RANCANG BANGUN SISTEM E – VOTING DENGAN METODE ENKRIPSI BLOCKCHAIN DI KOTA MOJOKERTO

Rizal Ardilla
Mahasiswa Teknik Informatika Universitas Islam Majapahit
Rizal.ardilla.154@gmail.com

ABSTRAK

Pemilu yang ada di Indonesia telah dilakukan sejak tahun 1955, hal ini merupakan syarat dari sistem demokrasi yang mana merupakan kedaulatan rakyat dalam memilih pemimpinnya. KPU selaku penyelenggara Pemilu dibantu dengan petugas yang ada di setiap daerah dan pihak kepolisian Republik Indonesia selalu berusaha menghadirkan Pemilu yang asas langsung, bebas, rahasia, jujur dan adil, namun tanpa dukungan masyarakat hal ini tidaklah memungkinkan karena pada saat Pemilu kekuasaan penuh berada pada tangan rakyat. Dengan semakin majunya sistem informasi diharapkan Pemilu bisa menjadi lebih baik dengan mengambil manfaat dari era digital ini, bukannya malah menjadi hancur karena kecurangan yang semakin canggih. Dengan menggunakan sistem *e – voting* Pemilu dapat dilaksanakan dengan hemat dan dalam waktu yang cepat dan adanya enkripsi data pada *e-voting* diyakini mampu mengamankan data Pemilu dan pesertanya sehingga praktik kecurangan bisa dihilangkan dan mampu membuat Pemilu yang sesuai asasnya. Enkripsi blockchain merupakan salah satu cara pengamanan data melalui desain yang canggih sehingga sulit untuk dilakukan penyusupan data ke dalamnya dan memberikan kerahasiaan pada data pemilih karena akan mengenkripsi data pemilih dan apa yang dipilihnya sehingga publik tidak tahu siapa yang memilih siapa namun akan tetap muncul siapa saja yang memiliki suara terbanyak.

Kata kunci : Pemilu, KPU*, E-Voting*, Blockchain

1. PENDAHULUAN

Penyelenggaraan Pemilihan Umum (PEMILU) yang bebas dan berkala menjadi prasyarat sistem politik demokrasi, karena Pemilu sebagai sarana pelaksanaan kedaulatan rakyat yang dilaksanakan secara langsung, umum, bebas, rahasia, jujur dan adil (LUBERJURDIL) dalam Negara Kesatuan Republik Indonesia (NKRI) untuk menghasilkan pemerintahan negara yang demokratis berdasarkan Pancasila dan UUD 1945 (Indonesia, 2011). Dampak dari Pilwali ini adalah besarnya biaya yang dihabiskan negara untuk pelaksanaannya yang dilakukan mulai dari pendataan pemilih sampai rekapitulasi akhir perhitungan suara. Selain itu terdapat kendala dalam hal adanya pemilih ganda atau pemilih yang tidak memenuhi syarat tapi tetap diperbolehkan mencoblos (Ramdhani, 2018), terlambatnya distribusi surat suara dan adanya surat suara yang rusak yang menyebabkan kurangnya surat suara saat hari pemilihan (Andayani, 2018). Pengamanan kotak suara juga menjadi permasalahan karena adanya kotak surat suara yang tidak tersegel ataupun rusak sehingga mengakibatkan sengketa antara Pasangan Calon (PASLON) karena ditengarai terjadi manipulasi surat suara.

Salah satunya cara untuk mengatasi masalah pada Pemilu konvensional adalah dengan menerapkan sistem *Electronic Voting (E-Voting).* Walaupun begitu sistem *e-voting* ini masih memerlukan sistem keamanan yang kuat karena pada sistem digital terdapat banyak celah keamanan yang bisa digunakan untuk merusak suatu sistem. Dengan menggunakan blockchain maka setiap transaksi yang terjadi akan di enkripsi menggunakan *Secure Hash Algorithm 256 (*SHA-256*)* dan secara bersambung sehingga terbentuk seperti rantai atau *block* dan kemudian di kirimkan ke seluruh jaringan yang terkoneksi dengannya secara *peer – to – peer* sehingga semua dapat memvalidasi transaksi tersebut dan tidak dibutuhkan server tunggal untuk menyimpan datanya.

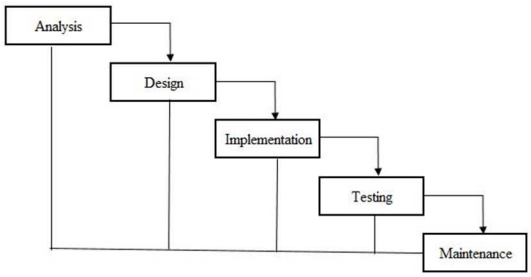
UU Nomor 32 tahun 2004 yang menyatakan bahwa " Kepala daerah dan wakil kepala daerah dipilih dalam satu pasangan calon yang dilaksanakan secara demokratis berdasarkan asas langsung, umum, bebas, rahasia, jujur dan adil." Dengan memanfaatkan teknologi blockchain tersebut yang saat ini sedang dikembangkan untuk dapat diimplementasikan pada bidang lain untuk mengamankan dan merahasiakan data, salah satunya adalah penerapan pada sistem *e-voting*. Maka dengan mengenkripsi hasil *voting* dan

menghubungkan antara satu *voting* dengan yang lainnya dalam blockchain diharapkan akan mampu mengamankan dan merahasiakan data *voting* dan identitas pemilih agar tidak akan diketahui sekalipun data enkripsi *voting* di tampilkan di hadapan publik saat perhitungan suara dilakukan.

Metode blockchain yang akan diterapkan dalam sistem e – voting ini adalah enkripsinya dengan menggunakan server tunggal untuk menyimpan data pemilih dan hasil voting sehingga akan menghemat biaya. Lokasi yang digunakan dalam penelitian ini adalah Kota Mojokerto yang pada tahun 2018 ini melakukan Pilwali dengan 4 Paslon. Diharapkan dengan adanya sistem e – voting ini dapat mengurangi tindak kecurangan yang terjadi pada Pilwali Kota Mojokerto.

Metodologi Penelitian

Penelitian ini menggunakan model SDLC (*Software Development Life Cycle*). Model SDLC yang dipakai dalam pembuatan sistem ini adalah model Waterfall. Setiap tahapan dalam waterfall harus diselesaikan terlebih dahulu sebelum melanjutkan ke tahap selanjutnya, Sehingga fokus pada masing – masing tahap dapat dilakukan dengan maksimal karena tidak adanya pengerjaan yang sifatnya paralel. Tahapan pembuatan dan perancangan sistem ini memiliki kerangka kerja seperti pada gambar di bawah:



Gambar 1 Model *Waterfall*

Tahapan – tahapan yang ada pada model *waterfall* adalah :

1. Analysis

Pada tahapan ini dilakukan analisa tentang masalah yang ada pada sistem yang sudah berjalan dan kebutuhan – kebutuhan untuk membentuk keseluruhan sistem yang berupa data mentah dan yang akan diaplikasikan dalam sistem, analisa ini didapatkan dari berbagai macam sumber pustaka maupun pengamatan langsung di lapangan.

2. Design

Design adalah proses dimana kebutuhan – kebutuhan yang telah dikumpulkan sebelumnya di rubah menjadi sebuah representasi dalam bentuk *interface* dan sistem aplikasi sebelum *implementation* dimulai. Pembuatan *user interface* akan menggunakan *Balsamiq Mockups 3* dan dan rancangan sistem akan menggunakan *UML (Unified Modelling Language)* menggunakan *usecase* diagram, *activity* diagram, ERD dan DFD Diagram.

3. Implementation

Peneliti mengubah *design* menjadi sebuah aplikasi agar dapat dimengerti oleh mesin, maka bentuknya diubah kedalam bahasa mesin menggunakan bahasa pemrograman *Java* dengan menggunakan *software Netbeans IDE 8.2*.

4. Testing

Selanjutnya adalah tahap *testing* artinya produk yang sudah jadi akan di uji coba oleh responden dan untuk mendapatkan tanggapan maka setiap responden yang sudah mencoba akan di berikan kuesioner yang berhubungan dengan sistem yang telah dibuat.

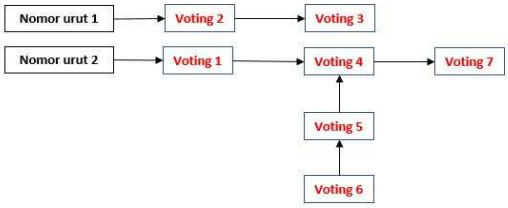
5. Maintenance

Pada tahap ini terdapat perbaikan – perbaikan yang berdasarkan pada tanggapan responden atau *error* yang masih terjadi saat tahap *testing*. Pada tahapan ini juga bisa dimasukkan tambahan – tambahan fitur baru untuk menutup kekurangan sistem yang telah dibuat.

Blockchain

Blockchain bisa didefinisikan sebagai teknologi *ledger* terdistribusi yang bisa merekam transaksi antar pengguna secara aman dan permanen. Blockchain sendiri dikenal telah digunakan dalam sistem *database* transaksi Bitcoin (Nakamoto, 2008). Hal ini menyebabkan transaksi keuangan melalui internet tanpa perlu bergantung pada institusi keuangan. Blockchain secara desain sangat aman dan merupakan contoh sistem dengan tingkat kesalahan yang kecil.

Bitcoin dan ethereum termasuk sebagai hasil dari pengaplikasian konsep blockchain untuk membuat mata uang yang bisa ditransaksikan melalui jaringan internet dan bergantung pada kriptografi untuk keamanan dan kerahasiaan data dalam bertransaksi tanpa perantara. Bitcoin menggunakan protokol konsensus yang disebut dengan PoW (*Proof of Work*) berdasarkan *cryptocurrency* yang berguna untuk memastikan hanya transaksi yang sah saja yang diperbolehkan masuk ke dalam sistem. Setiap blok dalam rantai dihubungkan dengan blok sebelumnya yang ada pada rantai. Blok pertama dalam rantai disebut dengan fondasi tumpukan atau Genesis. Setiap blok baru dibuat dengan meletakkannya di atas blok sebelumnya untuk membentuk tumpukan yang disebut blockchain, percabangan blok tetap dihitung sebagai blok yang sah dan ini tercipta karena ada blok yang masuk secara bersamaan ke dalam sistem.



Gambar 2 Model Blockchain *E -Voting*

Setiap blok yang ada di dalamnya terdapat nilai *hash* sebelumnya, data, *timestamp* dan nonce. *Timestamp* yang digunakan adalah *timestamp* dalam *millisecond* yang dimulai dari 1 Januari 1970 dan berguna untuk petunjuk waktu pembuatan *hash*, sedangkan nonce merupakan bilangan integer yang berguna untuk mengatur hasil *hash* agar nilainya sesuai dengan persyaratan. Nilai *hash* tersebut harus memenuhi persyaratan tertentu yang disebut dengan *difficulty* agar dapat dianggap *block* yang sah. Pengecekan nilai *hash* yang sesuai dengan persyaratan itulah yang dinamakan *Proof Of Work*. *Hash* ini dibuat dengan SHA-256 untuk membuat *hash* dengan ukuran tetap sebesar 256 – bit atau 64 - bit heksadesimal. Dari gambar di atas dapat dilihat bahwa fondasi dari blockchain ini adalah nomor urut dari setiap Pasangan Calon setiap pemilih akan melakukan *voting* dan pada *database* data tersebut akan diurutkan dan dibagi. Dari data yang ada sebelumnya akan dihubungkan dengan data yang datang selanjutnya dan jika ada data yang datang pada waktu yang bersamaan maka akan diposisikan sejajar yang mana semua data akan dianggap valid seperti voting 4, voting 5 dan voting 6 sehingga tidak ada data *voting* yang tidak terhitung.

SHA - 256

Proses *hash* SHA – 2 merupakan pengembangan dari SHA – 0 dan SHA – 1, di dalamnya terdiri dari 6 bagian yaitu SHA – 224, SHA – 256, SHA – 384, SHA – 512, SHA – 512/224, SHA – 512/256. Pemberian nama ini sesuai dengan panjangnya *message digest* yang dihasilkan. SHA-256 dibuat pada tahun 2002 oleh *The National Institute of Standards and Technology (NIST)*, sangat baik digunakan karena sesuai dengan hukum yang mengaturnya, dengan menggunakan algoritma SHA – 256 terbukti aman, termasuk jika digunakan dengan algoritma kriptografi dan protokol lain yang berfungsi untuk mengamankan file. SHA-256 aman karena didesain sedemikian rupa sehingga tidak memungkinkan mendapat pesan yang berhubungan dengan *message digest* atau untuk menemukan dua pesan yang berbeda yang menghasilkan *message digest* yang sama dan panjang maksimum sebuah pesan untuk dapat diproses adalah 2^{64} bit. Tahapan dalam proses SHA – 256 adalah sebagai berikut (Tammam, 2016) :

1. Mengonversi pesan (M) kedalam bentuk biner : Hal ini dilakukan karena proses yang terjadi akan berada dalam bentuk biner dan *hexadesimal*.
2. Memberikan *padding* : Memberikan *padding* dengan menambahkan bit ‘1’ pada pesan asli dan menambahkan bit ‘0’ sebanyak nilai K dengan rumus:

   $$M + 1 + K = 448\,bit + T = 512\,bit \text{.....(1)}$$

3. Menambahkan panjang pesan asli (T): Panjang pesan asli diubah dalam bentuk biner 64 bit dan memasukkannya pada akhir pesan.
4. *Parsing* : Pesan kemudian dibagi menjadi 16 dengan panjang masing -masing 32 bit yang diberi label $M_{(i)}$.
5. *Expansion* : Pada proses ini akan dilakukan ekspansi pesan dari berjumlah 16 menjadi 64 dengan label $W_{(i)}$ yang akan digunakan

dalam perhitungan dalam proses iterasi, rumus yang digunakan untuk ekspansi adalah:

$$W_{0 \le i \le 15} = M_i \quad \text{.....(2)}$$

$$W_{16 \le i \le 63} = W_{i-16} + S_0 + W_{i-7} + S_1 \quad \text{...(3)}$$

$$S_0 = (W_{i-15} \ggg 7) \oplus (W_{i-15} \ggg 18) \oplus (W_{i-15} \gg 3)$$

.....(4)

$$S_1 = (W_{i-2} \ggg 17) \oplus (W_{i-2} \ggg 19) \oplus (W_{i-2} \gg 10)$$

.....(5)

6. Menyiapkan 8 *working variable* dan nilai *hash* awal : *working* variabel ini akan digunakan pada perhitungan di proses iterasi, dalam penentuan *working* variabel ini digunakan huruf a – h dan nilai *hash* awalnya sudah ditentukan dalam SHA – 2 sehingga menjadi:

Tabel 1 Variabel dan Nilai Hash

working variabel	variabel	nilai *hash*
a	h0	0x6a09e667
b	h1	0xbb67ae85
c	h2	0x3c6ef372
d	h3	0xa54ff53a
e	h4	0x510e527f
f	h5	0x9b05688c
g	h6	0x1f83d9ab
h	h7	0x5be0cd19

7. Menentukan koefisien (k) : Koefisien yang digunakan adalah koefisien yang sudah ditetapkan sesuai standar SHA – 2 untuk SHA – 256, koefisien ini akan digunakan dalam perhitungan dalam proses iterasi dan disimpan dalam bentuk *array* sebagai berikut:

	1	2	3	4	5	6	7	8
1	0x428a2f98	0x71374491	0xb5c0fbcf	0xe9b5dba5	0x3956c25b	0x59f111f1	0x923f82a4	0xab1c5ed5
2	0xd807aa98	0x12835b01	0x243185be	0x550c7dc3	0x72be5d74	0x80deb1fe	0x9bdc06a7	0xc19bf174
3	0xe49b69c1	0xefbe4786	0x0fc19dc6	0x240ca1cc	0x2de92c6f	0x4a7484aa	0x5cb0a9dc	0x76f988da
4	0x983e5152	0xa831c66d	0xb00327c8	0xbf597fc7	0xc6e00bf3	0xd5a79147	0x06ca6351	0x14292967
5	0x27b70a85	0x2e1b2138	0x4d2c6dfc	0x53380d13	0x650a7354	0x766a0abb	0x81c2c92e	0x92722c85
6	0xa2bfe8a1	0xa81a664b	0xc24b8b70	0xc76c51a3	0xd192e819	0xd6990624	0xf40e3585	0x106aa070
7	0x19a4c116	0x1e376c08	0x2748774c	0x34b0bcb5	0x391c0cb3	0x4ed8aa4a	0x5b9cca4f	0x682e6ff3
8	0x748f82ee	0x78a5636f	0x84c87814	0x8cc70208	0x90befffa	0xa4506ceb	0xbef9a3f7	0xc67178f2

Gambar 3 Array Koefisien

8. Iterasi : Iterasi ini akan dilakukan sebanyak 64 kali dengan nilai awal yang berasal dari *working* variabel dan iterasi 0 – 63 mengikuti rumus sebagai berikut:

$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

.....(6)

$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

.....(7)

$$\mathrm{Ch} = (\mathrm{E} \wedge \mathrm{F}) \oplus (\sim \mathrm{E} \wedge \mathrm{G}) \quad \text{.....(8)}$$

$$\mathrm{Ma} = (\mathrm{A} \wedge \mathrm{B}) \oplus (\mathrm{A} \wedge \mathrm{C}) \oplus (\mathrm{B} \wedge \mathrm{C}) \quad \text{.....(9)}$$

$$T_1 = h + \Sigma_1 + Ch + k_{ij} + W_i \quad \text{.....(10)}$$

$$T_2 = \Sigma_0 + Ma \quad \text{.....(11)}$$

$$h = g \quad \text{.....(12)}$$

$$g = f \quad \text{.....(13)}$$

$$f = e \quad \text{.....(14)}$$

$$e = d + T_1 \quad \text{.....(15)}$$

$$d = c \quad \text{.....(16)}$$

$$c = b \quad \text{.....(17)}$$

$$b = a \quad \text{.....(18)}$$

$$a = T_1 + T_2 \quad \text{.....(19)}$$

9. Menambahkan: Pada proses ini hasil akhir iterasi akan ditambahkan dengan nilai *hash* awal dengan persamaan:

$$h0 = h0 + a \quad \text{.....(20)}$$

$$h1 = h1 + b \quad \text{.....(21)}$$

$$h2 = h2 + c \quad \text{.....(22)}$$

$$h3 = h3 + d \quad \text{.....(23)}$$

$$h4 = h4 + e \quad \text{.....(24)}$$

$$h5 = h5 + f \quad \text{.....(25)}$$

$$h6 = h6 + g \quad \text{.....(26)}$$

$$h7 = h7 + h \quad \text{.....(27)}$$

10. *Message Digest*: Hasil akhir *message digest* didapat dari penggabungan 8 variabel yang sudah di proses dengan persamaan:

$$h0 \parallel h1 \parallel h2 \parallel h3 \parallel h4 \parallel h5 \parallel h6 \parallel h7 \quad (28)$$

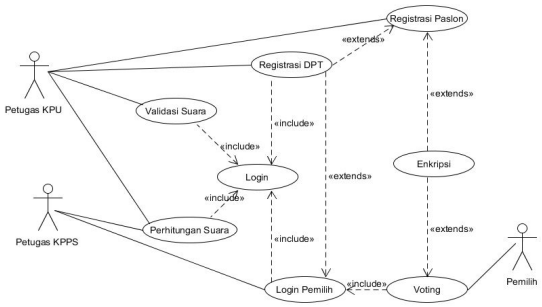
2. PERANCANGAN

Dalam melakukan perancangan sistem *e – voting* dibutuhkan beberapa persiapan perangkat keras dan perangkat lunak sebagai berikut :

1. Kebutuhan Perangkat Keras *(Hardware)*
   Analisis yang telah dilakukan dalam kebutuhan *hardware* untuk pengembangan sistem agar berjalan baik, disarankan mempunyai spesifikasi sebagai berikut :
   a. Processor 1.5 GHz
   b. Hardisk 500 Gb
   c. RAM 4 Gb.
   d. Printer
2. Kebutuhan Perangkat Lunak *(Software)*
   Analisis dalam kebutuhan *software* untuk pengembangan disarankan agar aplikasi dapat berjalan dengan baik. Kebutuhan *software* itu sebagai berikut:
   a. Windows 8
   b. Java

Use Case Diagram

Untuk menjelaskan hubungan setiap pengguna dengan sistem dan fungsi dari masing – masing bagian sistem akan digunakan *use case* diagram dengan menggunakan *software* UMLet, Setiap pengguna akan melakukan Login untuk bisa masuk kedalam sistem. Untuk petugas KPU dan Petugas KPPS bisa langsung login pada sistem *e -voting* namun untuk pemilih harus dibukakan dahulu menu login pemilih oleh petugas KPPS, ini berguna untuk tindak pencegahan agar setiap pemilih hanya bisa login jika sudah melalui pendaftaran di TPS yang sudah disediakan selama Pilwali berlangsung. detail diagram terdapat pada gambar berikut ini:



Gambar 4 Use Case *E - Voting*

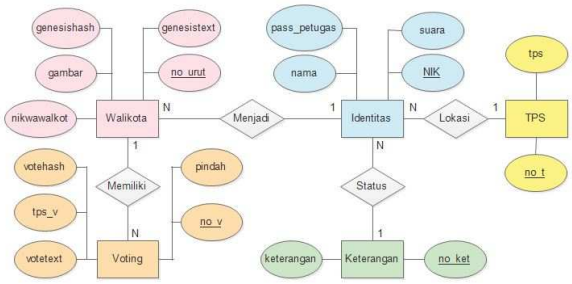
Pada tabel di bawah terdapat penjelasan mengenai fungsi dari masing – masing use case yang digunakan dalam sistem *e – voting* sehingga dapat digunakan sesuai aktornya.

Tabel 2 Deskripsi *Use Case*

No.	Nama	Deskripsi
1	*Login*	Digunakan untuk masuk kedalam sistem.
2	Registrasi DPT	Untuk memasukkan data DPT pada sistem.
3	Registrasi Paslon	Untuk memasukkan data Paslon dan membentuk genesis pada sistem.
4	Validasi Suara	Untuk memvalidasi hasil *voting* yang telah dilakukan.
5	Perhitungan Suara	Untuk menghitung perolehan suara tiap Paslon di TPS.
6	*Login* Pemilih	Untuk menentukan apakah pemilih dapat masuk ke menu *voting* atau tidak.
7	Voting	Untuk melakukan pemilihan Paslon.
8	Enkripsi	Untuk mengenkripsi data Paslon dan data hasil *voting*.

Entity Relationship Diagram

Pada bagian ini akan digunakan ERD untuk menggambarkan rancangan *database* yang akan digunakan dalam sistem beserta hubungan dari masing – masing *entity*. Pada gambar 3.33 terdapat 5 *entity* yang masing – masing memiliki atribut. *Entity* TPS akan menyimpan data TPS dengan No. TPS sebagai *primary key* yang menghubungkannya dengan *entity* Identitas secara *one to many* karena satu TPS bisa digunakan oleh lebih dari satu identitas. *Entity* keterangan akan berhubungan dengan *entity* identitas dan berfungsi untuk menyimpan data keterangan yang menerangkan status dari pemilik identitas. *Entity* identitas sendiri akan menyimpan data dari e – KTP yang berupa NIK sebagai *primary key* dan nama beserta *password* untuk Petugas dan suara untuk kesempatan *voting*. *Entity* ini akan berhubungan dengan *entity* walikota secara *one to many* karena data walikota akan diambil dari *entity* identitas.



Gambar 5 ERD *E - Voting*

Entity walikota akan berisi data No. urut Paslon yang ditentukan KPU, NIK wakil walikota yang sudah terdaftar di *entity* identitas, genesis *hash* dan genesis *text* yang berisi enkripsi dari data Paslon dan gambar Paslon untuk proses *voting*. Pada *entity voting* akan berhubungan dengan *entity* walikota secara *one to many* sehingga setiap walikota akan memiliki *votingnya* masing – masing, hal ini juga membuat hasil *voting* tidak bisa dihubungkan dengan *entity* identitas secara langsung. Pada *entity voting* ini akan tersimpan *No. voting,* enkripsi *voting* dan *plain textnya,* dan tempat TPS beserta keterangan Pindah TPS.

3. IMPLEMENTASI

Setelah tahap analisa dan perencangan terhadap sistem dilakukan, maka sistem tersebut siap diterapkan atau diimplementasikan. Tahap implementasi sistem ini merupakan tahap meletakkan perancangan sistem ke dalam bentuk coding bahasa pemrograman selain implementasi dalam aplikasi juga dalam dunia nyata.

Implementasi Antar muka

Dalam sub bab ini akan dijelaskan tampilan – tampilan pada sistem e – voting seperti dibawah ini :

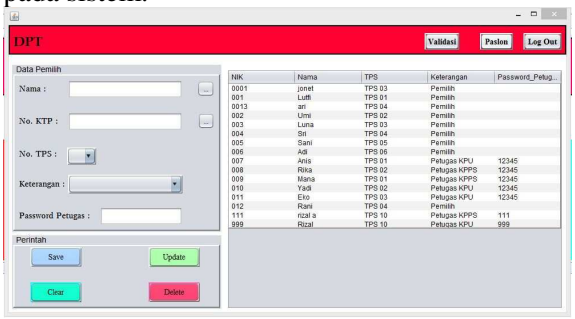
1. Halaman Login

Sesuai dengan namanya, halaman Log in ini petugas akan memasukkan username dan password untuk melakukan akses kedalam sistem.

Gambar 6 Menu Login

2. Halaman Registrasi DPT

Pada halaman ini petugas KPU akan melakukan registrasi data DPT pada sistem *e – voting* sehingga tiap pemilih bisa melakukan login pada sistem.



Gambar 7 Menu Registrasi DPT

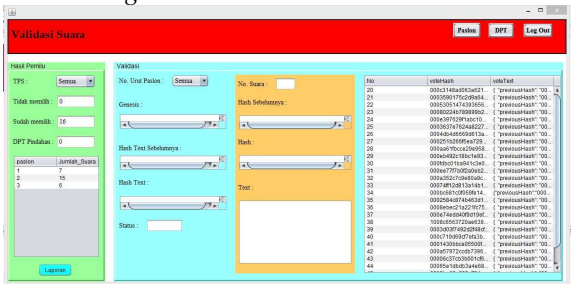
3. Halaman Regitrasi Paslon

Pada menu ini petugas KPU akan meregistrasikan data Paslon dan melakukan enkripsi untuk membuat blok genesis dari setiap Paslon.

Gambar 8 Menu Registrasi Paslon

4. Halaman Validasi

Pada halaman ini petugas KPU akan melakukan perhitungan suara TPS dan melakukan validasi hasil *voting*.



Gambar 9 Menu Validasi

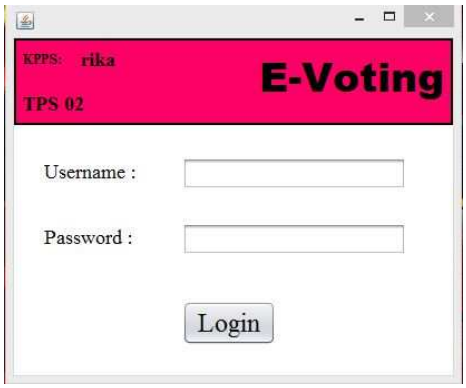
5. Halaman Perhitungan Suara

Pada menu ini hanya bisa diakses oleh petugas KPPS untuk melakukan perhitungan suara di TPS yang dijaganya.

Gambar 10 Menu Perhitungan Suara

6. Halaman Login Pemilih

Menu ini bisa diakses oleh petugas KPPS namun yang bisa log in hanyalah pemilih, karena menu ini akan membuka akses kemenu *voting*. Pada menu ini terdapat data petugas KPPS yang melakukan akses sehingga setiap pemilih dapat melakukan konfirmasi.



Gambar 11 Menu Login Pemilih

7. Halaman Voting

Pada menu ini pemilih akan melakukan *voting*, terdapat foto Paslon yang dapat dipilih dan identitas pemilih juga petugas KPPS yang akan dienkripsi bersama sehingga data hasil *voting* akan sulit dirubah.

Gambar 12 Menu *Voting*

Analisa Data

Untuk mendapatkan tanggapan terhadap sistem *e – voting* ini, maka dilakukan uji coba oleh responden sebanyak 20 orang yang didapat hasil sebagai berikut.

Tabel 3 Hasil Kuesioner

Responden	Pertanyaan				
	A	B	C	D	E
1	5	4	5	4	3
2	4	3	4	5	4
3	3	4	3	4	4
4	4	5	3	4	3
5	3	4	5	3	3
6	4	4	3	3	4
7	4	4	3	4	4
8	4	3	5	4	4
9	3	3	4	5	4
10	4	4	5	4	5
11	5	3	4	5	4
12	4	5	3	4	5
13	4	3	4	5	4
14	5	4	4	5	5
15	3	3	5	5	5
16	4	4	4	3	4
17	4	4	3	4	5
18	4	4	5	5	5
19	3	3	4	4	4
20	4	4	3	4	4
Total	78	75	79	84	83

4. PENUTUP

Kesimpulan

Berdasarkan penelitian yang telah dilakukan maka didapatkan kesimpulan sebagai berikut ini:

1. Untuk membuat sistem *e – voting* dengan metode enkripsi blockchain diperlukan proses sebagai berikut:
   1. Melakukan kajian pustaka dan studi lapangan mengenai sistem Pilwali yang sudah berjalan untuk menemukan permasalahan yang ada.
   2. Melakukan perancangan sistem *e – voting* untuk mengatasi permasalahan yang ditemukan dengan cara membuat DFD, *Use Case* Diagram, *Activity* Diagram,

Sequence Diagram, ERD, perancangan *database* dan perancangan *user interface*.

3. Membuat desain sistem *e – voting* berdasarkan perancangan sistem yang telah dibuat.
4. Melakukan uji coba sistem dengan melibatkan masyarakat sebagai penguji dan melakukan pengisian kuesioner untuk mengetahui kelayakan sistem.

2. Untuk melakukan pengujian kelayakan sistem *e – voting* yang telah dibuat adalah sebagai berikut:
   1. Memilih 20 responden dari penduduk Kota Mojokerto untuk melakukan uji coba sistem *e – voting* dan mengisi kuesioner yang telah disediakan.
   2. Melakukan pengumpulan dan melengkapi kuesioner.
   3. Melakukan perhitungan jawaban kuesioner.
   4. Berdasarkan dari hasil kuesioner yang telah diisi oleh responden didapat nilai sebesar 79,8% yang jika dicocokkan dengan tabel kategori kelayakan diperoleh nilai Layak. Sehingga dapat ditarik kesimpulan bahwa sistem *e – voting* dengan metode enkripsi ini Layak untuk digunakan.

Saran

Berdasarkan penelitian yang dilakukan maka diperoleh beberapa saran untuk pengembangan lebih lanjut dari sistem *e – voting* ini sebagai berikut:

1. Penambahan kemampuan sistem *peer – to – peer* untuk lebih memperkuat keamanan dari sisi server.
2. Perubahan sistem ke perangkat *mobile* sehingga sistem *e – voting* jadi lebih bisa menghemat biaya dan waktu.
3. Penggunaan teknologi *fingerprint* , *voice recognition* atau *face detection* untuk proses autentifikasi pemilih.

DAFTAR PUSTAKA

Ahmad, T. *et. al*. (2013). *Fingerprint – based Authentication And Cryptography In An E – Voting System*. Vol.02. Surabaya: Jurnal Manajemen Informatika.

Alan, D.S. dan John, S.C. (2005). *Revolutionising the voting process through online strategies*. dari: https://doi.org/10.1108/14684520510628909.

Andayani, D. (2018*). KPU: 9 Daerah Lakukan Pemungutan Suara Ulang*. Disitasi pada tanggal 29 Juni 2018. dari: https://m.detik.com/news/berita/4088159/_kpu-9-daerah-lakukan-pemungutan-suara-ulang.

Ayed, A.B. (2017). *A Conceptual Secure Blockchain-Based Electronic Voting System*, Vol.9. Internasional Journal of Network Security & Its Applications.

Azis, M.F. (2005). *Object Oriented Programming Php 5*. Elex Media Komputindo.

Booch, *et. al*. (2007). *Object-Oriented Analysis and Design with Applications*, 3rd Edition. Addison-Wesley *Professional.*

Brady, M. dan Loonam, J. (2010). *Exploring the use of entity relationship diagramming as a technique to support grounded theory inquiry*. Bradford: Emerald Group.

Bruza, P.D. (1993). *The Semantics of Data Flow Diagrams*. University of Nijmegen.

Cachin dan Vukolić. (2017). *Blockchain Consensus Protocols in the Wild.*

Chen, P. *(1976). The Entity-Relationship Model - Toward a Unified View of*

Data. ACM Transactions on Database Systems.

Christian. (2017). *Desain Dan Implementasi Visual Cryptography Pada Sistem E-Voting Untuk Meningkatkan Anonymity*, Institut Teknologi Bandung.

Bennett, S. *et. al*. (2108). Glossary Of Key Terms. Disitasi 16 Agustus 2018. dari: http://highered.mheducation.com/sites/0077110005/student_view0/glossary.html.

Indonesia, U.-U. R. (2011). *Undang Undang RI No. 15 Tahun 2011 Tentang Penyelenggara Pemilihan Umum.* Disitasi pada tanggal 9 Juni 2018. dari: http://www.dpr.go.id/dokjdih/document/uu/UU_2011_15.pdf.

Ibrahim, *et. al*. (2000). *Pembelajaran Kooperatif*. Surabaya: University Press.

KPU. (2016). *Peraturan Komisi Pemilihan Umum Republik Indonesia Nomor 4 Tahun 2016.* Disitasi pada tanggal 29 Juni 2018. dari: http://www.mahkamahkonstitusi.go.id/public/content/jdih/PKPU 4 2016.pdf.

KPU. (2017). *Panduan Pelaksanaan Pemungutan dan Penghitungan Suara di TPS PILKADA 2017.*

Muharram, A.T. dan Satrya, F. (2015). *Rancang Bangun Sistem E-Voting Menggunakan Protokol Two Central Facilities* (Vol.15). Jakarta: Jurnal Informatika.

Munir, A.Q. dan Utari, E.L. (2016). *Pemanfaatan E-KTP Untuk Proses Pemungutan Suara Pemilihan Umum Di Indonesia Menggunakan Sistem E-Vote*. Yogyakarta: STMIK AMIKOM.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disitasi pada tanggal 18 Juni 2018. dari: https://doi.org/10.1007/s10838-008-9062-0.

Niemeyer, P. dan Leuck, D. (2013). Learning Java. Sebastapol: O'Reilly Media, Inc.

Pahlevi, Indra. (2015). *Sistem pemilu di Indonesia : antara proporsional dan mayoritarian.* Jakarta Pusat: P3DI Setjen DPR Republik Indonesia dan Azza Grafika.

Ramdhani, J. (2017). *Bawaslu Temukan Pelanggaran Pemilih Gunakan Formulir C6 dan A5 Palsu.* Disitasi pada tanggal 29 Juni 2018. dari: https://news.detik.com/berita/d-3425720/bawaslu-temukan-pelanggaran-pemilih-gunakan-formulir-c6-dan-a5-palsu.

Roby, N. (2017). *Application of Blockchain technology In Online Voting*. University of Maryland: RSA Conference Security Scholar.

Rokhman, A. (2011). *Prospek dan Tantangan Penerapan E-Voting di Indonesia,* dari Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia (pp. 1–11).

Tammam, A.G. *et. al*. (2016). *Fungsi Hash dan Algoritma SHA – 256*. Kediri: Universitas Nusantara PGRI.

Valade, J.B.B. (2008). *PHP & MySQL Web Development All-in-One Desk*

Reference For Dummies. Canada: Wiley Publishing Inc.

Wijaya, D.A. (2016). *Bitcoin Tingkat Lanjut*.

Zamora, *et. al*. (2005). *Serine peptidase inhibitors, the best predictor of beef ageing amongst a large set of quantitative variables*.