

## Implementasi Blockchain dalam Aplikasi Pemilu

Yulfitno Wingga Pratama<sup>1\*</sup>, Denny Kurniadi<sup>2</sup>

<sup>1</sup>Prodi Pendidikan Teknik Informatika Fakultas Teknik Universitas Negeri Padang

<sup>2</sup>Jurusan Teknik Elektronika Fakultas Teknik Universitas Negeri Padang

\*Corresponding author e-mail: yulfitno@mail.com

### ABSTRAK

Pemilu merupakan kegiatan demokrasi di Indonesia yang dilaksanakan setiap lima tahun sekali untuk memilih pemimpin, namun dalam proses perhitungan pemilu secara manual, hasilnya bocor dan dapat menimbulkan masalah keamanan data. Melalui penelitian ini, kami dapat memberikan solusi dengan mengimplementasikan teknologi blockchain pada aplikasi pemilu yang akan memberikan keamanan terhadap data hasil pemilu yang tersimpan di blockchain. Teknologi Blockchain adalah rantai blok data yang terhubung satu sama lain secara peer to peer. Aplikasi ini menggunakan bahasa pemrograman Solidity dan menggunakan database blockchain ethereum lokal (Ganache). Menggunakan metode dalam pembuatan aplikasi ini adalah metode waterfall dengan pemodelan Unified Modeling Language (UML) dimana metode visual modeling pada perancangan sistem berorientasi objek. Dari hasil pengujian berdasarkan aspek dasar *blockchain* hasil diperoleh aplikasi ini bisa menyimpan data hasil pemilu yang akan tersimpan di node pada setiap transaksinya.

**Kata kunci :** Pemilu, Blockchain, Ganache (Local Blockchain Ethereum)

### ABSTRACT

*Elections are a democratic activity in Indonesia which are carried out every five years to elect leaders, but in the process of manual election calculations, the results are leaked and can cause data security problems. Through this research, we can provide solutions by implementing blockchain technology in election applications that will provide security for election results data stored on the blockchain. Blockchain technology is a chain of data blocks that are connected to each other by peer to peer. This application uses the Solidity programming language and uses a local ethereum blockchain database (Ganache). Method used to build this application is the waterfall method with Unified Modeling Language (UML) modeling where the visual modeling method is in object-oriented system design. From the test results based on the basic aspects of the blockchain, the results obtained that this application can store election results data that will be stored in nodes for each transaction.*

**Keywords:** Election, Blockchain, Ganache (Local Ethereum Blockchain).

## I. PENDAHULUAN

Pemilihan umum berkala merupakan prasyarat bagi suatu bentuk pemerintahan yang demokratis. [1] Manipulasi suara sering terjadi pada akhir pemilu, seperti segel safety box rusak atau hasil pemilu rusak karena perselisihan antar Pasangan Calon (Paslon). Pada pemilu serentak 2019 permasalahan yang paling menonjol antara lain kotak suara yang tidak tersegell pada 6.474 tps, selain itu terjadi juga kasus surat suara yang tertukar antar daerah pemilihan tps.[2] Salah satu cara mengatasi permasalahan pemilu

konvensional adalah dengan menerapkan sistem pemilu elektronik. Dengan menggunakan teknologi blockchain, pada dasarnya *blockchain* adalah buku besar yang menyimpan daftar transaksi dengan cara yang tidak berubah dan hanya di tambahkan seiring waktu dan memperluas rantai dengan cara yang aman [3].

Transaksi yang dilakukan akan dienkripsi menggunakan Secure Hash Algorithm 256 (SHA-256) dan akan membuat semacam rantai blok dan mengirimkannya jaringan yang terhubung peer-to-

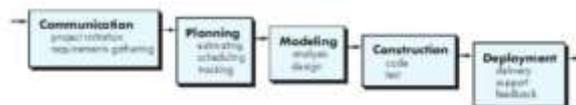
peer sehingga semua dapat memvalidasi masing-masing transaksi.[4] Setiap data hasil pemilihan oleh pemilih akan di simpan dalam jaringan peer to peer blockchain dan seiring waktu akan bertambah dan tidak dapat dirubah sehingga menjamin data hasil pemilu akan aman tanpa ada gangguan pihak yang tidak bertanggung jawab.[5]

Perancangan aplikasi ini diharapkan dapat mengatasi proses penghitungan hasil akhir penghitungan suara di TPS oleh panitia KPU.[8] Dengan menerapkan blockchain dan memanfaatkan setiap node yang terhubung dalam jaringan Ethereum blockchain di dapatkan hasil bahwa setiap node yang ada dalam jaringan akan menampung hasil pemilihan dari setiap pemilih.[6]

## II. METODE

### Metode Waterfall

Menurut Pressman (2015:42), *waterfall* model adalah model klasik yang sistematis, berurut dalam membangun *software*. Nama model ini sebenarnya adalah “*Linear Sequential Model*”. Model ini sering disebut juga dengan “*classic life cycle*” atau metode waterfall. Model ini termasuk ke dalam model generic pada rekayasa perangkat lunak dan pertama kali diperkenalkan oleh Winston Royce sekitar tahun 1970 dan merupakan model yang paling banyak di pakai dalam *Software Engineering* (SE). Berikut merupakan fase-fase dalam model waterfall menurut Pressman :



Gambar.1 Model waterfall menurut pressman

Dalam perancangan ini menggunakan Teknik sebagai berikut :

- a. Planning  
Tahapan perencanaan yang menjelaskan tentang teknis, sumber daya dan hasil dari prodek yang ingin dihasilkan
- b. Modelling  
adalah proses pemodelan dan perancangan arsitektur yang terfokus pada perancangan struktur data, arsitektur software, algoritma program dan tampilan interface.
- c. Construction  
adalah proses penerjemahan bentuk desain menjadi kode atau bentuk yang dapat dibaca oleh mesin. Setelah pengkodean selesai dilakukan pengujian terhadap sistem dan kode yang sudah dibuat.
- d. Deployment

Tahapan ini merupakan tahapan implementasi software ke penelitian yang dilakukan

### Analisis Sistem

Menurut (Yogiyanto, 1995) adalah penguraian dari suatu sistem informasi yang utuh kedalam bagian komponennya dengan maksud untuk mengevaluasi dan mengidentifikasi permasalahan, kesempatan, hambatan yang terjadi sesuai kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan. Tujuan dari analisis sistem ini untuk mempersiapkan hal-hal yang perlu dikembangkan dalam perancangan suatu sistem informasi, serta menganalisis permasalahan, kebutuhan, dan kelemahan oleh pemakai sistem untuk dapat memberikan solusi ke dalam unsur-unsur yang terlibat yaitu :

### Analisis Proses Bisnis

Proses bisnis (*business process*) dapat didefinisikan sebagai banyak aktivitas atau pekerjaan terstruktur saling terkait untuk mengakhiri masalah tertentu atau yang menghasilkan produk dan atau layanan tertentu (Weske, 2007).

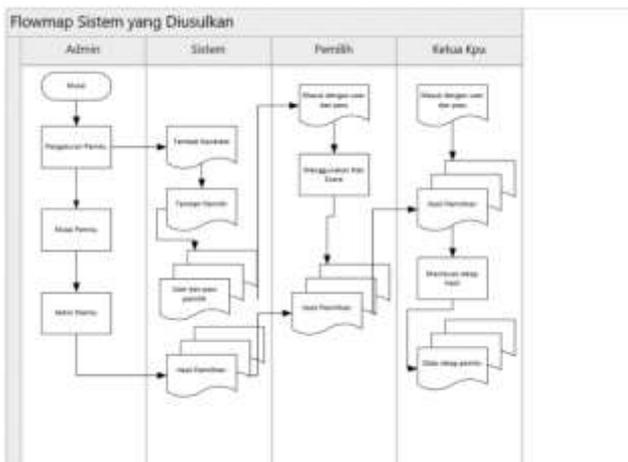
Tabel 1. Analisis Proses Bisnis

No	Proses bisnis	Aktivitas
1	Pengelolaan Pemilihan	<ul style="list-style-type: none"> <li>• Admin atau staff terkait mengisi data yang diperlukan untuk pelaksanaan pemilu</li> <li>• Admin atau staff terkait membuat akun</li> <li>• Admin atau staff terkait memulai pemilihan umum</li> <li>• Admin atau staff terkait mengakhiri pemilihan umum</li> </ul>
2	Pengelolaan pemilih	<ul style="list-style-type: none"> <li>• Pemilih mndaftar di sistem dengan alamat, nama dan no ktp</li> <li>• Admin atau staff terkait menerima dan memverifikasi data dari pemilih</li> </ul>
3	Proses voting	<ul style="list-style-type: none"> <li>• Data pemilih yang telah diverifikasi oleh admin dan bisa langsung menggunakan hak</li> </ul>

		suara
4	Proses Hasil Pemilu	<ul style="list-style-type: none"> <li>Setiap vote dari pemilih akan langsung masuk ke database blockchain dan akan membuat blockc setiap data yang masuknya</li> <li>Rekap hasil akan ditampilkan setelah waktu pemilu habis dan di akhiri oleh admin</li> </ul>

**Flowmap Sistem Yang diusulkan**

Menurut (Meza Silvana, Dkk, 2015) flowmap adalah penggambaran grafik secara lengkap dari Langkah-langkah prosedur suatu program. Flowmap sistem yang diusulkan ini berisi tentang alur aplikasi dari beberapa actor mulai dari mulai sampai akhir proses aplikasi.



Gambar 2. Flowmap Sistem yang diusulkan

Flowmap sistem dijelaskan tahap berjalannya sistem dimulai dengan admin yang mengatur segala hal tentang pemilihan mulai dari penambahan kandidat, tambah akun pemilih, memulai dan mengakhiri pemilu. Pemilih yang telah mendapatkan *username* dan *password* akan bisa menggunakan hak suara. Ketika pemilihan berakhir semua *user* akan bisa mengakses hasil dari pemilihan.

**Analisis Kebutuhan**

analisis kebutuhan merupakan suatu proses yang sistematis dalam menentukan kebutuhan dalam menjalankan aplikasi.[9] ada dua kebutuhan perangkat lunak dan perangkat keras. Kebutuhan untuk perangkat keras adalah spesifikasi perangkat keras yang digunakan untuk menjalankan aplikasi ini yaitu : min cpu (intel core i3/amd A5), disk (10GB), ram (4GB), monitor (14 inch) dan input (keyboard

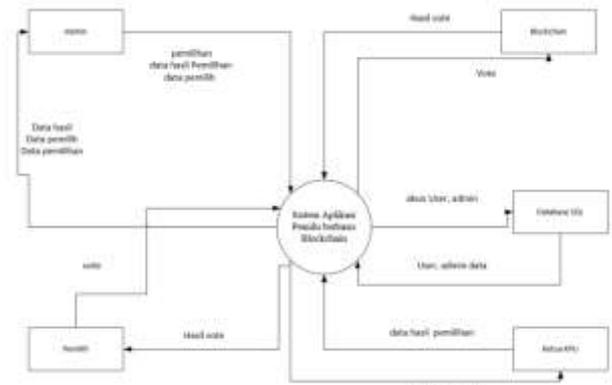
dan mouse). Untuk perangkat lunak yaitu : sistem operasi ( win 7/win 10), database (ganache), web server (web3.js), framework (truffle) dan aplikasi pendukung (metamask dan google).

**Perancangan Sistem**

(Kenneth dan Jane, 2006 : G12) mengemukakan perancangan sistem adalah aktivitas dalam merancang dan menentukan untuk mengolah sistem informasi dari hasil Analisa sehingga sistem tersebut sesuai dengan requirement

**Context Diagram**

Context diagram adalah diagram awal dalam rangkaian data diagram *flow* yang menggambarkan hubungan antar entitas dengan sistem (jogiyanto, 2005).

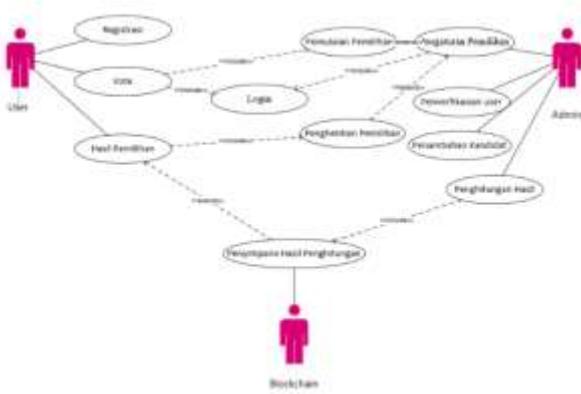


Gambar 3. Context Diagram

Context diagram diatas terlihat ada 5 terminator dalam aplikasi ini adalah, admin, pemilih, *database sql*, ketua kpu dan *blockchain*. Data admin dan pemilih akan disimpan di *sql* dan data hasil pemilih akan disimpan di *blockchain*.

**Use Case Diagram**

Sukanto dan Shalahuddin (2014: 155) mengemukakan use case diagram adalah pemodelan untuk sistem yang dibuat .Use case diagram menjelaskan bahwa alur dari suatu kegiatan yang mencapai tujuan tertentu. Pada *use case* dibawah ini dijelaskan pada gambar bahwa yang punya akun hanya dapat memvoting sekali

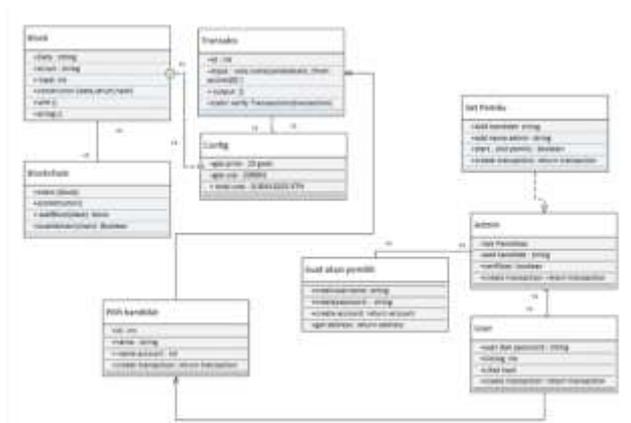


Gambar 4. Use Case Diagram

Use case dijelaskan admin memiliki fungsi mengatur pemilihan, mengatur pemilih dan hasil pemilihan. Setelah user registrasi akan diverifikasi oleh admin dan user baru bisa melakukan hasil voting, hasil voting akan masuk ke blockchain.

**Class Diagram**

Sri Mulyani (2016: 247) mengemukakan adalah diagram yang digunakan untuk mempresentasikan kelas, kelas komponen dan hubungan antar kelas. Menunjukkan hubungan antar class dalam sistem yang dibangun dan bagaimana diagram tersebut saling berhubungan untuk mencapai suatu tujuan.

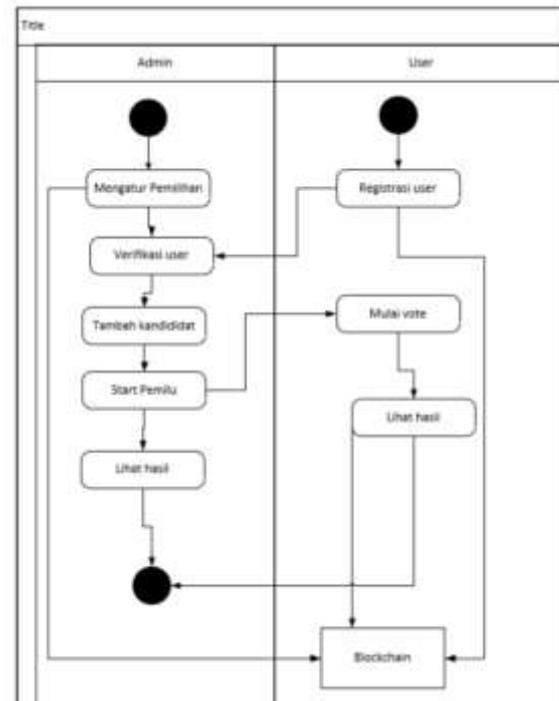


Gambar 5. Class Diagram

Class diagram diatas menunjukkan class diagram pada transaksi blockchain dan sudah ditambah dengan implementasi sistem yang dibuat

**Activity Diagram**

Activity Diagram adalah menggambarkan aliran kerja dari sebuah sistem pada perangkat lunak [15]. Teknik mendeskripsikan logika procedural, proses bisnis dan aliran kerja dalam banyak kasus.

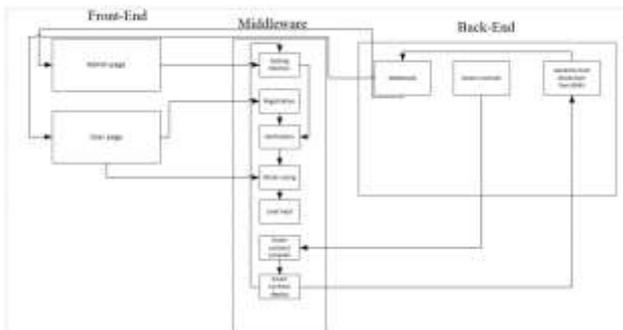


Gambar 6. Activity Diagram

Activity diagram dari admin mengatur pemilihan kemudian menambah kandidat kemudian menjalankan pemilu dan kemudian user melakukan registrasi setelah itu admin akan memverifikasi data user dan data user baru bisa melakukan voting dari hasil pemilu akan tersimpan di jaringan blockchain.

**Perancangan Arsitektur Sistem**

Arsitektur sistem adalah model konsep yang mendeskripsikan, perilaku, struktur dan pandangan dari suatu sistem, deskripsi dari arsitektur adalah deskripsi representasi dan formal dari suatu sistem yang digunakan untuk mendukung penjelasan tentang struktur sistem. [10] Dalam perancangan arsitektur sistem ini terdapat beberapa bagian yaitu front-end, middleware dan backend



Gambar 7. Arsitektur Perancangan Sistem

ada beberapa bagian dari arsitektur sistem yaitu sebagai berikut :

- *User page (front-end)* Menurut Career Foundry, frontend adalah bagian yang bertugas menghubungkan sebuah situs atau aplikasi pengguna. Pada frontend aplikasi ini

menampilkan nama kandidat *vote*, info akun dan *button vote* dan halaman admin serta registrasi dan *setting* pemilihan

- *Middleware*, pada bagian ini merupakan bagian tengah yang menghubungkan komponen *front-end* dengan komponen lainnya
- *Back-end*, merupakan bagian belakang dari sebuah web.[16] Backend sistem yang menggunakan *local host blockchain port 8545*, metamask penghubung *smart contract* dengan *browser*.

### Analisis Kebutuhan Blockchain

Perancangan sistem dengan *blockchain* ada beberapa bahan pendukung yang akan bisa membuat *blockchain* berjalan disistem yang ada sebagai berikut :

- *Ethereum*, dengan *Ethereum blockchain* dapat diprogram membuat aplikasi desentralisasi sesuai kebutuhan pengguna[11]
- *Smart contract*, sebuah perjanjian yang diubah dalam bentuk digital sehingga perjanjian sulit dilakukan.[12]
- *Address*, untuk membuat identitas unik dalam *ethereum blockchain* [13]
- *Node.js*, alat open source yang digunakan untuk menulis kontrak *solidity* langsung dari browser.
- *Solidity*, Bahasa pemrograman objek untuk menulis *smart contract blockchain*. [14]
- *Metamask*, Aplikasi *browser* yang memudahkan untuk berinteraksi dengan web berbasis *Ethereum*. [15]
- Sublime text 3 sebagai teks editor.

### Rancangan Antar Muka Aplikasi

Perancangan antar muka aplikasi ini terdapat dua halaman yang ada yaitu halaman *admin* dan halaman user (pemilih). Untuk rancangan antar muka aplikasi ini menggunakan model *react.js* yang juga digunakan dalam pembuatan *UI Facebook* dan *Instagram*. Ada beberapa halaman *interface* yang akan dibahas sebagai berikut :

#### Desain Halaman Admin

Pada halaman admin berisi data admin dan pengaturan pemilihan



#### Desain Halaman Tambah Kandidat

Halaman tambah kandidat calon oleh admin



#### Desain Halaman Registrasi User

Halaman registrasi pemilih berdasarkan alamat akun ether



#### Desain Halaman Verifikasi User

Halaman verifikasi pemilih oleh admin



#### Desain Halaman Voting

Halaman voting calon kandidat oleh pemilih



### Desain Tampilan Halaman Hasil

Halaman hasil baik pemilih maupun admin sistem bisa melihat hasil ketika pemilihan berakhir



## III. HASIL DAN PEMBAHASAN

### Hasil Pembuatan

Pembuatan Aplikasi pemilu ini dengan implementasi *blockchain* ini memiliki tujuan untuk mengamankan data hasil pemilihan umum sehingga data hasil yang rentan akan kecurangan akan tersimpan di setiap *block* di dalam jaringan *blockchain* secara *peer-to-peer*. [17]

### Implementasi Sistem

Tahap implementasi merupakan kegiatan pembangunan sistem atau aplikasi dengan bantuan perangkat lunak dan perangkat keras sesuai dengan analisis dan perancangan untuk menghasilkan suatu sistem yang bekerja. Sistem ini diimplementasikan menggunakan *solidity v5.0* untuk pengolahan kode program (*back-end*), *javacript Sintax Ekstensiom (JSX)* sebagai pengolah *user interface (front-end)*.

### Pengujian Sistem Berdasarkan Aspek Dasar Blockchain

Tahap pengujian ini didasarkan sifat dasar *blockchain* yaitu sebagai berikut :

- *Immutability*  
Adalah sifat dimana data input yang masuk ke dalam sistem *blockchain* tidak dapat dirubah atau di hapus [18]



Seperti yang terlihat pada gambar diatas terdapat beberapa detail komponen transaksi *blockchain* yaitu Hash, Nonce, *blockHash*, *blockNumber*, Transaction Index, value dan v,r,s. ada 7 layer keamanan dalam suatu *block* dan membutuhkan waktu dan resources yang tepat untuk membuka dan merubah data dalam keamanan 7 tingkat layer tersebut bisa di pertanggungjawabkan sifat *immutability* nya.

- *Transparansi*  
Adalah sifat *blockchain* dimana setiap perubahan data yang terjadi dalam sistem berbasis *blockchain* dapat dilihat oleh seluruh partisipan yang terlibat. [19] Setiap *vote* yang dilakukan makan pada *blockchain* akan terbentuk *block* baru seperti berikut



- *Terdesentralisasi*  
Pada sifat ini data yang terdistribusi kepada setiap partisipan yang terlibat sehingga semua partisipan mempunyai data Salinan yang sama [20]. Pada kasus ini perancangan aplikasi ini semua jenis user akan dapat mengakses data hasil pemilihan sehingga bisa disebut terdesentralisasi

## IV. KESIMPULAN

Berdasarkan perancangan yang telah dilakukan, beberapa poin kesimpulan sebagai berikut :

1. Perancangan ini dilakukan dengan mendefinisikan *asset participant* dan *transaction* yang terlibat dalam sistem database yang dibangun. Dengan hasil berupa jaringan *local blockchain* port 8545 dengan *local host metamask* port yang sama
2. Hasil fungsionalitas aplikasi sekitar 90% dari keseluruhan analisis fungsionalitas

**V. SARAN**

Saran yang di peroleh dari perancangan aplikasi pemilu dengan implementasi blockchain adalah ketersediaan akun ether untuk pemilih yang harus disediakan oleh pemerintah dan aplikasi ini hanya mempunyai satu fungsi database dan belum bisa diterapkan pada pemilu nasional.

**DAFTAR PUSTAKA**

- [1] Riko Herwanto, Firmansyah YA. (2020). ” KawalPilkada : Electronic Vote Aman Konseptual Teknologi Blockchain Berbasis Sistem”. *Jurnal Teknika ; Politeknik Negeri Brijayaya*.
- [2] Aryojati , Ardipadanto. (2019). “Jurnal Permasalahan Penyelenggara Pemilu Serentak Tahun 2019”
- [3] Narayan, A.; Bonneau, J.; Merasa, E.; Miller, A.; Goldfter, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction; Princenton University Press: Princenton, NJ, USA, 2016
- [4] Scheiner, Bruce. (1996). “ Applied Cryptography, Second Edition : Protocols, Algorithms”
- [5] Xie. S, Zheng. Z, Chen. W, Wu . J , Dai. H, - N. Imran, M. Blockchain for cloud exchange : A survey. *Comput, Electr. Eng.*2020,81,106526.[crossRef]
- [6] Wood, G. Ethereum : A secure decent ralised generalized transaction ledger. *Ethereum Proj. Yellow Pap.*2014, 151, 1-32
- [7] S. Bragagnollo, H, Rocha, M.Denker, and S, Ducause. (2018). "SmartInspect: Solidity Smart Contract inspector" . *IEEE 1st Int. Work. Blockchain Priented Softw. Eng IWBOSE 2018-Proc.; vol 2018-Janua, pp. 9-18-2018*.
- [8] Dagher, G., Marella, P., Milojkovic, M. and Mohler, J. “BroncoVote: Secure Voting System using Ethereum’s Blockchain”, In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pages 96-107. 2018.
- [9] Leslie J. Briggs. *Instructional Design : Principle and Aplications (New Jersey : Educational Technology, 1991)*, h.18
- [10] Nugroho, Adi. Analisis dan Perancangan Sistem Informasi dengan metodologi Berorinetasi Objek Edisi Revisi, *INFORMATIKA*. Bandung. 2005.
- [11] Bhatia, A, (2019). Ethereum/wiki. [online] Github Available at :[https://github.com/ethereum/wiki/wiki/Javas\\_cript-Api](https://github.com/ethereum/wiki/wiki/Javas_cript-Api) [ Accessed 12 jun, 2020]
- [12] Atzei N., Bartoletti M., & Cimoli, T. (2017) : A Survey of Attacks on Ethereum Smart contracts. *International Conference on Principles of Security and Trust* hal. 164-186
- [13] Liu, Yi and Wang, Qi. “An E-voting Protocol Based on Blockchain”,. *Cryptology ePrint Archive*, 1043. 2017
- [14] Dannen, C. (2017). Introducing Ethereum and Solidity. *Introducing Ethereum and Solididty* [https://doi.org/10/1007/978-1-4842-25-35-6\\_7](https://doi.org/10/1007/978-1-4842-25-35-6_7)
- [15] A. D. Samala and B. R. Fajri, “Rancang Bangun Aplikasi E-Sertifikat Berbasis Web Menggunakan Metode Pengembangan Waterfall,” *J. Tek. Inform.*, vol. 13, no. 2, pp. 147–156, 2021, doi: 10.15408/jti.v13i2.16470.
- [16]<https://medium.com/@makersinstitute/front-end-back-end-full-stack-apa-artinya-36e0f25e8142> diakses tanggal 8 agus 2020
- [17] Joshua davis, PEER TO PEER INSURANCE ON AN ETHEREUM BLOCKCHAIN General Consideration of the Fundamentals of Peer to Peer Insurance
- [18]Narayan, A.; Bonneau, J.; Merasa, E.; Miller, A.; Goldfter, S. Bitcoin and Cryptocurrency Technologies: A

Comprehensive Introduction; Princeton University Press: Princeton, NJ, USA, 2016

- [19] Xinyi, Y., Yi, Z., dan He, Y. “*Technical Characteristics and Model of Blockchain*”, 10th International Conference on Communication Software and Networks. 2018
- [20] Zheng, Zhibin et.al., “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, 2017 IEEE 6th International Congress on Big Data (BigData Congress). 2017