

**Blockchain dan Smart Contract untuk Keamanan
Dokumen Elektronik: Studi Kasus Ijazah dan Transkrip**

Proposal Tugas Akhir

Kelas MK Penulisan Proposal (TA-TELE-CYBERSECURITY)

1301164305

NERO CHANIAGO



Program Studi Sarjana Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2019

Lembar Persetujuan

Blockchain dan Smart Contract untuk Keamanan Dokumen Elektronik: Studi Kasus Ijazah dan Transkrip

Blockchain and Smart Contract for Electronic Document Security: Case Studies Diplomas and Transcripts

NIM :1301164305

NERO CHANIAGO

Proposal ini diajukan sebagai usulan pembuatan tugas akhir pada
Program Studi Sarjana Informatika
Fakultas Informatika Universitas Telkom

Bandung, 20 November 2019

Menyetujui

Calon Pembimbing 1

Calon Pembimbing 2

Parman Sukarno,S.T.,M.Sc.,Ph.D

NIP. 17770073

Aulia Arif Wardana,S.Kom.,M.T

NIP. 19920009-3

ABSTRAK

Ijazah dan Transkrip merupakan sertifikat yang diterbitkan secara resmi sebagai pengakuan terhadap prestasi belajar untuk penyelesaian suatu jenjang pendidikan. Banyak ijazah yang dikeluarkan setiap tahunnya, namun kasus pemalsuan ijazah masih menjadi masalah utama. Ditjen Belmawa meluncurkan Sistem Verifikasi Ijazah Elektronik (SIVIL) serta agar meningkatkan pelayanan kepada masyarakat Kemristekdikti juga meluncurkan Penomoran Ijazah Nasional (PIN), namun data ijazah dan transkrip tersebut disimpan secara terpusat sehingga rentan terhadap peretasan yang dapat menyebabkan kerusakan dan kehilangan data dalam jumlah besar. Solusi untuk permasalahan tersebut adalah dengan menggunakan Blockchain dan smart contract. Smart contract adalah sebuah media yang bersifat immutable untuk menyimpan aturan terkait negosiasi ketentuan kontrak, cara tersebut akan otomatis melakukan verifikasi saat pencapaian dari konsensus. Blockchain disamakan dengan buku besar digital yang menyimpan transaksi / sebuah basis data terdesentralisasi. Setiap transaksi divalidasi dengan node kriptografi. Untuk itu akan dibangun sistem keamanan dan verifikasi dokumen elektronik berdasarkan ijazah dan transkrip dengan teknologi Blockchain dan smart contract, dan melakukan pengujian *Steganography* terhadap dokumen elektronik tersebut. Hipotesa dari metode yang digunakan akan menghasilkan tingkat pada sistem keamanan karena penyimpanan menggunakan basis data terdesentralisasi dan transaksi dilakukan dengan media smart contract.

Kata Kunci: Blockchain, Smart Contract, Ijazah, Tanskrip, *Steganography*.

DAFTAR ISI

Lembar Persetujuan	1
ABSTRAK	2
DAFTAR ISI	3
BAB 1	4
1. PENDAHULUAN	4
1.1. Perumusan Masalah	5
1.2. Tujuan.....	5
1.3. Batasan Masalah	5
1.4. Rencana Kegiatan	5
1.5. Jadwal Kegiatan.....	6
BAB 2	7
2. KAJIAN PUSTAKA	7
2.1. <i>Comparative Study</i>	7
BAB 3	14
3. PERANCANGAN SISTEM	14
3.1. Model Perancangan untuk Keamanan Sistem .Error! Bookmark not defined.	
3.1.1. Proses Perancangan Keamanan SistemError! Bookmark not defined.	
3.1.2. <i>Breakdown Web3JS</i>	14
3.2. Proses Pengujian	15
3.3. Model Pengujian Terhadap Serangan <i>Steganography</i> .. Error! Bookmark not defined.	
DAFTAR PUSTAKA	16

BAB 1

1. PENDAHULUAN

Ijazah dan Transkrip merupakan sertifikat yang diterbitkan secara resmi sebagai pengakuan terhadap prestasi belajar untuk penyelesaian suatu jenjang pendidikan. Banyak ijazah dan transkrip yang dikeluarkan oleh suatu universitas setiap tahunnya. Tetapi, pemalsuan ijazah masih menjadi masalah utama. Kepala bagian HKLI Ditjen Belmawa, Nuri Fulkan pada tahun 2019, memaparkan laporan atau berita tentang maraknya ijazah palsu yang meningkat laporannya seiring pesta politik dan setelah pesta politik digelar [2]. Sedangkan menurut [3], kasus yang berkaitan dengan penggunaan ijazah palsu ini banyak terjadi di Indonesia. Kasus ijazah dan transkrip palsu ini terjadi salah satunya dikarenakan pihak perusahaan atau sebuah institusi yang sulit dalam memverifikasi keaslian ijazah dan transkrip tersebut [4]. Ditjen Belmawa telah membuat dan meluncurkan suatu sistem yang bernama Sistem Verifikasi Ijazah Elektronik (SIVIL), serta Kemristekdikti pun telah meluncurkan Penomoran Ijazah Nasional (PIN) dalam ijazah dan transkrip [14]. Namun masalah dalam sistem tersebut ialah data ijazah dan transkrip dari berbagai universitas disimpan secara terpusat pada sisi server, sehingga server tersebut rentan terhadap peretasan yang dapat menyebabkan kerusakan dan kehilangan data dalam jumlah cukup besar. Untuk itu dalam tugas akhir ini penulis mengusulkan sistem pengamanan dan verifikasi dokumen elektronik berdasarkan ijazah dan transkrip yang dikeluarkan oleh universitas.

Guna meningkatkan keamanan server dan menjaga keaslian dari dokumen elektronik ijazah dan transkrip tersebut, pada tugas akhir ini akan dilakukan pembangunan sistem dengan metode Blockchain dan smart contract. Smart contract adalah sebuah media yang bersifat immutable untuk menyimpan aturan terkait negosiasi ketentuan kontrak, cara tersebut akan otomatis melakukan verifikasi saat pencapaian dari konsensus. [5], dan memiliki proses transaksi yang kredibel sehingga tidak bisa dilacak ataupun diubah [12]. Blockchain disamakan dengan buku besar digital yang menyimpan transaksi / sebuah basis data terdesentralisasi [8], setiap transaksi divalidasi dengan node dan transaksi hash kriptografi [6], Blockchain menggunakan teknologi jaringan *peer-to-peer* yang terdesentralisasi sehingga Blockchain adalah tempat penyimpanan yang paling aman untuk data digital dengan adanya kerahasiaan dan integritas data [12], dengan arti sebuah data seperti informasi penting dapat dipindahkan dari satu pengguna ke pengguna yang lain tanpa bantuan pihak ketiga [8]. Setelah transaksi smart contract ditambahkan pada Blockchain, tidak ada yang dapat memodifikasi atau mengubahnya [6], sehingga integritas file ijazah dan transkrip yang dikeluarkan oleh universitas dapat dijaga keamanannya dan tidak dapat diubah maupun dipalsukan.

Oleh karena itu, tugas akhir ini akan membahas mengenai sistem keamanan dan verifikasi dokumen elektronik ijazah dan transkrip, dan mengkombinasikannya dengan sistem berbasis Blockchain dan smart contract. Kemudian menguji dokumen elektronik ijazah dan transkrip dengan serangan *Steganography*, sehingga diharapkan akan mendapatkan sistem yang aman.

1.1. Perumusan Masalah

Berdasarkan permasalahan yang disebutkan pada latar belakang diatas, dapat disimpulkan yaitu:

Masih terdapatnya ijazah dan transkrip palsu, dan penyimpanan data pada Sistem Verifikasi Ijazah Elektronik (SIVIL) masih menggunakan database/sisi server secara terpusat sehingga rentan terhadap peretasan data dalam jumlah besar.

1.2. Tujuan

Berdasarkan permasalahan yang telah dikemukakan diatas berikut adalah rincian tujuan penulisan tugas akhir ini yaitu:

Mengamankan dan memverifikasi dokumen ijazah dan transkrip elektronik menggunakan Blockchain dan smart contract.

1.3. Batasan Masalah

Agar penelitian ini dapat dilakukan lebih fokus, sempurna, dan mendalam maka penulis memandang permasalahan penelitian yang diangkat perlu dibatasi, berikut adalah batasan masalahnya:

1. Menggunakan algoritma kriptografi Proof of-Work (PoW) SHA-256.

1.4. Rencana Kegiatan

Rencana kegiatan yang akan saya lakukan adalah sebagai berikut:

1. Studi Literatur
Pada tahap ini dilakukan pencarian literatur secara mandiri ke berbagai sumber.
2. Menganalisa Kebutuhan
Pada tahap ini dilakukan kajian mengenai kebutuhan-kebutuhan teknologi yang akan di implementasikan dalam tugas akhir ini.
3. Analisis dan Perancangan Sistem
Analisis dan perancangan sistem yang akan dibangun menggunakan metode Blockchain dan smart contract. Tahapan umum dari sistem ini terdiri dari input dokumen elektronik ijazah dan transkrip, lakukan hashing terhadap dokumen elektronik, memasukan hashing tersebut pada Blockchain, memverifikasi kebenaran dokumen elektronik tersebut.
4. Implementasi Sistem

Tahap ini merupakan implementasi dari perancangan sistem dimana akan membuat sebuah aplikasi menggunakan bahasa pemrograman Remix Solidity, Node JS, Meta Mask, Ganache/EVM, *Steganography*.

5. Pengujian Sistem

Pengujian sistem dilakukan berdasarkan metode yang sudah dibuat.

6. Penulisan Laporan

Hasil dari seluruh rangkaian kegiatan pada penelitian Tugas Akhir (TA) ini akan didokumentasikan ke dalam laporan.

1.5. Jadwal Kegiatan

Jadwal kegiatan yang akan saya lakukan adalah sebagai berikut:

Tabel 1 Jadwal Kegiatan.

Kegiatan	Bulan					
	1	2	3	4	5	6
Studi Literatur						
Menganalisa Kebutuhan						
Analisis dan Perancangan Sistem						
Implementasi Sistem						
Pengujian Sistem						
Penulisan Laporan						

BAB 2

2. KAJIAN PUSTAKA

2.1. Comparative Study

Ada beberapa aplikasi dan teknik yang dapat digunakan untuk melakukan pengamanan pada dokumen elektronik dan Blockchain. Pada bagian ini akan dibahas mengenai teknik dan aplikasi pada penelitian tentang pengamanan dokumen elektronik dan juga tentang penelitian berbasis Blockchain yang sudah ada sebelumnya.

Tabel 2 *Comparative Study*.

Judul	<i>Physical Document Validation with Perceptual Hash.</i>
Penulis	Prasetyo Adi Wibowo Putro
Penerbit	IEEE
Review	Penelitian [10] ini bertujuan untuk membuat dokumen persyaratan validasi secara elektronik. Masalah yang ada, dokumen fisik akan selalu mempunyai nilai hash yang berbeda setiap kali didigitalkan. Melalui penelitian ini ditinjau apakah hash perseptual dapat digunakan untuk validasi elektronik dari dokumen fisik. Kesimpulan yang dihasilkan dari penelitian ini, persepsi dapat menggunakan hash dan dapat mendeteksi semua modifikasi yang terjadi pada dokumen elektronik.
Kelebihan	Menggunakan hash perseptual dan dapat mendeteksi semua modifikasi yang terjadi pada dokumen elektronik.
Kekurangan	Nilai hash perseptual tidak dimasukkan kedalam basis data Blockchain agar lebih aman, karena menyangkut dokumen elektronik pribadi.
Judul	<i>SecureCEdit: An Approach for Secure cloud-based Document Editing.</i>

Penulis	Shashank Arora, Gaurav Varshney, Pradeep K. Atrey, Manoj Mishra
Penerbit	IEEE
Review	Penelitian [11] ini bertujuan untuk membuat layanan pengeditan dokumen online berbasis cloud. Seperti Google Documents, dan menyediakan cara yang murah dan efisien untuk mengelola dokumen. Namun, menyimpan data di cloud juga menimbulkan masalah keamanan dan privasi tertentu. Terutama ketika data bersifat rahasia dan sensitif. Untuk mengatasi masalah kerahasiaan dengan layanan pengeditan dokumen online saat ini, penelitian ini menyajikan metode pengeditan dokumen yang aman yang disebut SecureCEdit, menggunakan aplikasi berbasis web yang menyimpan dokumen pengguna diatas penyimpanan cloud (pada penelitian ini studi kasus adalah google drive) dalam bentuk terenkripsi, namun menyediakan sebagian besar fungsi pengeditan online. Solusi yang diberikan tidak hanya aman secara komputasi, tetapi juga memberikan peningkatan kinerja.
Kelebihan	Mampu menyimpan data pengguna pada cloud dalam bentuk terenkripsi dan solusi yang diberikan aman terhadap komputasi.
Kekurangan	Kekurangan dalam penelitian ini layanan memakai cloud dan hanya mengenkripsi data, data tidak dimasukkan pada database Blockchain yang dapat mengamankan data tersebut.
Judul	Desain e-Transkrip Dengan Teknologi Blockchain.
Penulis	Agus Winarno
Penerbit	Trijurnal-Online Universitas Trisakti Lembaga Penelitian
Review	Penelitian [4] ini menjelaskan tentang kegunaan teknologi Blockchain yang banyak digunakan pada bidang pendidikan. Menurut [4] Teknologi

	Blockchain memiliki keunggulan dengan sistem yang terdesentralisasi dan kriptografi yang kuat dapat membantu universitas dalam membangun infrastruktur dalam penyimpanan arsip berupa transkrip nilai, sertifikasi dan ijazah. Penerapan teknologi Blockchain dalam dunia pendidikan antara lain adalah BlockCert, e-Portfolio, dan Book Copyright. BlockCert adalah salah satu tool yang diciptakan MIT yang dapat digunakan untuk membuat, menerbitkan, dan memverifikasi sertifikat berbasis Blockchain. Penelitian ini mencoba mendesain e-Transkrip yang berbasis Blockchain menggunakan tool BlockCert dari MIT.
Kelebihan	Membuat desain e-Transkrip dengan database Blockchain yang aman dan menggunakan tools BlockCert dalam mengamankan, memverifikasi, dan menyimpan data.
Kekurangan	Belum direalisasikan sehingga tidak mengetahui apakah berhasil.
Judul	<i>An Overview of Smart Contract and Use cases in Blockchain Technology.</i>
Penulis	Bhabendu Khumar Mohanta, Soumyashree S Panda, Debasish Jena
Penerbit	IEEE
Review	Penelitian [6] ini menjelaskan tentang kontrak pintar yang terintegrasi dengan teknologi Blockchain yang mampu melakukan tugas secara <i>real time</i> dengan biaya rendah dan memberikan tingkat keamanan yang lebih besar. Makalah ini pertama-tama, menjelaskan berbagai komponen dan prinsip kerja dari kontrak pintar. Kedua, mengidentifikasi dan menganalisis berbagai kasus penggunaan kontrak pintar bersama dengan keuntungan menggunakan kontrak pintar dalam aplikasi Blockchain.

Kelebihan	Menjelaskan tentang kinerja kontrak pintar dan Blockchain akan menghasilkan keamanan yang tinggi serta menganalisisnya.
Kekurangan	Tidak ada proses pengujian yang melihat apakah data tersebut tetap aman apabila dilakukan testing blackbox, whitebox ataupun serangan <i>cyber</i> .
Judul	<i>PHOTOGROUP: DECENTRALIZED WEB APPLICATION USING ETHEREUM BLOCKCHAIN.</i>
Penulis	Keyur Paralkar, Shiwani Yadaf, Shikha Kumari, Apurva Kulvarni, S.P. Pingat
Penerbit	Semanthics Scholar
Review	Penelitian [7] ini menjelaskan tentang privasi para pengguna media sosial. Di sebagian sistus web, data disimpan pada sistem terpusat yang disebut sebagai server. Salah satu database terdesentralisasi adalah Blockchain. Karena itu makalah ini menyajikan aplikasi web untuk berbagi foto media sosial yang terdesentralisasi yang didasarkan pada teknologi Blockchain, dimana pengguna akan dapat melihat, menyukai, mengomentari, berbagi foto yang di bagi oleh pengguna yang berbeda.
Kelebihan	Sudah menggunakan aplikasi Blockchain untuk berbagi foto pada media sosial yang terdesentralisasi.
Kekurangan	Tidak menjelaskan hash yang digunakan pada file foto tersebut.
Judul	<i>File Encryption and Hiding Application based on Advance Encryption Standard (AES) and Append Insertion Steganography Method.</i>
Penulis	Gotfried C. Prasetyadi, Achmad Benny Mutiara, Rina Refianti
Penerbit	IEEE

Review	<p>Penelitian [15] ini menjelaskan <i>Steganography</i> adalah metode menyembunyikan pesan rahasia di objek lain yang tampak tidak berbahaya sehingga keberadaannya tidak terlihat. Dalam makalah ini, sebuah pesan yang merupakan file komputer dari jenis apapun, disembunyikan dari file sampul yang merupakan file komputer dari jenis tertentu. Metode <i>Steganography</i> yang digunakan dimakalah ini disebut metode <i>Steganography</i> penyisipan append. Metode <i>Steganography</i> ini dipilih sebagai upaya untuk menghilangkan batasan format pesan, yang muncul dalam banyak metode <i>Steganography</i> populer. Untuk mengacak pesan tersembunyi, AES-256 (Algoritma Rijndael) digunakan untuk mengenkripsi pesan dengan frasa sandi rahasia. Blok byte khusus digunakan untuk mengidentifikasi dan memverifikasi pesan asli sehingga dapat dipulihkan sambil mempertahankan integritasnya. Dalam pengujian, 5 file acak digunakan sebagai pesan rahasia, untuk integritas dihitung menggunakan metode SHA-256 sebelum di rusak dan setelah dirusak file nya. Dalam pengujian integritas dokumen dapat dipertahankan.</p>
Kelebihan	Melakukan pengujian dengan 5 file acak untuk melihat verifikasi integritas file tersebut dengan menggunakan algoritma SHA-256.
Kekurangan	Untuk meng-enkripsi pesan menggunakan AES-256, tidak menggunakan SHA-256.
Judul	<i>BroncoVote: Secure Voting System Using Ethereum's Blockchain.</i>
Penulis	Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic, Jordan Mohler
Penerbit	Semanthics Scholar
Review	<p>Penelitian [13] menjelaskan sistem voting, voting adalah bagian mendasar dari sistem demokrasi, e-Voting adalah solusi dari masalah tersebut.</p>

	<p>Dalam makalah ini mengusulkan sistem pemungutan suara berbasis Blockchain, bernama BroncoVote, yang menjaga privasi pemilih dan meningkatkan aksesibilitas, sambil menjaga sistem pemungutan suara tetap aman, transparan, dan hemat biaya. BroncoVote mengimplementasikan kerangka kerja pemungutan suara skala universitas yang menggunakan blockchain dan kontrak pintar Ethereum untuk mencapai administrasi pemilih dan catatan pemungutan suara yang dapat diaudit. Selain itu, BroncoVote menggunakan beberapa teknik kriptografi, termasuk enkripsi homomorfik, untuk mempromosikan privasi pemilih. Implementasi kami digunakan di Ethernet Testnet untuk menunjukkan kegunaan, skalabilitas, dan efisiensi.</p>
Kelebihan	<p>Menerapkan sistem Blockchain pada e-voting untuk melindungi data pemilih, dan menggunakan teknik kriptografi dan melakukan implementasi pada Ethernet Testnet untuk melihat kegunaannya, skalabilitas, dan efisiensi.</p>
Kekurangan	<p>Tidak melakukan pengujian serangan terhadap sistem.</p>
Judul	<p><i>Steganography & tools used for Steganography.</i></p>
Penulis	<p>Manisha Saini, Gaurav Saini</p>
Penerbit	<p>International Journal of Scientific & Engineering Research</p>
Review	<p>Makalah [16] ini membahas konsep di belakang <i>Steganography</i> dengan menjelajah terlebih dahulu apa itu dan bagaimana <i>Steganography</i> telah digunakan diseluruh aspek dan dasar-dasar <i>Steganography</i>. Makalah ini menjelaskan tentang cara kerja, metode, dan tools apa saja dalam <i>Steganography</i>.</p>

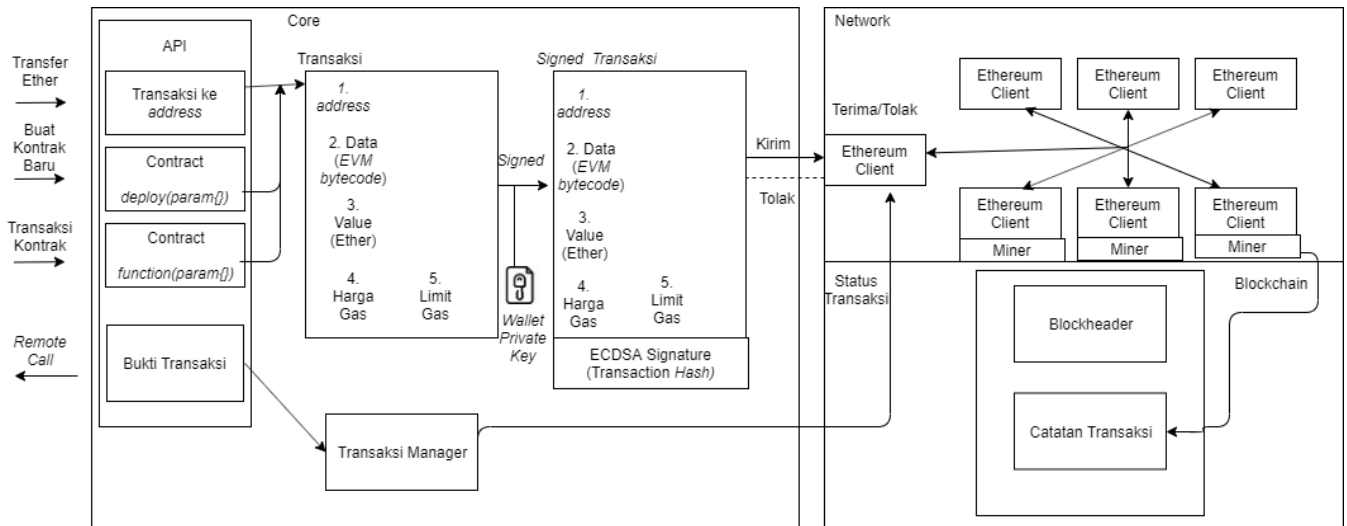
Kelebihan	Menjelaskan tools apa saja yang ada dalam <i>Steganography</i> seperti tools untuk file Img, audio, PDF, musik.
Kekurangan	Tidak semuanya dijelaskan secara terperinci hanya menuliskan tools saja.

Pada penelitian diatas telah disimpulkan penelitian-penelitian yang menggunakan pendekatan yang berbeda-beda tetapi targetnya sama yaitu mengamankan dokumen elektronik. Namun dalam penyimpanan dan verifikasi datanya masih terbilang cukup rentan. Maka akan dilakukan pembangunan sistem pengamanan dokumen dan verifikasi dokumen elektronik menggunakan Blockchain dan smart contract, serta pada tugas akhir ini akan melakukan pengujian terhadap dokumen elektronik menggunakan serangan *Steganography* agar terlihat apakah sistem yang dibangun dapat menahan dan mendeteksi dokumen elektronik yang telah dirusak oleh *Steganography* pada saat di verifikasi, sehingga apabila tahan terhadap serangan *Steganography*, maka dapat disimpulkan bahwa dokumen elektronik ijazah dan transkrip tidak dapat dipalsukan.

BAB 3

3. PERANCANGAN SISTEM

3.1.1. Breakdown Web3JS



Gambar 12 : Breakdown Web3JS

Dari ketiga gambar perancangan keamanan sistem diatas, berikut detail penjelasan sistem yang akan digunakan pada tugas akhir ini.

1. Dataset menggunakan dokumen elektronik ijazah dan transkrip bertipe PDF.
2. Untuk memulai transaksi smart contract dan membuat kontrak baru perlu memiliki Ether (bahan bakar dari Blockchain Ethereum).
3. Membuat kontrak baru dan melakukan transaksi yang memuat *address*, data (*EVM byte*), *value (Ether)*, harga gas dan limit gas.
4. Sebelum transaksi disetujui, file dokumen elektronik ijazah dan transkrip dihitung terlebih dahulu hash nya untuk mendapatkan digital signature file tersebut.
5. File tersebut telah memiliki digital signature yang sudah tidak bisa diubah kembali dan dilakukan transaksi menggunakan *private key wallet* dari Ganache CLI/EVM.
6. Kemudian jika file tersebut berhasil dilakukan transaksi, maka digital signature dari file tersebut masuk pada Ethereum client dan tercatat pada Blockchain.

7. Dokumen elektronik ijazah dan transkrip telah memiliki digital signature dan telah berada pada jaringan Blockchain sehingga akan meningkatkan pengamanan data tersebut dan tidak dapat dipalsukan.
8. Jika ingin melihat integritas dokumen elektronik ijazah dan transkrip, unggah file dokumen elektronik ijazah dan transkrip tersebut pada sistem dan jika terdapat pada Blockchain maka sistem mendeteksi bahwa file dokumen elektronik ijazah dan transkrip tersebut adalah asli.

3.2. Proses Pengujian

Proses pengujian adalah dengan melakukan serangan dan keamanan sistem yang telah dibuat dan akan menghasilkan keamanan yang tinggi dalam segi integritas dan keamanan data pada database terdesentralisasi. Data yang akan di analisis adalah dokumen elektronik ijazah dan transkrip terhadap serangan *Steganography*, karena jika dokumen elektronik ijazah dan transkrip tahan terhadap serangan *Steganography* maka dokumen tersebut tidak dapat dipalsukan.

Langkah-langkah yang dilakukan adalah sebagai berikut :

1. Masukkan dokumen elektronik ijazah dan transkrip bertipe PDF pada sistem. Lalu algoritma Proof of-Work SHA-256 melakukan hashing dan mengenerate digital signature pada file tersebut.
2. Meta Mask melakukan transaksi smart contract dari digital signature file tersebut untuk selanjutnya dimasukan pada Blockchain Ethereum Ganache CLI. Jika berhasil melakukan transaksi maka dokumen elektronik ijazah dan transkrip tersebut sudah terdapat pada Blockchain.
3. Pengujian serangan, dokumen yang telah atau yang belum dimasukan pada Blockchain akan dirusak oleh *Steganography*. Kemudian dokumen elektronik yang dirusak tersebut dimasukan pada sistem verifikasi terdesentralisasi untuk memverifikasi.
4. Sistem memverifikasi dokumen elektronik ijazah dan transkrip yang rusak tersebut, sehingga akan menghasilkan bahwa dokumen tersebut tidak terdapat pada Blockchain yang artinya bahwa dokumen tersebut palsu atau sudah diubah maupun dirusak.
5. Jika file yang belum dirusak oleh serangan *Steganography* akan menghasilkan bahwa dokumen tersebut terdapat pada Blockchain dan digital signature tersebut akurat, pada Blockchain file tersebut memiliki block number, address, dan alamat transaksi.

DAFTAR PUSTAKA

- [1] Fitri. (2015). Blangko Ijazah Pendidikan Tinggi. Diakses pada 15 Oktober 2019. Available: <http://lldikti12.ristekdikti.go.id/2015/11/26/blangko-ijazah-pendidikan-tinggi.html>
- [2] Belmawa dan Tamsis. (2019). Waspada Ijazah Palsu, Subbagian Hukum Ditjen Belmawa Selenggarakan Sosialisasi. Diakses pada 15 Oktober 2019. Available: <https://belmawa.ristekdikti.go.id/2019/08/23/waspada-ijazah-palsu-subbagian-hukum-ditjen-belmawa-selenggarakan-sosialisasi/>
- [3] Tempo. (2018). Kemenristek Dikti Terima Laporan 141 Pejabat Berijazah Palsu. Diakses pada 15 Oktober 2019. Available: <https://nasional.tempo.co/read/842273/kemenristekdikti-terima-laporan-141-pejabat-berijazah-palsu>
- [4] Agus Winarno. (2019). Desain e-Transkrip Dengan Teknologi Blockchain. 2019 Seminar Nasional Pakar ke 2.
- [5] Rina Candra Noorsanti., Herlbertus yulianton., Kristophorus Hadiono. (2018). Blockchain-Teknologi Mata Uang Kripto (*Crypto Currency*). 2018 Seminar Nasional Multi Disiplin Ilmu dan Call for Papers.
- [6] Bhabendu Khumar Mohanta., Soumyashree S Panda., Debasish Jena. (2018). an Overview of *Smart Contract* and Use cases in Blockchain Technology. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).
- [7] Keyur Paralkar., Shiwani Yadaf., Shikha Kumari., Apurva Kulvarni., S.P. Pingat. (2018). Photogroup: Decentralized Web Application using Ethereum Blockchain. 2018 International Research Journal of Engineering and Technology (IRJET).
- [8] Rajness Gupta. Hands-On Cybersecurity with Blockchain. Livery Place 35 Livery Street Birmingham B3 2PB, UK. ISBN 978-1-78899-018-9. Packt Publishing, 2018.
- [9] Gerbang Investasi. (2019). Inilah 7 Platform dan Alat untuk Mengembangkan dan Menguji Aplikasi Blockchain. Diakses pada 18 Oktober 2019. Available: <https://internationalinvestorclub.com/2019/06/10/inilah-7-platform-dan-alat-untuk-mengembangkan-dan-menguji-aplikasi-blockchain/>
- [10] Prasetyo Adi Wibowo Putro. (2017). Physical Document Validation with Perceptual Hash. 2017 IEEE 3rd International Conference on Science in Information Technology.
- [11] Shashank Arora, Gaurav Varshney, Pradeep K. Atrey, Manoj Mishra. (2016). SecureCEdit: An Approach for Secure cloud-based Document Editing. 2016 IEEE Conference on Communications and Network Security (CNS).

- [12] Achmad Muhaimin Aziz., Avon Budiono., Adityas Widjajarto. (2019). Analisis dan Implementasi Komunikasi Antar Node IPFS (Interplanetary File System) Pada *Smart Contract* Ethereum.
- [13] Gaby G. Dagher., Praneeth Babu Marella., Matea Milojkovic., Jordan Mohler. (2018). BroncoVote: Secure Voting System Using Ethereum's Blockchain.
- [14] Kementrian Riset, Teknologi dan Pendidikan Tinggi Lembaga Layanan Pendidikan Tinggi Wilayah XII Maluku, Maluku Utara. (2016). Sistem Verifikasi Ijazah Elektronik (SIVIL) dan Penomoran Ijazah Nasional (PIN). Diakses pada 16 Oktober 2019. Available: <http://ldikti12.ristekdikti.go.id/2016/05/02/sistem-verifikasi-ijazah-elektronik-sivil-dan-program-penomoran-ijazah-nasional-pin.html>
- [15] Gotfried C. Prasetyadi., Achmad Benny Mutiara., Rina Refianti. (2017). File Encryption and Hiding Application based on Advance Encryption Standard (AES) and Append Insertion Steganography Method. 2017 Second International Conference on Informatics and Computing (ICIC).
- [16] Manisha Saini., Gaurav Saini. (2014). *Steganography* & tools used for *Steganography*. International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014.
- [17] Jurnal Web. (2014). Cara Mengetahui Informasi Lengkap dari Sebuah Website. Diakses pada 20 November 2019. Available: <https://www.jurnalweb.com/cara-mengetahui-informasi-data-lengkap-dari-sebuah-website/>
- [18] Quality Nonsense LTD. (2019). Discover who is hosting any website. Diakses pada 20 November 2019. Available: <https://www.whoishostingthis.com/#search=ijazah.ristekdikti.go.id>