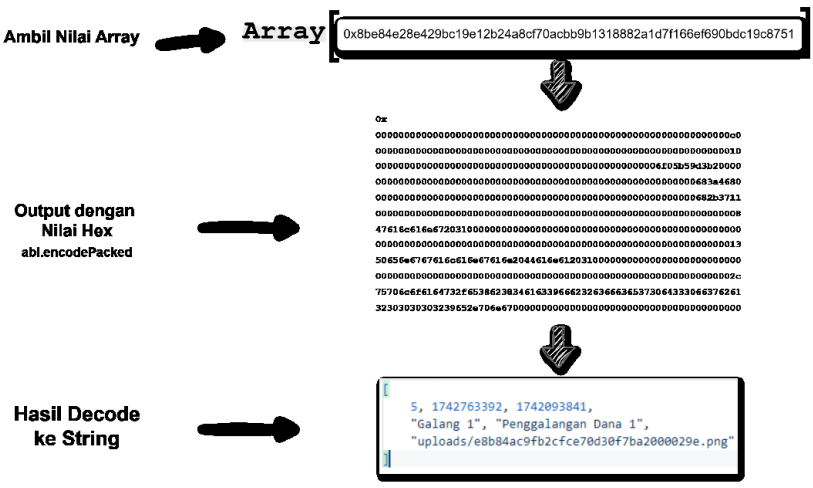
Gambar 9 Proses generate ID dengan Keccak-256

Pada Setiap kampanye crowdfunding memiliki ID unik yang dihasilkan menggunakan algoritma Keccak-256. ID ini dibuat dengan melakukan hashing pada kombinasi nama, deskripsi, gambar, target dana, dan batas waktu kampanye. Dengan peran algoritma Keccak-256, setiap kampanye memiliki identitas unik tanpa risiko duplikasi.



Gambar 10 Hash Keccak-256 sebagai endpoint URL

ID hasil hashing ini juga digunakan sebagai bagian dari endpoint URL untuk mengambil data spesifik dari smart contract. Sistem frontend akan memanggil data kampanye berdasarkan ID. Kemudian endpoint memungkinkan setiap kampanye diakses secara langsung melalui jalur data yang unik.



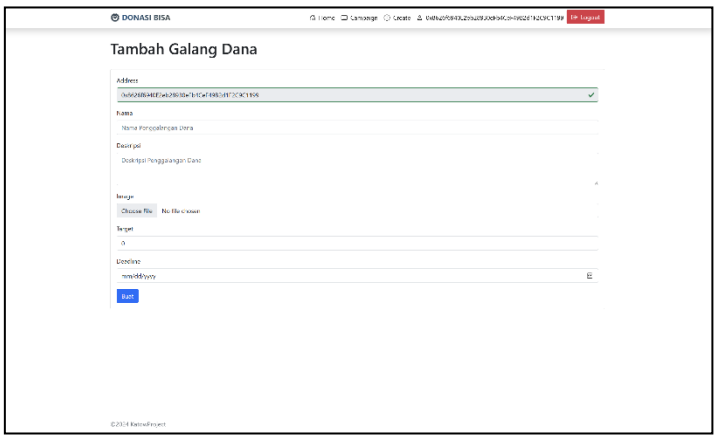
Gambar 11 Proses Ambil Data di Smart Contract

Setelah hash ID terbentuk, data kampanye disimpan di dalam mapping smart contract dengan hash tersebut sebagai key. Pada proses retrieval data, hash ID inilah yang digunakan sebagai parameter untuk mendapatkan detail kampanye secara langsung dari blockchain. Dengan cara ini, sistem dapat memastikan bahwa setiap entri data benar-benar unik dan tidak bisa digandakan, karena input yang sama akan menghasilkan hash yang sama, dan percobaan duplikasi akan ditolak oleh smart contract

ISSN: 2715-2766
Vol. 7 No. 1, Januari 2026

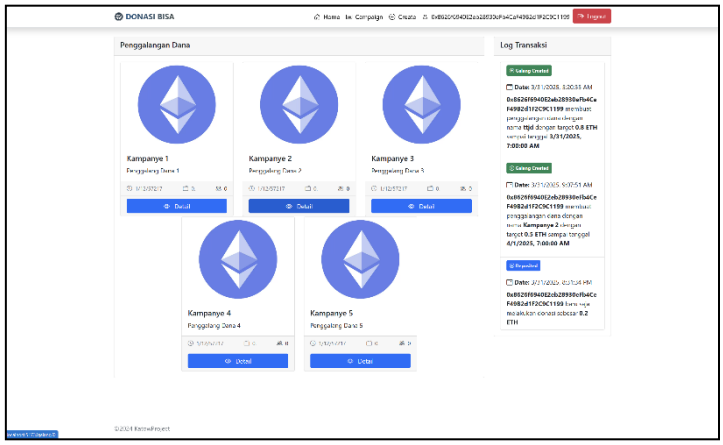
C. Tampilan Aplikasi

Bagian ini berisi tampilan antarmuka aplikasi yang digunakan oleh pengguna. Screenshot dari halaman utama, formulir pembuatan kampanye, halaman transaksi, dan riwayat transaksi ditampilkan untuk memberikan gambaran visual tentang bagaimana pengguna berinteraksi dengan sistem.



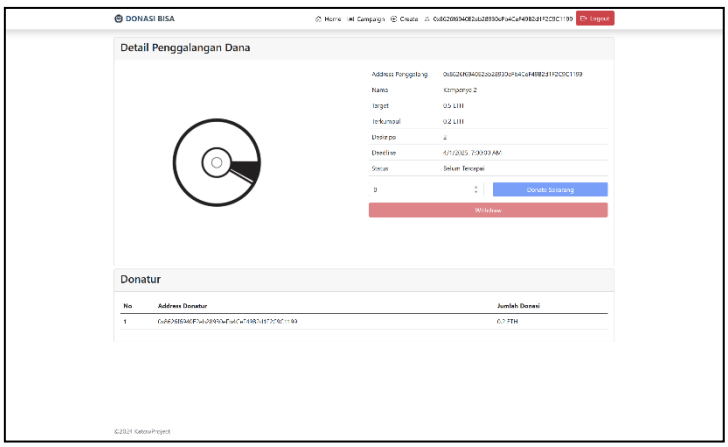
Gambar 12 Tampilan Aplikasi Tambah Galang Dana

Pada Gambar 11, tampilan aplikasi pada fitur Tambah Galang menampilkan beberapa komponen input, yaitu alamat dompet (wallet address) pengguna, nama penggalang dana, deskripsi kampanye, gambar pendukung, target dana, dan batas waktu (deadline). Di bagian akhir, terdapat tombol Submit yang digunakan untuk membuat kampanye crowdfunding baru.



Gambar 13 Tampilan Aplikasi List Penggalang Dana

Pada Gambar 12, tampilan daftar kampanye menampilkan beberapa penggalangan dana yang sedang berlangsung. Setiap elemen kampanye menampilkan informasi berupa judul, deskripsi singkat, target dana, jumlah donasi yang telah terkumpul, serta batas waktu penggalangan. Di sisi kiri layar, terdapat sidebar yang menampilkan log transaksi terbaru dari seluruh aktivitas kampanye yang tercatat di sistem.



Gambar 14 Tampilan Aplikasi Detail Penggalangan Dana

Pada Gambar 13, tampilan detail penggalangan dana menampilkan informasi lengkap seperti alamat penggalang, target dana, jumlah dana yang telah terkumpul, deskripsi kampanye, batas waktu (deadline), serta status kampanye. Tersedia pula input donasi bagi pengguna yang ingin berkontribusi. Selain itu, terdapat tombol berwarna merah yang hanya dapat diakses oleh pemilik kampanye untuk melakukan penarikan dana (withdraw), dan tombol ini akan aktif jika target dana telah tercapai atau batas waktu penggalangan telah terlewati.

D. Pengujian Sistem

Pada tahap pengujian dilakukan terhadap beberapa aspek utama yaitu verifikasi smart contract, keamanan dan keaslian data, dan transparansi sistem. Setiap aspek diuji berdasarkan skenario yang telah ditentukan untuk mengamati apakah sistem memberikan respons yang sesuai. Hasil pengujian akan diberikan dalam bentuk tabel, yang mencakup skenario pengujian, langkah-langkah yang dilakukan, serta hasil yang diperoleh.

1) Verifikasi Smart Contract

Tabel 2 Pengujian Verifikasi Smart Contract

No	Skenario	Pengujian	Ekspetasi	Hasil
1	Pembuatan Crowdfunding	Input data kampanye → Submit Form → konfirmasi transaksi metamask	Kampanye berhasil dibuat dan muncul di list penggalangan dana	Sesuai
2	Donasi ke kampanye	Pilih Kampanye → input jumlah donasi → konfirmasi transaksi metamask	Saldo kampanye bertambah	Sesuai
3	Penarikan dana oleh pemilik kampanye	Ajukan penarikan → validasi syarat penarikan	Jika validasi penarikan seperti jumlah donasi melebihi target atau sudah melewati batas waktu valid, dana masuk ke pemilik	Sesuai
4	Donasi dengan Saldo tidak cukup	Pilih Kampanye → Input jumlah donasi → konfirmasi transaksi metamask	Muncul alert donasi ditolak karna saldo tidak cukup	Sesuai
5	Penarikan dana pada saat kampanye berjalan	Ajukan penarikan → validasi syarat penarikan	Muncul alert penarikan ditolak karna kampanye belum selesai	Sesuai
6	Set Fraud Kampanye	Pilih Kampanye → Ubah status ke fraud	Kampanye tidak dapat diakses lagi dan status menjadi fraud	Sesuai

2) Keamanan dan Keaslian Data

Tabel 3 Pengujian Keamanan dan Keaslian Data

No	Skenario	Pengujian	Ekspetasi	Hasil
1	Pembuatan Kampanye dan Pembentukan Hash	Buat form kampanye → isi data → klik submit → konfirmasi transaksi metamask	Hash Kampanye terbantuk dan tersimpan sebagai index array mapping di blockchain	Sesuai
2	Duplikasi Kampanye dengan Data Sama	Buat dua kampanye dengan data yang sama → Sistem membandingkan hash	Kampanye ditolak karna terdapat ID Duplikat	Sesuai

3	Variasi Input Menghasilkan Hash Berbeda	Buat Kampanye dengan data sedikit berbeda → klik submit → konfirmasi transaksi metamask	Hash berbeda (efek *avalanche*), tidak ada tabrakan	Sesuai

3) Transparasi

Tabel 4 Pengujian Transparasi Data

No	Skenario	Pengujian	Ekspetasi	Hasil
1	Cek list donatur	Buka halaman list kampanye → klik detail penggalangan dana → bandingkan dengan data blockchain	Daftar donasi muncul sesuai data di blockchain	Sesuai
2	Cek log semua aktivitas pengguna	Buka halaman utama → pilih bagian log aktivitas	Semua aktivitas teraudit dengan lengkap sesuai dengan data di blockchain	Sesuai

E. Gas Fee setiap Transaksi

Setelah tahap pengujian, setiap transaksi memiliki *gas fee*. Pada tahap ini dilakukan untuk mengetahui estimasi biaya transaksi yang dibutuhkan pada setiap aksi yang dilakukan di dalam sistem smart contract. Setiap transaksi dalam sistem, seperti pembuatan kampanye, donasi, penarikan dana, hingga penandaan kampanye penipuan, akan mengonsumsi sejumlah gas yang dibayarkan oleh pengguna kepada jaringan. Biaya ini bervariasi tergantung pada kompleksitas fungsi smart contract yang dijalankan. Berdasarkan hasil pengujian yang dilakukan di jaringan uji (*local Hardhat network*) menggunakan *Hardhat Gas Reporter*, sehingga hasilnya bersifat simulatif namun dapat memberikan gambaran tentang beban biaya transaksi pada sistem. berikut adalah rata-rata penggunaan gas untuk setiap jenis transaksi:

Tabel 5 Estimasi *Gas Fee* pada setiap transaksi

No	Jenis Transaksi	Fungsi Smart Contract	Biaya Gas (*Gas Unit*)	Perkiraan Biaya (ETH)	Perkiraan Biaya (Rp)
1	Pembuatan Kampanye	createGalang(...)	285,204	0.000936 ETH	Rp 24,513.40
2	Donasi ke Kampanye	deposit(...)	142,452	0.000454 ETH	Rp 12,592.50
3	Penarikan Dana	withdraw(...)	60,178	0.00015 ETH	Rp 4,411.76
4	Menandai Kampanye Penipuan	setFraud(...)	61,000	0.00017 ETH	Rp 4,915.50

IV. KESIMPULAN DAN SARAN

Penelitian ini telah berhasil mengembangkan sistem *crowdfunding* berbasis teknologi *blockchain* menggunakan *smart contract Ethereum*. Sistem yang dirancang mampu menangani proses utama seperti pembuatan kampanye, penerimaan donasi, penarikan dana oleh penggalang, serta penandaan kampanye *fraud*. Semua proses tersebut berjalan sesuai dengan ketentuan yang ditetapkan di dalam *smart contract* dan telah diuji menggunakan *metode blackbox* untuk memastikan fungsionalitas dari sudut pandang pengguna.

Keamanan dan integritas data dijaga melalui penerapan algoritma *Keccak-256*, yang digunakan untuk menghasilkan ID unik setiap kampanye berdasarkan input data. Hasil pengujian menunjukkan bahwa algoritma ini mampu mencegah duplikasi dan memastikan setiap kampanye memiliki identitas yang berbeda meskipun perbedaannya kecil. Selain itu, transparansi sistem tercapai melalui pencatatan transaksi secara terbuka di blockchain, memungkinkan pengguna untuk memverifikasi informasi kampanye secara langsung.

Terakhir pada *gas fee* untuk setiap transaksi berada dalam batas yang wajar. Meskipun demikian, sistem ini masih memiliki keterbatasan, seperti penyimpanan gambar yang dilakukan secara lokal dan belum adanya validasi sistem secara langsung melalui *feedback* pengguna.

PENGAKUAN

Naskah ilmiah ini adalah sebagian dari penelitian Tugas Akhir milik M. Naufal Faqih, dengan judul “Implementasi Blockchain Ethereum Smart Contract Pada Aplikasi Crowdfnding Berbasis Website dengan Keamanan Algoritma Keccak-256” yang dibimbing oleh Deden Wahiddin dan Kiki Ahmad Baihaqi

DAFTAR PUSTAKA

[1] S. Hidayanto, A. Z. Tofani, A. P. Pratiwi, S. Rahmah, D. Alfurqaan, and P. Christian, "Aksi Sosial Di Internet: Peran Social Media Influencer Sebagai Aktor Dalam Crowdfunding Di Media Sosial," *J. Komunikasi, Masy. Dan Keamanan*, vol. 4, no. 1, pp. 13–29, Mar. 2022, doi: 10.31599/komaskam.v4i1.1134.

[2] V. Butticè and S. Vismara, "Inclusive digital finance: the industry of equity crowdfunding," *J. Technol. Transf.*, vol. 47, no. 4, pp. 1224–1241, Aug. 2022, doi: 10.1007/s10961-021-09875-0.

[3] P. A. Setyaningrum, "Pengaruh Inovasi Crowdfunding, Technology Acceptance Model, dan Kepercayaan Terhadap Keputusan Berdonasi Secara Online Pada Platform Crowdfunding," Universitas Islam Indonesia, 2021. [Online]. Available: http://dspace.uii.ac.id/123456789/43960

[4] A. W. Asshidiq, "Penerapan Prinsip Keterbukaan Dalam Securities Crowdfunding Sebagai Upaya Melindungi Investor Dari Informasi Yang Menyesatkan," Universitas Islam Indonesia, 2023. [Online]. Available: dspace.uii.ac.id/123456789/47619

[5] D. Irawan, A. A. Puspitasari, S. W. W. Astuti, and A. Widyastuti, "Persepsi Keamanan, Kepercayaan, dan Akuntabilitas Perusahaan Terhadap Niat Berdonasi Melalui Fintech Crowdfunding," *ISOQUANT J. Ekon. Manaj. dan Akunt.*, vol. 6, no. 1, pp. 73–89, Apr. 2022, doi: 10.24269/iso.v6i1.1035.

[6] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, p. 100067, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.

[7] J. Karamachoski, N. Marina, and P. Taskov, "Blockchain-Based Application for Certification Management," *Teh. Glas.*, vol. 14, no. 4, pp. 488–492, Dec. 2020, doi: 10.31803/tg-20200811113729.

[8] S. Müller, "Ascon-Keccak AEAD Algorithm (Cryptology ePrint Archive, Paper 2024/858)," 2024. [Online]. Available: https://ia.cr/2024/858

[9] F. Aprialim, Adnan, and A. W. Paundu, "Penerapan Blockchain dengan Integrasi Smart Contract pada Sistem Crowdfunding," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 148–154, Feb. 2021, doi: 10.29207/resti.v5i1.2613.

[10] H. S. Kartiko, T. Rismawan, and I. Ruslianto, "Implementasi IPFS untuk Mengurangi Gas Fee Smart Contract Ethereum pada Aplikasi Penggalangan Dana," *J. Edukasi dan Penelit. Inform.*, vol. 9, no. 2, p. 195, Aug. 2023, doi: 10.26418/jp.v9i2.61876.

[11] A. M. Mabruroh, F. Dewanta, and A. A. Wardana, "Implementasi Ethereum Blockchain dan Smart Contract Pada Jaringan Smart Energy Meter," *MULTINETICS*, vol. 7, no. 1, pp. 82–91, Oct. 2021, doi: 10.32722/multinetics.v7i1.4122.

[12] H. Sa'diyah and Yunita Ardilla, "Pengaruh Reputasi Lembaga dan Financial Technology Crowdfunding Terhadap Keputusan Berdonasi di Dompet Al-Qur'an Indonesia," *J. Islam. Manag.*, vol. 4, no. 1, pp. 51–62, Jan. 2024, doi: 10.15642/jim.v4i1.1579.

[13] F. N. Rohmah, "Indonesia Tetap Paling Dermawan, Meski Dana Sering Diselewengkan." Accessed: Dec. 21, 2024. [Online]. Available: https://tirto.id/indonesia-tetap-negara-dermawan-walau-banyak-kasus-penyelewengan-gXDC

[14] B. Yasar, "The new investment landscape: Equity crowdfunding," *Cent. Bank Rev.*, vol. 21, no. 1, pp. 1–16, Mar. 2021, doi: 10.1016/j.cbrev.2021.01.001.

[15] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions," *Electronics*, vol. 13, no. 17, p. 3568, Sep. 2024, doi: 10.3390/electronics13173568.

[16] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, and A. Kerrouche, "Implementation of Blockchain Consensus Algorithm on Embedded Architecture," *Secur. Commun. Networks*, vol. 2021, pp. 1–11, Apr. 2021, doi: 10.1155/2021/9918697.

[17] Y. Wang, C.-H. Hsieh, and C. Li, "Research and Analysis on the Distributed Database of Blockchain and Non- Blockchain," in *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, IEEE, Apr. 2020, pp. 307–313. doi: 10.1109/ICCCBDA49378.2020.9095589.

[18] J. Scherer and an O. M. C. Safari, *Hands-On JavaScript High Performance*. Packt Publishing Ltd, 2020.

[19] N. Foundation, "Hardhat Documentation." [Online]. Available: https://hardhat.org/

[20] A. Kumar and S. Kumar, "Secured Ethereum Transactions using Smart Contracts & Solidity," *YMER Digit.*, vol. 21, no. 05, pp. 432–442, May 2022, doi: 10.37896/YMER21.05/47.

[21] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger (Paris Version 71beac3)," 2024. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[22] N. Nguyen, "Development & deployment of a web server as an executable with Node.js, Express.js and Vercel/pkg," no. January, pp. 1–56, 2022.

[23] V. R. Kurada and P. K. Baruah, "Blockchain Enabled, Collaborative Platform for Ai as a Service," *ICTACT J. Soft Comput.*, vol. 13, no. 3, pp. 2909–2916, Apr. 2023, doi: 10.21917/ijsc.2023.0411.

[24] A. Dolmeta, M. Martina, and G. Masera, "Comparative Study of Keccak SHA-3 Implementations," *Cryptography*, vol. 7, no. 4, p. 60, Nov. 2023, doi: 10.3390/cryptography7040060.

[25] Supriyono, "Software Testing with the approach of Blackbox Testing on the Academic Information System," *IJISTECH*

(International J. Inf. Syst. Technol., vol. 3, no. 2, pp. 227–233, 2020, doi: 10.30645/ijistech.v3i2.54.

[26] P. A. D. A. Santi, R. Afwani, M. A. Albar, S. E. Anjarwani, and A. Z. Mardiansyah, "Black Box Testing with Equivalence Partitioning and Boundary Value Analysis Methods (Study Case: Academic Information System of Mataram University)," in *Proceedings of the First Mandalika International Multi-Conference on Science and Engineering 2022, MIMSE 2022 (Informatics and Computer Science)*, I. G. P. S. Wijaya, J. Hwang, A. M. Widodo, and B. Irawan, Eds., Dordrecht: Atlantis Press International BV, 2022, pp. 207–219. doi: 10.2991/978-94-6463-084-8_19.