SISTEM VERIFIKASI DOKUMEN HASIL INVESTIGASI FORENSIK DIGITAL BERBASIS TEKNOLOGI *BLOCKCHAIN*

Dzaky Ahmad Badawi
Program Studi Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia
Yogyakarta, Indonesia
15523205@students.uii.ac.id

***Abstract*—Penggunaan dan perkembangan teknologi, setidaknya sudah banyak manfaat yang bisa diambil dari penggunaan teknologi tersebut. Meskipun juga tidak jarang ditemukan tindak kejahatan yang memanfaatkan pengunaan teknologi atau yang disebut dengan *cybercrime*. Para ahli dalam forensik, khususnya pada bidang forensik digital tentunya sudah memiliki SOP untuk penanganan dalam penyelidikan kasus kejahatan digital, sehingga dapat memudahkan proses penyelidikan dan menghasilkan hasil laporan investigasi forensik digital. Berkaitan dengan pelaporan dan verifikasi dokumen hasil investigasi forensic digital yang harus terjaga integritas datanya, maka kehadiran teknologi *Blockchain* tentunya memiliki potensi yang besar apabila diterapkan pada sistem informasi maupun aplikasi, karena mendukung pencatatan setiap data transaksi dan mengutamakan integritas data. Untuk menjamin integritas data dokumen tersebut, maka penulis membangun sebuah sistem verifikasi dokumen hasil investigasi forensik digital yang menerapkan teknologi *Blockchain* pada *platform* Ethereum. Adapun tujuan penelitian ini adalah penulis menghasilkan rancangan arsitektur sistem yang terintegrasi dengan *Blockchain* Ethereum serta membangun sistem verifikasi dokumen investigasi forensik digital berbasis *Blockchain* Ethereum yang dapat digunakan oleh pihak penyidik untuk mengirimkan dokumen laporan investigasinya, yang kemudian supaya dapat diperiksa oleh pihak pemeriksa, sehingga dengan adanya sistem yang dibangun, diharapkan dapat menjaga keaslian data yang dibuktikan dengan bukti *receipt transaksi* yang disimpan pada *Blockchain*.**

Kata Kunci—Forensik digital, *Blockchain*, Ethereum, *cybercrime*

I. PENDAHULUAN

Penerapan teknologi informasi pada masa kini dapat dikatakan telah banyak memiliki peran penting dalam berbagai bidang kehidupan. Namun dengan perkembangan teknologi informasi terlebih dengan adanya *internet* yang terus berlanjut, dapat dikatakan telah menciptakan dunia baru yang disebut dengan *cyberspace* (dunia maya). Penggunaan teknologi informasi khususnya *internet* tentu memiliki dampak positif yang membantu akan kebutuhan penggunanya, baik secara individu maupun organisasi. Akan tetapi juga terdapat berbagai dampak negatif dari penggunaan teknologi tersebut, seperti salah satunya adalah *cybercrime* (kejahatan siber). *Cybercrime* adalah semua jenis pemakaian jaringan komputer untuk tujuan kriminal dengan penyalahgunaan kemudahan teknologi digital [1]. Pada ranah kejahatan komputer ini sudah terdapat upaya atau cara penanganan dalam mengungkap kasus-kasus yang berkaitan dengan *cybercrime* tersebut. Adapun upaya yang bisa dilakukan adalah dengan menggunakan pendekatan metode saintifik yang dikenal dengan sebutan *digital forensic* atau forensik digital. Pengertian forensik digital merupakan ilmu dan metode yang digunakan di dalam perlindungan, pengumpulan, identifikasi, analisis, dokumentasi, dan presentasi barang bukti digital dengan tujuan untuk memfasilitasi atau membuat kemajuan dalam proses rekonstruksi kejadian kriminal [11], dari pengertian tersebut diketahui bahwa forensik digital dapat membantu proses pengungkapan sebuah kasus yang berkaitan dengan tindak kriminal yang melibatkan teknologi. Sedangkan dalam proses pengungkapan kasus pada ranah *cybercrime* ini dilakukan oleh pihak khusus yang terlibat, salah satunya yaitu ahli forensik digital.

Dalam penanganan sebuah kasus kejahatan siber, seorang ahli forensik khususnya pada bidang forensik digital tentunya sudah memiliki prosedur standar terkait dengan proses penanganan kasus. Adapun proses atau SOP terkait penanganan kasus kejahatan siber sudah diatur dalam dokumen SNI 27037:2014 yang diawali dengan melakukan identifikasi kasus, pengumpulan barang bukti, melakukan pemeriksaan atau akuisisi, dan melakukan preservasi bukti digital [3]. Berdasarkan prosedur tersebut, diharapkan dapat membantu penyidik dalam menangani proses penyelidikan dan dapat menjaga integritas data dari hasil temuan dan akuisisi barang bukti, dan hasil dari semua temuan dalam proses analisis forensik disusun dalam sebuah dokumen laporan investigasi forensik digital. Dokumen ini kemudian akan disampaikan kepada pihak berwajib seperti kepolisian dan juga dapat digunakan sebagai penjelasan terkait kasus yang ditangani. Yang selanjutnya akan dijadikan sebagai alat bukti pada proses peradilan untuk mendukung pengungkapan kasus tersebut.

Namun sebelum dapat diserahkan kepada pihak yang berwajib, tentu saja laporan investigasi forensik digital yang akan diserahkan harus melewati proses verifikasi dahulu dan juga hasil dari sebuah temuan tentu tidak dapat secara langsung menjelaskan kronologi kejahatan, apalagi menjelaskan tersangka dan membuktikan sebuah tindak kejahatan. Sebab sebuah bukti harus dapat memenuhi asas ***In criminalibus, probationes bedent esse luce clariores***, dimana bukti harus lebih terang dari cahaya atau bukti yang diberikan dan diperlihatkan dalam persidangan harus jelas. Dengan asas ini, maka laporan investigasi tak terkecuali investigasi forensik digital mensyaratkan jelasnya temuan dan keterkaitannya dengan kasus. Sesuai dengan ketentuan yang berlaku dalam Pasal 184 ayat (1) mengenai alat bukti yang sah yang dimaksud adalah keterangan ahli, keterangan saksi, surat, petunjuk, dan keterangan terdakwa [12], sehingga dari pernyataan pada Pasal 184 ayat (1), maka sebuah laporan dokumen investigasi forensik digital tersebut, sangat diperlukan selama proses penyelidikan dan pemeriksaan yang kemudian dapat mendukung dan dijadikan sebagai alat bukti yang sah di pengadilan. Pentingnya sebuah laporan dokumen investigasi forensik ini dalam membuktikan sebuah tindak kejahatan mengharuskan validitas dan integritas dari laporan tersebut, dengan mengutamakan aspek kerahasiaan dan keamanan dalam proses preservasinya. Karena dokumen ini bermula dari penyidik ke ahli forensik digital. Maka dari hal tersebut perlu dijadikan perhatian supaya sistem yang akan diterapkan dapat mempermudah proses verifikasi laporan dokumen investigasi dan terjamin integritasnya.

Supaya dapat mencapai tujuan tersebut, maka terdapat sebuah teknologi yang disebut dengan Blockchain yang dapat digunakan sebagai tempat penyimpanan data dan memiliki tingkat keamanan yang tinggi dalam menjaga integritas data yang disimpan. Digagas oleh Satoshi Nakamoto, pengertian dari *Blockchain* adalah sistem yang memiliki arsitektur yang mirip dengan rantaian blok, di mana tiap blok memuat data atau menyimpan data transaksi yang dikelolah oleh semua pengguna tanpa adanya pihak ketiga atau pengawasan yang terpusat [10], sehingga dengan adanya teknologi tersebut maka, *Blockchain* tentunya memiliki potensi yang besar apabila diterapkan pada sistem informasi maupun aplikasi seperti dalam pengamanan integritas laporan forensik digital dapat terjamin, karena mendukung pencatatan setiap transaksi atau pengiriman data maupun informasi tanpa adanya penggunaan pihak ketiga, bersifat kekal, dan sangat mengutamakan informasi yang valid [5]. Oleh karena itu penulis memiliki usulan untuk merancang sistem verifikasi dokumen elektronik yang berupa dokumen laporan hasil investigasi forensik digital. Sistem ini dibangun dengan memanfaatkan teknologi *Blockchain* yang menerapkan layanan jaringan Ethereum, supaya dokumen elektronik yang berupa laporan investigasi forensik digital dapat membantu penyidik mengirimkan dokumennya kepada ahli forensik digital. Demikian dengan adanya sistem ini, proses pengelolaan dokumen laporan investigasi forensik digital, pemeriksaan atau verifikasi dokumen dapat dilakukan secara mudah, aman, dan terjamin keasliannya.

II. LANDASAN TEORI

A. Verifikasi Dokumen Investigasi Forensik Digital

Merujuk pada dokumen SNI ISO 9000:2005 mengenai sistem manajemen mutu pada poin 3.8.4, definisi verifikasi adalah konfirmasi, melalui penyediaan bukti objektif, bahwa persyaratan yang ditentukan telah dipenuhi. Sedangkan sistem verifikasi dokumen hasil investigasi forensik digital merupakan sistem yang mengelola laporan terkait dengan dokumen investigasi forensik digital yang telah dibuat dan dikirimkan oleh pihak penyidik kepada pemeriksa atau ahli forensik digital dalam membantu proses verifikasi laporan [2].

Karena laporan yang ditulis dan dikirimkan tersebut juga bersifat resmi dan juga mengikuti pedoman penulisan yang disesuaikan untuk umum supaya dapat dimengerti dan juga mengandung penulisan dengan bahasa hukum untuk menjelaskan pembuktian. Maka tentu saja terdapat panduan atau struktur laporan dokumen hasil investigasi forensik digital yang baik dan juga harus memuat beberapa hal seperti; halaman judul laporan, daftar isi, ringkasan investigasi, tujuan investigasi, analisis barang bukti, metodologi atau tahapan investigasi, temuan-temuan yang berkaitan, alur investigasi, kesimpulan, bagian tanda tangan, dan lampiran [7].

B. Teknologi *Blockchain*

Blockchain merupakan *ledger* atau buku besar digital yang terdistribusi dari transaksi yang ditandatangani secara kriptografis dan dikelompokkan ke dalam blok. Setiap blok dihubungkan secara kriptografis dengan *hash* blok sebelumnya setelah dilakukan validasi dan menjalani keputusan konsensus. Ketika blok baru berhasil dibuat dari proses *mining*, maka data pada blok sebelumnya akan hampir mustahil untuk diubah atau dimanipulasi [13].

Berdasarkan jenis *Blockchain* terdapat tiga jenis *Blockchain* yaitu:

1) *Public Blockchain*

Merupakan jaringan terdistribusi yang besar karena memiliki sifat publik yang berarti terbuka kepada semua orang yang berpartisipasi dan memiliki kode yang bersifat *open-source*, sehingga para komunitas dapat berdistribusi.

2) *Private Blockchain*

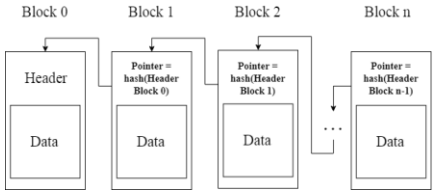
Private Blockchain adalah jenis *Blockchain* yang bersifat tertutup dan bertujuan untuk melakukan pertukaran informasi secara internal saja, sehingga pihak-pihak yang tidak bergabung, tentu saja tidak dapat melihat proses-proses apa saja yang dilakukan pada *Blockchain* tersebut.

3) *Semi-Private Blockchain*

Merupakan jenis *Blockchain* yang memberikan hak akses kepada siapa saja yang berhak menggunakannya dan memiliki source code yang tertutup. Mirip seperti dengan *private Blockchain*, namun untuk penyimpanan data yang dikirimkan melalui transaksi tetap akan tersimpan pada jaringan *public Blockchain*.

Beberapa contoh kelebihan dari teknologi *Blockchain* yang telah diketahui dari definisi penjelasan sebelumnya yaitu; adanya transparansi atau keterbukaan, bersifat kekal atau tetap, memiliki sistem keamanan yang kuat. Pada proses penyimpanan data atau transaksi pada *Blockchain* akan disimpan dalam bentuk *hash*. Karena selain untuk penyimpanan, fungsi *hash* pada *Blockchain* juga dijadikan sebagai *pointer* atau penghubung antar blok dan digunakan untuk menghasilkan dan memvalidasi blok baru. Sedangkan pada Ethereum juga menggunakan teknik *hashing* yang disebut dengan Keccak256 untuk melakukan *hash* pada setiap transaksi yang terjadi.

Di balik bagaimana cara proses *Blockchain* bekerja. Tentunya terdapat bagian-bagian penting yang terstruktur supaya *Blockchain* dapat digunakan. Struktur dari *Blockchain* tersusun dari banyaknya *block* yang merupakan representasi untuk sebuah daftar transaksi yang sah dan disimpan pada jaringan. Setiap blok memiliki sebuah *hash* kriptografis sebagai *pointer* atau sebagai identitas setiap *block* supaya dapat saling terhubung antara satu dengan yang lainnya [8].



Gambar 1 Diagram Skema *Blockchain*

C. Ethereum

Ethereum pertama kali diperkenalkan pada tahun 2013 oleh salah satu pengembangnya yaitu Vitalik Buterin. Secara definisi Ethereum merupakan salah satu implementasi dari *Blockchain* yang memperkenalkan kemampuan komputasi untuk membangun kembali pemanfaatan *Blockchain* yang hanya dapat melakukan pertukuran mata uang digital menjadi transaksi nilai terutama aset digital antar pengguna melalui bahasa *scripting* [4].

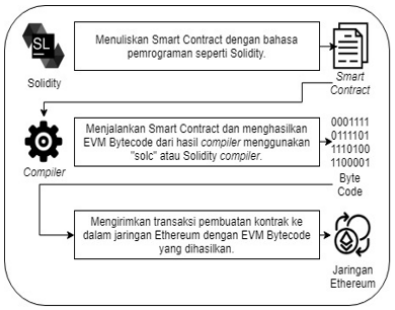
Secara komponennya Ethereum memiliki dua komponen penting yaitu prosesor virtual turing (*Turing-complete virtual processor*) yang disebut sebagai *Ethereum Virtual Machine* (EVM) yang memungkinkan prosesor Turing dalam Ethereum tersebut menjalankan *script* atau bahasa pemrograman yang disebut Solidity untuk membangun aplikasi terdesentralisasi dan juga nilai token yang disebut dengan Ether sebagai satuan *cryptocurrency* yang disahkan oleh jaringan Ethereum supaya pengguna dapat melakukan transaksi atau sebagai kompensasi bagi para *miner* [6].

Akun pada Ethereum merupakan hal yang mendasari bagaimana cara kerja *Blockchain* Ethereum. Akun-akun tersebut digunakan untuk menyimpan dan menelusuri informasi pengguna dalam jaringan. Pada *platform* Ethereum terdapat dua jenis akun [9], yaitu:

1) *User Account* (*externally owned accounts*)
2) *Contract Accounts* (*contract address*)

Selain itu juga pada *platform* Ethereum ini juga menawarkan fitur yang dinamakan dengan *smart contract*. Kontrak cerdas atau s*mart contract* merupakan penerapan dari *platform Blockchain* yang memiliki tujuan untuk menentukan kesepakatan (*consensus*) antara beberapa pihak berdasarkan jenis konsensus yang digunakan dan diaplikasikan dalam bentuk *script* atau kode sebagai logika bisnis yang terkait dalam penggunaan sistem atau aplikasi berbasis teknologi *Blockchain* [8]. Implementasi *smart contract* tentunya dapat dibangun sesuai dengan kebutuhan yang diinginkan dan digunakan secara aktif melalui *platform Blockchain* manapun seperti Ethereum dengan menggunakan bahasa pemrograman yang bernama Solidity.

Solidity merupakan bahasa pemrograman berorientasi obyek yang memiliki tujuan untuk merancang *smart contract* supaya dapat berjalan pada *Ethereum Virtual Machine* (EVM), serta disimpan dalam sebuah file dengan ekstensi (.sol). Segala kode yang dituliskan dalam bahasa pemrograman Solidity akan dikompilasi menggunakan Solidity *compiler* atau biasa disebut dengan "solc" yang menghasilkan bytecode (sekumpulan fungsi yang telah di-*encode*), supaya dapat dijalankan dan dieksekusi pada EVM seperti yang digambarkan pada Gambar 2.

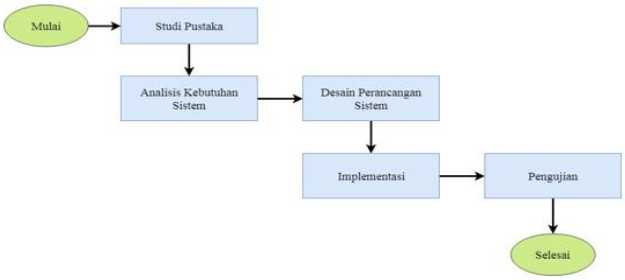


Gambar 2 Proses *Compile* dan *Deploy* Kontrak

Pada proses *encoding* dengan *compiler* supaya menghasilkan Bytecode yang digunakan sebagai referensi fungsi dan kontrak untuk diekseskusi pada EVM. Proses *encoding* tersebut dibantu dengan menggunakan ABI (*Application Binary Interface*) yang merupakan daftar definisi fungsi dalam kontrak dan beberapa argumen yang ditulis dalam format *Javascript Object Notation* (JSON). Daftar fungsi dan argument tersebut diubah dengan *hash* menjadi ABI, kemudian dapat diolah oleh EVM. ABI sangat diperlukan supaya dapat menentukan fungsi mana yang ada pada kontrak untuk dijalankan, serta menjamin fungsi tersebut akan mengembalikan data dalam format yang sudah ditentukan [6].

III. METODOLOGI PENELITIAN

Terkait dengan tahapan penelitian untuk menghasilkan sistem atau aplikasi web verifikasi dokumen investigasi forensik digital berbasis *Blockchain*, maka terdapat tahapan-tahapan yang dilakukan untuk dapat memperoleh hasil dari penelitian ini. Adapun tahapan penelitian tersebut telah digambarkan pada Gambar 3.



Gambar 3 Alur Penelitian

Sesuai dengan Gambar 3, pada tahapan penelitian ini terdapat lima tahapan yang dimulai dengan melakukan studi pustaka melalui berbagai referensi maupun buku yang berkaitan dengan sistem yang akan dikembangkan dan juga teknologi *Blockchain*. Kemudian dilanjutkan tahapan pengembangan sistem yang mirip seperti metodologi pengembangan *waterfall*, dimulai dengan menganalisis kebutuhan sistem, melakukan desain perancangan sistem. Apabila analisis kebutuhan sistem dan desain perancangan sistem sudah ditentukan maka lanjut ke tahap selanjutnya yaitu melakukan implementasi sistem, dan setelahnya dilakukan pengujian terhadap hasil implementasi sistem.

A. Analisis Kebutuhan Sistem

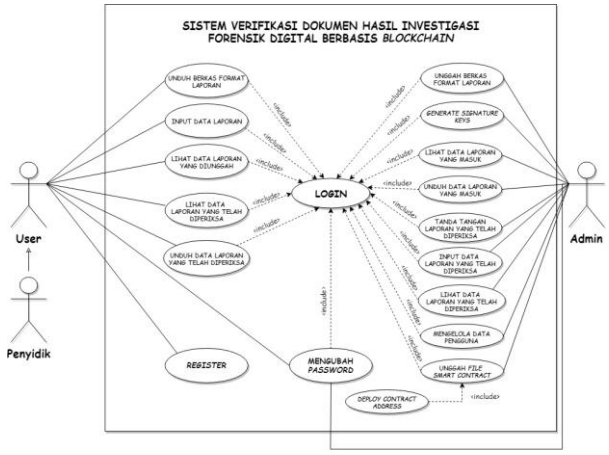
Tujuan dari adanya analisis kebutuhan sistem adalah untuk mengetahui kebutuhan sistem yang nantinya dapat digunakan dalam tahap perancangan sistem. Adapun metode analisis terhadap kebuthan sistem ini diantaranya adalah analisis kebutuhan masukkan (*input*), analisis kebutuhan proses, analisis kebutuhan keluaran (*output*), dan analisis kebutuhan antarmuka (*interface*).

B. Desain Perancangan Sistem

Tujuan dari adanya analisis kebutuhan sistem adalah untuk mengetahui kebutuhan sistem yang nantinya dapat digunakan dalam tahap perancangan sistem. Adapun metode analisis terhadap kebuthan sistem ini diantaranya adalah analisis kebutuhan masukkan (*input*), analisis kebutuhan proses, analisis kebutuhan keluaran (*output*), dan analisis kebutuhan antarmuka (*interface*).

1) *Use Case Diagram*

Use case diagram merupakan suatu model untuk memberikan gambaran sistem secara keseluruhan. Diagram ini menggambarkan semua aktor dan interaksi-interaksi yang terjadi dalam sistem. Dengan adanya use case ini, diharapkan dapat memberikan informasi mengenai fungsionalitas apa saja yang terdapat pada sistem yang dibuat. *Use case diagram* yang terlihat pada Gambar 4, merupakan rancangan *use case* untuk sistem yang akan dibuat.

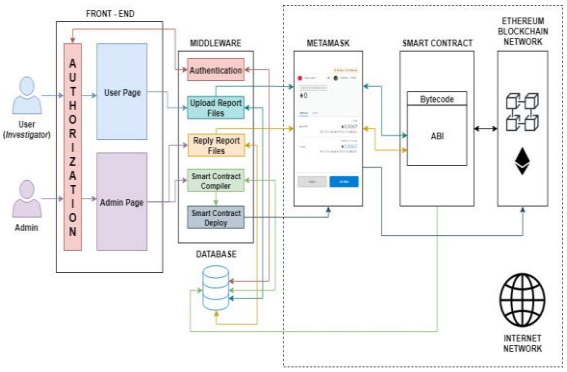


Gambar 4 *Use Case Diagram*

Seperti yang digambarkan pada Gambar 4 terkait diagram *use case* untuk mendeskripsikan jenis fungsionalitas dan aktor yang berperan dalam sistem. Pada diagram use case tersebut terdapat dua jenis aktor yang berperan sebagai Penyidik yang digeneralisasikan sebagai user juga terdapat aktor lain yaitu admin. Sebagai penyidik, aktor tersebut dapat menggunakan fungsionalitas sistem seperti melakukan unduh berkas format laporan, input data laporan, mengunduh laporan yang telah diperiksa, mengubah *password*, dan melihat detail laporan, namun untuk dapat menggunakan fungsionalitas tersebut penyidik harus melakukan proses login terlebih dahulu.

Demikian juga untuk aktor admin, dimana admin dapat menggunakan fungsionalitas sistem seperti mengunggah berkas format laporan, melihat laporan yang masuk, mengelola data pengguna, memeriksa laporan dimana pada fungsionalitas tersebut admin harus melakukan input data hasil pemeriksaan laporan, dan mengatur *smart contract* yang digunakan dengan cara mengunggahnya terlebih dahulu, kemudian admin dapat melakukan *compile smart contract* yang digunakan supaya dapat menghasilkan ABI dan Bytecode yang digunakan untuk menghubungkan fungsi yang ada di dalam sistem supaya dapat terhubung dengan jaringan *Blockchain*, serta untuk menggunakan semua fungsionalitas tersebut, admin juga harus melakukan proses login terlebih dahulu.

2) Rancangan Arsitektur Sistem



Gambar 5 Rancangan Arsitektur Sistem

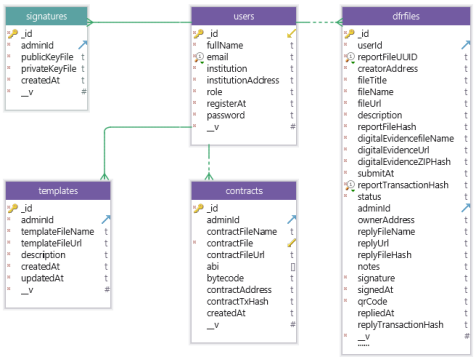
Pada Gambar 5 digambarkan sebuah rancangan arsitektur sistem verifikasi dokumen hasil investigasi forensik digital. Dalam gambar tersebut dapat dilihat adanya interaksi antara komponen-komponen yang saling terhubung, supaya sistem dapat berjalan dengan baik. Adapun komponen-komponen tersebut adalah:

- *Front-end*, merupakan bagian antarmuka pada sistem yang memuat otoriasi atau hak akses pengguna supaya pengguna yang mengakses ke sistem dapat dikenali dan menggunakan fungsi berdasarkan hak aksesnya, apakah pengguna itu admin atau user (investigator).
- *Middleware*, merupakan komponen yang menghubungkan antara komponen front-end dengan komponen lainnya. Dimana pada middleware tersebut terdapat berbagai proses untuk masing-masing fungsi yang akan digunakan.
- *Database* (Basis data), merupakan media penyimpanan data internal untuk menyimpan data laporan, data pengguna untuk melakukan authentication dan authorization, dan juga menyimpan hasil *compile smart contract* dalam bentuk ABI dan Bytecode.
- Metamask, merupakan aplikasi yang dipasang pada browser untuk memudahkan pengguna dalam berinteraksi dengan sistem berbasis *Blockchain* Ethereum. Selain itu juga Metamask dapat digunakan untuk melakukan konfirmasi transaksi seperti yang telah diterapkan pada sistem ini.
- *Smart Contract*, merupakan komponen terpenting dimana pada komponen ini digunakan oleh sistem verifikasi dokumen hasil investigasi forensik digital supaya dapat berinteraksi dengan komponen jaringan *Blockchain* Ethereum.
- Ethereum *Blockchain Network*, merupakan komponen yang berupa salah satu jenis jaringan *Blockchain*. Pada komponen ini semua transaksi dari fungsi unggah laporan, fungsi unggah balasan laporan, maupun melakukan *deploy* terhadap *smart contract* akan diproses dan disimpan pada jaringan Ethereum ini yang menggunakan *testnet* Rinkeby.

3) Rancangan Basis Data

Berikut pada Gambar 6, terdapat visualisasi basis data yang sudah disesuaikan dengan kebutuhan fungsi sistem. Dimana pada sistem verifikasi dokumen hasil investigasi forensik digital ini menggunakan MongoDB (NoSQL) sebagai basis data. Karena basis data yang digunakan berbasis NoSQL, maka tidak ada relasi antara satu tabel dengan tabel lainnya atau pada MongoDB istilah tabel disebut dengan *collections* (koleksi). Pada perancangan basis data, setidaknya terdapat *collections (koleksi*) yang sudah dibuat dengan fungsinya masing-masing:

- Koleksi users, merupakan menyimpan data pengguna yang terdaftar, dan dapat digunakan sebagai referensi untuk disimpan pada koleksi yang lain seperti pada koleksi templates, contracts, sessions, maupun dfrfiles.
- Koleksi *templates*, digunakan oleh pengguna admin dan menjadikan admin sebagai referensi dari atribut "adminId", supaya admin dapat menyimpan data format laporan.
- Koleksi *contracts*, digunakan oleh pengguna admin dan menjadikan admin sebagai referensi dari atribut "adminId", juga digunakan admin supaya dapat menyimpan data yang berhubungan dengan *smart contract*, seperti berkas kontrak, ABI, Bytecode, dan lainnya.
- Koleksi dfrfiles, digunakan oleh pengguna penyidik dan menjadikan pengguna penyidik sebagai referensi ketika penyidik menyimpan data laporan investigasi forensik digital, serta dapat menjadikan pengguna admin sebagai referensi ketika admin menyimpan data balasan laporan investigasi forensik digital kepada penyidik yang bersangkutan.
- Koleksi *signatures*, merupakan tempat penyimpanan data *public key* dan *private key* yang dieksekusi oleh admin supaya dari koleksi ini dapat digunakan ketika admin melakukan penandatanganan digital terhadap dokumen laporan investigasi yang sudah diperiksa.



Gambar 6 Rancangan Basis Data

IV. HASIL DAN PEMBAHASAN

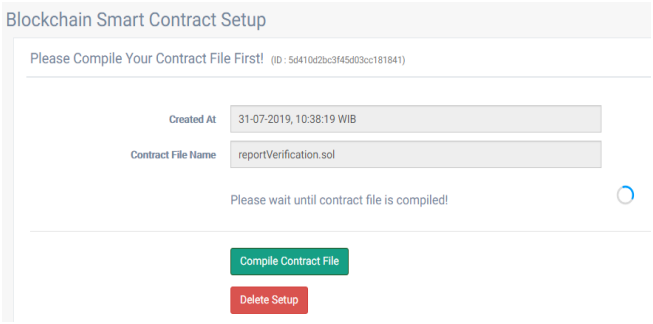
A. Implementasi Sistem dengan *Blokchain*

Pada tahapan ini terdapat penjelasan hasil implementasi sistem yang telah dibangun dan juga sudah terintegrasi dengan *smart contract* maupun jaringan *Blockchain* Ethereum. Berikut merupakan hasil implementasi sistem dengan fitur utama yang telah terhubung dengan *Blockchain* seperti:

1) Fitur Pengaturan *Smart Contract*

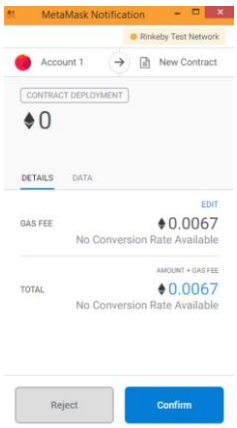
Sebelum sistem dapat digunakan terutama pada fitur-fitur yang terintegrasi dengan fungsi *smart contract* supaya sistem dapat terhubung ke jaringan *Blockchain* Ethereum, maka diperlukan untuk melakukan pengaturan *smart contract* yang akan digunakan. Pengaturan ini hanya dapat dilakukan oleh admin, dengan mengunggah *file smart contract* yang sudah dirancang. Terlebih dahulu kemudian, dilakukan *compile* supaya *smart contract* yang telah diunggah dapat dijalankan untuk menghasilkan ABI dan Bytecode, dari proses tersebut ABI dan Bytecode akan disimpan pada basis data lokal, dan

akan digunakan dalam proses *deploy contract address* dan fitur lainnya seperti untuk mengunggah Laporan Investigasi oleh *User* (Penyidik) dan juga membalas laporan investigasi yang sudah diperiksa oleh admin.



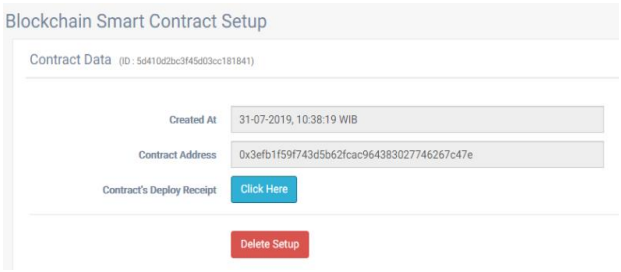
Gambar 7 *Compile* Berkas *Smart Contract*

Pada Gambar 7 admin akan melakukan *compile smart contract* untuk menghasilkan ABI dan Bytecode, yang kemudian dari hasil tersebut akan digunakan untuk melakukan *deploy contract address*. Pada saat admin melakukan proses *deploy contract address*, maka Metamask yang sudah terpasang pada *browser* akan menampilkan konfirmasi untuk melakukan transaksi pembuatan alamat kontrak baru seperti pada Gambar 8. Pada tampilan tersebut admin dapat melihat besaran biaya Ether yang dikeluarkan sebagai kompensasi untuk melakukan transaksi ini. Apabila admin setuju dengan menekan tombol "Confirm" maka proses transaksi akan diproses dan tentunya memerlukan waktu hingga akhir eksekusi transaksi berhasil.



Gambar 8 Konfirmasi *Contract Address* dengan Metamask

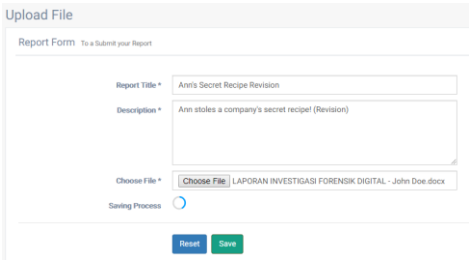
Dan jika proses transaksi ini berhasil, maka pada tampilan sistem akan menyimpan data *contract address* baru yang dihasilkan beserta *receipt* transaksi yang sudah dilakukan. *Contract address* yang sudah berhasil dibuat dan disimpan dapat digunakan sebagai tujuan alamat kontrak untuk fungsi-fungsi yang sudah didefenisikan pada *file smart contract*, seperti pada Gambar 9.



Gambar 9 Hasil *Contract Address* yang Di-*deploy*

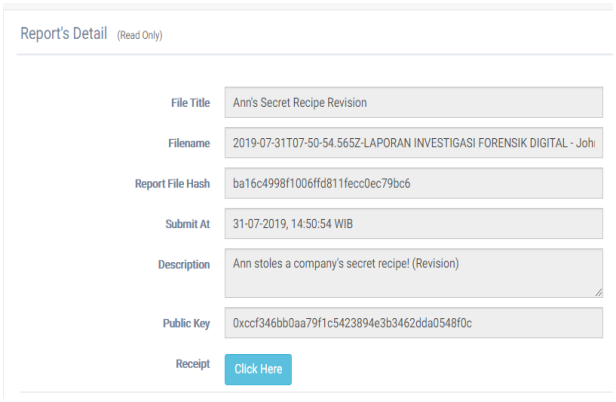
2) Unggah Laporan Investigasi oleh *User* (Penyidik)

Pada fungsi utama yang ditawarkan sistem ini, *user* dapat mengunggah laporan investigasi yang sudah dibuat untuk dilakukan verifikasi. Karena fitur atau *middleware* ini juga menggunakan fungsi dari *smart contract* yang telah dibuat dan supaya dapat menyimpan data-data pendukung pada *Blockchain* untuk menjamin integritas laporan investigasi, maka *user* yang menggunakan diharuskan memiliki akun Metamask dan Ether yang digunakan dalam *testnet* Rinkeby sebagai kompensasi transaksi ketika penggunaan fungsi ini. Ketika *user* akan menggunakan fungsi unggah laporan investigasi, *user* diharuskan mengisi informasi terkait dengan kasus laporan yang telah dibuat (Gambar 10).

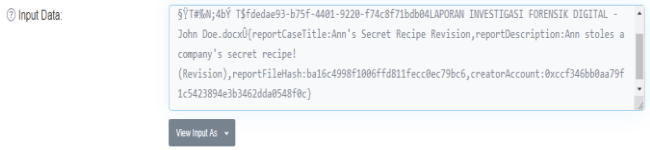


Gambar 10 *Form* Unggah Laporan oleh *User* (Penyidik)

Karena fungsi ini terintegrasi dengan *smart contract* supaya data yang dikirim juga dapat disimpan pada sisi *Blockchain* Ethereum maka akan muncul tampilan Metamask pada *browser user* untuk melakukan konfirmasi transaksi, apabila *user* menyetujui maka transaksi akan diproses pada *Blockchain* dan setelah *block* yang memiliki data transaksi *hash* dan berisikan data laporan investigasi *user* sudah terkonfirmasi, maka sistem akan menyimpan hasil *receipt* transaksi beserta data laporan yang telah diunggah (Gambar 11).



Gambar 11 Tampilam Data Laporan Investigasi yang Diunggah oleh *User* pada Sistem



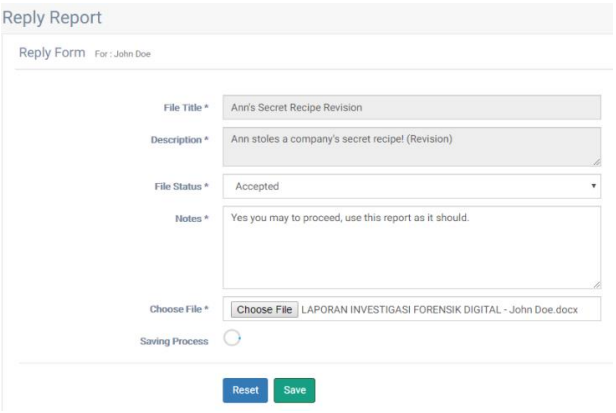
Gambar 12 Hasil Data Laporan Investigasi yang Disimpan pada *Blockchain* Ethereum

Gambar 13 Hasil Data Laporan Investigasi yang Diunggah Admin

Sedangkan pada sisi *Blockchain* yang menyimpan data laporan investigas *user* supaya dapat selalu terjaga integritasnya, maka pada Gambar 11 atau Gambar 12 terdapat juga informasi mengenai laporan investigasi yang tersimpan disimpan pada *Blockchain*. Perlu diketahui juga bahwa data yang telah tersimpan pada *Blockchain* tentu tidak dapat dihapus maupun diubah secara mudah, karena *Blockchain* merupakan *database* terdistribusi dimana setiap *block* saling terhubung.

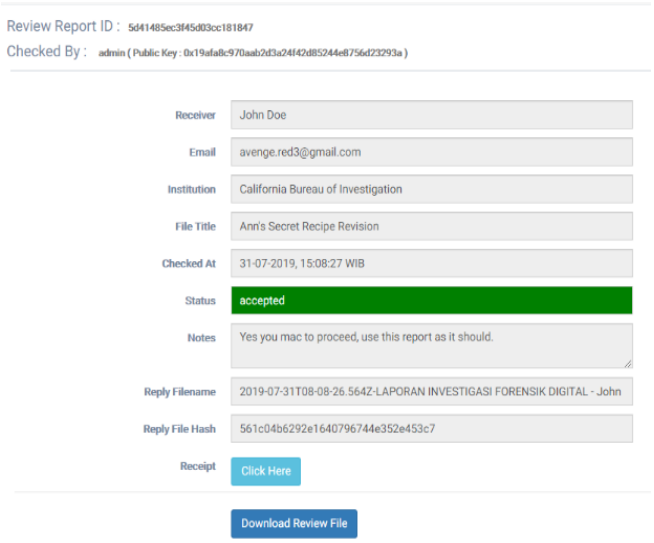
3) Balas Laporan Investigasi *User* oleh Admin

Kemudian apbila admin akan membalas laporan investigasi *user* yang telah diunduh dan diperiksa sebelumnya, maka sama seperti pada fungsi unggah laporan investigasi oleh *user*, pada fungsi atau *middleware* balas laporan ini juga menerapkan fungsi dari *smart contract* yang telah dibuat dan supaya dapat menyimpan data-data pendukung pada *Blockchain* untuk menjamin integritas hasil verifikasi atau pemeriksaan laporan investigasi *user*, maka admin yang menggunakan diharuskan memiliki akun Metamask dan Ether yang digunakan dalam *testnet* Rinkeby sebagai kompensasi transaksi ketika penggunaan fungsi ini. Ketika admin akan menggunakan fungsi balas laporan investigasi, admin diharuskan mengisi informasi terkait dengan hasil pemeriksaan dokumen laporan terkait (Gambar 14).



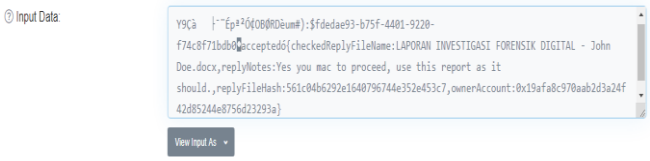
Gambar 14 *Form* Balas Laporan Investigasi *User* oleh Admin

Sama seperti fungsi unggah laporan pada sisi *user*, karena fungsi ini terintegrasi dengan *smart contract* supaya data yang dikirim juga dapat disimpan pada sisi *Blockchain* Ethereum maka akan muncul tampilan Metamask pada *browser* admin untuk melakukan konfirmasi transaksi. Apabila admin menyetujui maka transaksi akan diproses pada *Blockchain* dan setelah *block* yang berisikan data hasil pemeriksaan laporan investigasi *user* sudah terkonfirmasi, maka sistem akan menyimpan hasil *receipt* transaksi beserta data laporan yang telah diunggah (Gambar 15).

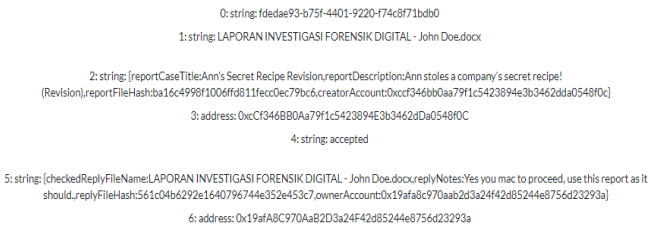


Gambar 15 Hasil Tampilan Data Laporan Investigasi yang Sudah Diperiksa pada Sistem

Berikut pada Gambar 16 atau pada Gambar 17 terdapat data hasil pemeriksaan investigasi yang disimpan pada *Blockchain*. Data-data yang disimpan dan disajikan pada gambar tersebut merupakan data-data yang berkaitan dengan laporan investigasi forensik digital *user*, seperti data *filehash* laporan yang menggunakan MD5, status hasil pemeriksaan, nama *file* laporan, akun Metamask, dan lain sebagainya.



Gambar 16 Hasil Data Laporan Investigasi yang Telah Diperiksa dan Disimpan pada *Blockchain* Ethereum



Gambar 17 Hasil Data Laporan Investigasi yang Sudah Diperiksa oleh Admin

Sehingga dengan adanya penyimpanan data-data pendukung tersebut, dapat juga digunakan sebagai bukti beserta integritas data hasil pemeriksaan laporan investigasi yang dilakuan melalui layanan sistem ini.

B. Pengujian

Pengujian merupakan tahap terakhir dalam tahapan penelitian seperti yang sudah digambarkan pada Gambar 3 terkait alur atau tahapan penelitian. Pada tahap ini, terdapat dua jenis pengujian yang telah dilakukan yaitu:

1) Pengujian Waktu Eksekusi Transaksi pada *Blockchain* Ethereum

Pengujian ini dilakukan untuk mengetahui besaran biaya transaksi yang digunakan ketika pengguna mengeksekusi sebuah fungsi yang terintegrasi dengan *Blockchain* Ethereum dan juga untuk mengetahui apakah besaran gas yang digunakan mempengaruhi lamanya waktu eksekusi transaksi. Pada Tabel 1 terdapat hasil dari skema pengujian berdasarkan fungsinya masing-masing, selain itu juga terdapat dua parameter yang digunakan dalam pengujian ini seperti lamanya waktu eksekusi transaksi yang dihitung dari awal pemanggilan fungsi sampai selesai dieksekusi, dan yang terakhir adalah besaran gas yang digunakan yang didapat dari hasil transaksi yang sudah berhasil dikonfirmasi.

Tabel 1 Hasil Pengujian Waktu Eksekusi Transaksi

No	Skema Pengujian	Ukuran (bytes)	Waktu Eksekusi (detik)	Gas yang Digunakan	Biaya Transaksi (ETH)
1	Melakukan *deploy contract address* oleh admin	7417	162	2018809	0.002018809
2	Penyidik 1 mengunggah laporan investigasi	804	59	504590	0.00050459
3	Penyidik 2 mengunggah laporan investigasi	676	63	415262	0.000415262
4	Penyidik 3 mengunggah laporan investigasi	644	66	394226	0.000394226
5	Penyidik 4 mengunggah laporan investigasi	1220	58	794892	0.000794892
6	Penyidik 5 mengunggah laporan investigasi	708	99	438922	0.000438922
7	Admin membalas laporan investigasi penyidik 1	1860	75	1196003	0.001196003
8	Admin membalas laporan investigasi penyidik 2	1828	38	1173366	0.001173366
9	Admin membalas laporan investigasi penyidik 3	1858	60	1195491	0.001195491
10	Admin membalas laporan investigasi penyidik 4	1830	54	1174070	0.00117407
11	Admin membalas laporan investigasi penyidik 5	1988	114	1284628	0.001284628

Dari penyajian tabel tersebut terdapat berbagai macam variasi nilai yang telah didapatkan, dan untuk pengolahan data yang dilakukan terdapat pada bagian kolom biaya transaksi (*transaction fee*) dengan satuan Ether (ETH). Seperti yang sudah dijelaskan pada pembahasan Ethereum, bahwa Ether (ETH) merupakan satuan nilai dari Ethereum, yang apabila digunakan pada jaringan publik Ethereum nilai ini akan menjadi nilai acuan sebagai kompensasi untuk melakukan transaksi. Sedangkan untuk perhitungan mendapatkan biaya transaksi dalam Ether untuk sebuah fungsi yang telah dilakukan, terdapat cara perhitungannya sendiri, seperti pada persamaan (1)

$$\text{ETH } Transaction\ Fee = \frac{G_{used} \times G_{price}}{1 \times 10^9} \quad (1)$$

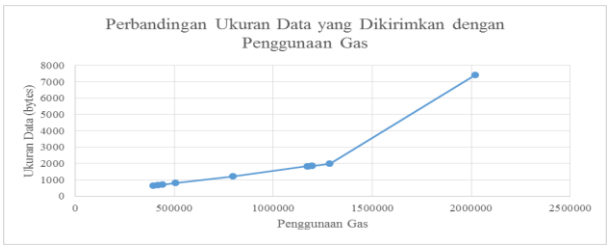
Pada persamaan (1) merupakan rumus yang digunakan untuk menghitung nilai biaya transaksi (ETH), dan juga pada tersebut terdapat dua variabel yang dibutuhkan dalam menghitung nilai transaksi. Seperti G_used yang merupakan besaran gas yang digunakan dan G_price merupakan harga gas yang dijadikan sebagai acuan pada jumlah Ether yang pengguna bayarkan untuk setiap unit gas yang digunakan serta biasa diukur dalam satuan Gwei (1 Gwei = 0.000000001 Ether).

Sebagai contoh untuk menghitung nilai transaksi pada saat admin men-*deploy contract address* seperti pada Tabel 1, membutuhkan gas yang digunakan sebesar 2.018.809 gas,

dan karena pada proses ini dijalankan pada jaringan publik *Blockchain* Ethereum maka untuk G_price sudah ditetapkan pada saat proses transaksi terjadi yaitu benrilai 1 Gwei atau 0.000000001 Ether. Lalu apabila diterapkan pada persamaan (4.1) akan diperoleh hasil berikut:

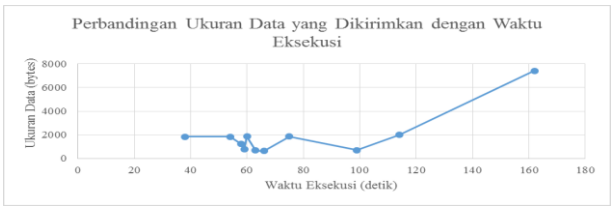
$$\text{ETH } Transaction\ Fee = \frac{2.018.809 \times 1 \text{ Gwei}}{1 \times 10^9} = 0.002018809 \text{ Ether}$$

Hasil perhitungan tersebut didapatkan nilai biaya transaksi yang admin harus bayarkan ketika men-*deploy contract address* adalah sebesar 0.002018809 Ether.



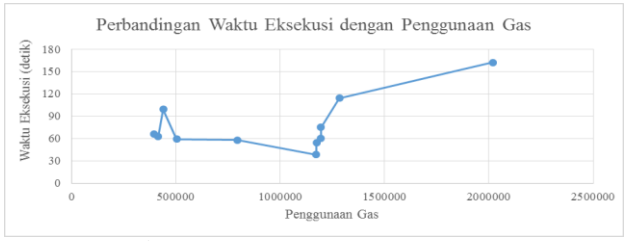
Gambar 18

Pada Tabel 1 terkait dengan hasil pengujian performa transaksi pada jaringan *Blockchain* Ethereum, apabila dibahas hubungan antara besaran data transaksi yang dikirimkan dengan penggunaan gas seperti yang digambarkan pada Gambar 18. Dihasilkan sebuah kesimpulan berdasarkan grafik perbandingan tersebut, jika semakin besar ukuran data yang dikirimkan, tentu akan semakin besar juga kebutuhan dalam penggunaan gas. Hal ini disebabkan pada setiap perhitungan gas, dihitung dari banyaknya karakter atau data yang dimasukan pada sebuah fungsi [14]. Apabila merujuk pada *yellow paper* Wood (2014), maka akan sangat relevan dengan apa yang telah dijelaskan pada *yellow paper* tersebut. Karena semakin kompleks data yang dimasukan, tentu akan meningkatkan penggunaan gas pada saat melakukan transaksi pada jaringan *Blockchain* Ethereum.



Gambar 19

Seperti pada Gambar 19 yang menggambarkan grafik perbandingan ukuran data transaksi yang dikirimkan dengan lama waktu eksekusi transaksi. Diketahui bahwa ukuran data transaksi yang dikirimkan, tidak mempengaruhi kecepatan waktu eksekusi transaksi. Jika dihitung untuk setiap rata-rata waktu eksekusi transaksi pada setiap fungsi, didapatkan rata-rata waktu yaitu 77 detik. Sejalan dengan perbandingan waktu eksekusi dan penggunaan gas yang dapat dilihat pada Gambar 20, tentunya hubungan antara besaran ukuran data yang dikirimkan dengan lama waktu eksekusi transaksi juga tidak berbanding lurus.



Gambar 20 Grafik Perbandingan Penggunaan Gas dan Waktu Eksekusi

Berdasarkan grafik pada Gambar 20, dapat diambil kesimpulan mengenai pengujian waktu eksekusi transaksi pada *Blockchain* Ethereum yang menggunakan *testnet* Rinkeby bahwa perbandingan waktu eksekusi transaksi tidak berbanding lurus dengan penggunaan gas yang digunakan. Hal tersebut bisa terjadi karena dipengaruhi oleh beberapa faktor ketika pertama kali fungsi atau transaksi dijalankan pada jaringan publik *Blockchain* Ethereum. Seperti adanya waktu pending dalam mengkonfirmasi transaksi atau berdasarkan tingkat *difficulty* atau kesulitan dari sebuah fungsi yang dijalankan.

2) Pengujian Implementasi Sistem kepada Responden

Pada pengujian implementasi sistem ini telah dilakukan pengujian kepada 11 responden yang dipilih dengan kriteria mahasiswa yang berasal dari jurusan Teknik Informatika, Universitas Islam Indonesia. Adapun proses pengujian dilakukan dengan cara penguji dipersilahkan untuk mencoba sistem secara langsung sambil dibimbing dan diberikan penjelasan. Tujuan dari pengisian kuesioner ini adalah sebagai alat ukur pengujian kelayakan sistem. Lalu berkaitan dengan rekapitulasi hasil dari kuesioner yang telah diisi oleh para penguji sistem dapat dilihat pada Tabel 2.

Tabel 2 Hasil Kuesioner Pengujian Implementasi Sistem

No	Pernyataan	Nilai
A	**Manfaat dan Kesesuaian Konten**	
1.	Sistem ini bermanfaat bagi penyidik untuk mendapatkan hasil verifikasi dokumen hasil investigasi forensik digital	88%
2.	Sistem membantu pemeriksa laporan untuk melakukan verifikasi dokumen hasil investigasi forensik digital sebagai cara pengesahan laporan	82%
3.	Konten format laporan investigasi forensik digital sudah sesuai dengan kebutuhan dalam penulisan hasil laporan	73%
4.	Adanya format laporan investigasi forensik digital yang telah ditentukan akan bermanfaat dalam menghasilkan penulisan hasil laporan yang baik	83%
5.	Penerapan *Blockchain* dapat membantu meningkatkan kevalidan sebuah *file* atau data	77%
6.	Penerapan *Blockchain* dapat meningkatkan keamanan dalam proses penyimpanan data	88%
7.	Data atau informasi yang disimpan pada jaringan publik *Blockchain* Ethereum memiliki tingkat kecepatan proses transaksi yang baik	75%
Rata-Rata Manfaat dan Kesesuaian Konten		**81%**
B	**Usabilitas Sistem**	**Nilai**
1.	Menu yang tersedia mudah dipahami	80%
2.	Menu yang tersedia mudah digunakan	83%
3.	Dari sisi halaman penyidik atau User memiliki tampilan yang baik	70%
4.	Dari sisi halaman admin memiliki tampilan yang baik	75%
5.	Pemilihan warna pada sistem nyaman dilihat	68%
6.	Informasi yang disajikan pada sistem mudah dipahami	75%
7.	Informasi yang disajikan pada sistem sudah sesuai dengan kebutuhan	78%
Rata-Rata Usabilitas Sistem		**76%**

C	Fungsionalitas pada Sisi *User*	Nilai
1.	Fungsi registrasi *User* baru dapat berfungsi dengan baik	80%
2.	Fungsi unduh format laporan dapat berfungsi dengan baik	82%
3.	Fungsi unggah laporan dan menyimpan data transaksi *Blockchain* dapat berfungsi dengan baik	78%
4.	Lihat detail informasi laporan yang telah diunggah oleh *User* dapat berfungsi dengan baik	78%
5.	Lihat detail informasi balasan laporan yang dikirimkan oleh admin dapat berfungsi dengan baik	83%
6.	Fungsi unduh laporan yang telah diperiksa dan dikrimkan oleh admin dapat berfungsi dengan baik	83%
7.	Lihat data profil *User* dapat berfungsi dengan baik	98%
8.	Fungsi ubah *password* dapat berfungsi dengan baik	80%
9.	Melakukan verifikasi laporan investigasi forensik digital dengan memasukkan data *transaction hash* dan laporan investigasi forensik digital yang telah disahkan, dapat berfungsi dengan baik	82%
Rata-Rata Fungsionalitas pada Sisi *User*		**83%**
D	**Fungsionalitas pada Sisi Admin**	**Nilai**
1.	Pengaturan untuk mengunggah dan *compile* berkas *smart contract* dapat berfungsi dengan baik	78%
2.	Fungsi *deploy contract address* dapat berfungsi dengan baik	73%
3.	Fungsi hapus pengaturan *smart contract* dapat berfungsi dengan baik	80%
4.	Fungsi mengunggah format laporan dapat berfungsi dengan baik	80%
5.	Fungsi mengubah data format laporan dapat berfungsi dengan baik	88%
6.	Fungsi hapus format laporan dapat berfungsi dengan baik	82%
7.	Lihat detail informasi laporan investigasi yang dikirimpkan oleh *User* dapat berfungsi dengan baik	82%
8.	Fungsi unduh laporan yang telah dikirimkan oleh *User* dapat berfungsi dengan baik	85%
9.	Mengunggah dan menandatangani laporan investigasi forensik digital *User* yang telah diperiksa dalam format .pdf, dengan menggunakan *signature key*s yang dihasilkan sebelumnya, sebagai bukti pengesahan, dapat berfungsi dengan baik	77%
10.	Mengunduh laporan investigasi forensik digital *User* yang telah ditandatangani atau disahkan dalam bentuk kode QR dapat berfungsi dengan baik	85%
11.	Mengisi form balasan serta mengunggah laporan investigasi forensik digital yang telah ditanda tangani dan menyimpan data transaksi pada *Blockchain* Ethereum dapat berfungsi dengan baik	77%
12.	Fungsi unduh laporan yang telah dikirimkan ke *User* dapat berfungsi dengan baik	85%
13.	Lihat informasi data *User* secara keseluruhan dan secara detail dapat berfungsi dengan baik	92%
14.	Fungsi menghapus data *User* dapat berfungsi dengan baik	82%
15.	Fungsi ubah *password* akun admin dapat berfungsi dengan baik	82%
Rata-Rata Fungsionalitas pada Sisi Admin		**82%**

Setelah hasil akhir didapatkan, hasil tersebut dapat dikategorikan ke beberapa kategori yang ada pada Tabel 3.

Tabel 3 Kategori Penilaian

Skor Pengujian	Kategori Penilaian
0% - 19,99%	Sangat Kurang
20% - 39,99%	Kurang
40% - 59,99%	Cukup
60% - 79,99%	Baik
80% - 100%	Sangat Baik

Berdasarkan perhitungan skor pengujian kuesioner yang telah dilakukan terhadap 12 responden penguji sistem sebelumnya pada Tabel 2, didapatkan bahwa untuk skor pengujian dengan kategori manfaat dan kesesuaian konten memiliki skor sebesar 81%, lalu untuk kategori pengujian usabilitas sistem memiliki skor sebesar 76%, kemudian untuk kategori pengujian fungsionalitas pada sisi user memiliki skor sebesar 83%, dan skor pengujian fungsionalitas pada sisi admin memiliki skor sebesar 82%, sehingga dapat disimpulkan dari hasil pengujian implementasi kepada responden bahwa sistem yang telah dibuat merupakan sistem yang bermanfaat dan sesuai dengan kebutuhan pengguna, memiliki usabilitas yang baik, dan juga memiliki fungsionalitas yang sangat baik pada sisi *user* maupun pada sisi admin.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian dan perancangan sistem verifikasi dokumen hasil investigasi forensik digital dengan menggunakan teknologi *Blockchain* yang dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1) Penelitian ini telah menghasilkan sistem verifikasi dokumen hasil investigasi forensik digital berbasis *Blockchain* Ethereum yang diharapkan dapat dijadikan sebagai solusi atas kevalidan verifikasi dan pelaporan dokumen investigasi forensik digital dengan memastikan integritas atau keaslian dokumen yang disimpan. Adapun cara bagaimana sistem atau aplikasi tersebut dapat terhubung dan menyimpan data transaksi pada jaringan *Blockchain* Ethereum adalah dengan membangun dan mengimplementasikan *smart contract* yang berisikan fungsi-fungsi yang telah disesuaikan dengan kebutuhan sistem.

2) Adapun cara melakukan proses verifikasi dokumen laporan investigasi forensik digital yang telah diperiksa atau disahkan, pengguna dapat memasukan data berupa dokumen laporan investigasi forensik digital yang akan diverifikasi dan data *transaction hash* yang telah didapatkan dari hasil proses transaksi di *Blockchain* Ethereum yang juga dapat diperiksa melalui situs rinkeby.etherscan.io, sehingga dapat disimpulkan sistem verifikasi dokumen hasil investigasi forensik digital yang telah dibangun dapat digunakan untuk melakukan verifikasi dokumen yang juga dapat dilihat buktinya melalui *transaction hash* pada jaringan *Blockchain* Ethereum dengan testnet Rinkeby.

3) Berdasarkan hasil pengujian implementasi sistem yang ditujukan kepada para penguji dengan kriteria yang telah ditentukan melalui daftar pertanyaan dalam bentuk kuesioner dan simulasi pengujian fungsionalitas. Didapatkan hasil dari berbagai aspek pengujian seperti fungsionalitas sistem, bahwa sistem yang telah dibangun berjalan dengan baik dan berfungsi sebagaimana mestinya, serta untuk

pengujian usabilitas sistem, manfaat dan kesesuaian konten, juga memiliki hasil yang baik. Selain itu terkait dengan hasil uji performa transaksi dalam melakukan penyimpanan data pada jaringan Blockchain Ethereum dengan menggunakan *testnet* Rinkeby, menunjukkan respon rata-rata waktu transaksi yaitu 77 detik walaupun dengan besaran gas yang berbeda, sehingga dapat dapat disimpulkan apabila sistem yang dikembangkan menerapkan jaringan publik *Blockchain* Etherum tentu akan memerlukan waktu dalam memproses transaksi yang dilakukan. Namun berkaitan dengan besaran uang digital Ether yang dibayarkan ketika melakukan sebuah proses transaksi dalam menjalan sebuah fungsi, besaran Ether yang dikeluarkan tersebut dapat diketahui dengan melakukan perkalian dari jumlah gas yang digunakan dengan harga gas yang ditentukan. Di mana besaran penggunaan gas tersebut telah terbukti berbanding lurus dengan ukuran data yang dikirimkan pada saat melakukan transaksi, sehingga dapat dikatakan jumlah Ether yang harus dikeluarkan ketika melakukan sebuah transaksi dalam menjalankan sebuah fungsi dipengaruhi oleh besarnya ukuran data yang dikirimkan melalui proses transaksi pada jaringan publik *Blockchain* Ethereum.

B. Saran

Setelah melakukan penelitian ini, penulis menyadari masih terdapat beberapa kekurangan dalam sistem yang telah dirancang. Pada penelitian selanjutnya, diharapkan dapat mengurangi atau menutupi kekurangan yang masih ada pada sistem ini, serta dapat mengembangkan sistem yang menerapkan teknologi *Blockchain* lebih luas lagi. Berikut beberapa saran untuk penelitian selanjutnya adalah sebagai berikut:

1) Berkaitan dengan pengguna admin untuk melakukan pemeriksaan dan verifikasi laporan, sistem ini hanya memiliki satu admin saja untuk melakukan aktivitas tersebut. Diperlukan adanya jenis pengguna lain supaya admin tidak terlalu banyak memiliki aktivitas yang sebenarnya tidak perlu dilakukan.
2) Beberapa informasi pada tampilan sistem tidak perlu ditampilkan seluruhnya, dan berdasarkan hasil pengujian terkait dengan usabilitas sistem masih perlu dilakukan perbaikan terhadap tampilan antarmuka sistem pada pengguna khususnya pada tampilan user dan admin.
3) Pengembangan implementasi sistem yang sama dapat diteliti lebih lanjut tentunya dengan menyesuaikan kebutuhan sistem dan *smart contract*, serta dapat menerapkan secara penuh sebuah sistem yang terdesentralisasi dengan jaringan *Blockchain* Ethereum.

REFERENSI

[1] Wahid, A. & Mohammad L., 2005, Kejahatan Mayantara (Cyber Crime), Bandung: PT Refika Aditama.

[2] Badan Standardisasi Nasional. (2008). Sistem manajemen mutu - Dasar-dasar dan kosakata.

[3] Badan Standardisasi Nasional. (2014). SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital. Jakarta.

[4] Buterin, V., Wiederhold, B. K., Riva, G., & Graffigna, G. (2013). A next-generation *smart contract* and decentralized application platform. Etherum, 11(January), 7. https://doi.org/10.1016/j.jchromb.2013.02.015

[5] Bhiantara, I. B. P. (2018). Teknologi Blockchain Cryptocurrency Di Era Revolusi Digital. Seminar Nasional Pendidikan Teknik Informatika (SENAPATI), 9(September), 173–177. Retrieved from http://eproceeding.undiksha.ac.id/index.php/senapati/article/view/1204

[6] Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain Enabled Applications. Blockchain Enabled Applications. https://doi.org/10.1007/978-1-4842-3081-7

[7] Kelley, M. (2012). Report Writing Guidelines. Diakses pada 24 Juli 2019, dari https://www.forensicmag.com/article/2012/05/report-writing-guidelines

[8] Laurance, T. (2017). Blockchain for Dummies.

[9] Modi, R. (2018). Solidity Programming Essentials. Packt Publishing.

[10] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. Journal for General Philosophy of Science, (1), 1–9. https://doi.org/10.1007/s10838-008-9062-0

[11] Palmer, G. (2001). A Road Map for Digital Forensic Research. Proceedings of the 2001 Digital Forensics Research Workshop (DFRWS 2004), 1–42. http://doi.org/10.1111/j.1365-2656.2005.01025.x

[12] Pemerintah Indonesia. 1981. *Undang-Undang Republik Indonesia Nomor 8 tahun 1981 tentang Hukum Acara Pidana*

[13] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. https://doi.org/10.6028/NIST.IR.8202

[14] Wood, G. (2014). Ethereum: a Secure Decentralised Generalised Transaction Ledger Eip-150 Revision. *Ethereum Project Yellow Paper*, *1-32*. https://doi.org/10.10177/CBO9781107415324.004