Implementasi Blockchain: Studi Kasus e-Voting

Satria Damai Kurnia Hu, Henry Novianus Palit, Andreas Handojo
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jln. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
E-mail : satria.dkh@gmail.com, hnpalit@petra.ac.id, handojo@petra.ac.id

ABSTRAK

Voting atau pemungutan suara telah menjadi salah satu metode yang digunakan manusia untuk menentukan keputusan dalam sebuah hal. Voting juga sering digunakan dalam menentukan hal-hal yang sangat penting, seperti menentukan wakil-wakil rakyat, atau menentukan pemimpin baru. Di samping itu, saat ini pemungutan suara masih dilakukan dengan cara konvensional, yaitu menggunakan kertas dalam melakukan pembuatan ballot, pencoblosan, dan perhitungan suara. Hal ini dapat mengakibatkan terjadinya human error yang mempengaruhi hasil pemungutan suara dan dapat merugikan pihak tertentu. Selain itu, pemungutan suara yang dilakukan dengan teknologi komputer juga mempunyai masalah tertentu. Banyak pihak yang meragukan keamanan dari vote yang mereka lakukan, apakah benar masuk dan terhitung di akhir pemungutan suara, atau tidak.

Untuk menjawab persoalan tersebut, dirancang suatu sistem pemungutan suara elektronik dengan memanfaatkan teknologi Blockchain dalam aplikasi berbasis website. Dengan memanfaatkan teknologi ini, data pemungutan suara yang telah dilakukan tidak dapat diubah, digandakan ataupun dihapus. Sehingga dapat meningkatkan keamanan dari pemungutan suara. Selain itu, teknologi ini juga dapat menjaga kerahasiaan dari pihak yang melakukan pemungutan suara. Aplikasi ini juga membantu proses pemungutan suara agar lebih mudah dalam hal pengelolaan pihak terkait, pemungutan suara, hingga perhitungan suara.

Dari penelitian dan pengujian sistem yang telah dibuat, aplikasi dapat membantu memudahkan penyelenggaraan pemungutan suara. Teknologi blockchain yang digunakan mampu membantu menyimpan data hasil pemungutan suara yang transparan dan dapat diakses oleh publik. Teknologi ini juga membantu menjaga kerahasiaan dari voter. Data pemungutan suara juga tidak dapat diubah, digandakan atau dihapus. Selain itu, teknologi blockchain juga membantu melakukan verifikasi dan memilah data vote yang valid.

Kata Kunci: *Blockchain*, sistem *e-voting*, keamanan data vote.

ABSTRACT

Voting has become one of the methods that used by humans to determine decisions. Voting is also often used in determining things that are very important, such as determining people's representatives, or determining new leaders. In addition, currently voting is still done in conventional way, namely using paper in making ballot, voting, and tallying votes. These can lead to human error that affects the results of voting and can harm certain parties. In addition, voting carried out with computer technology also has certain problems. Many parties doubted the security of the votes they made, whether its entered and counted to the result, or not.

To answer these problems, an electronic voting system was designed by utilizing Blockchain technology in website-based applications. By utilizing this technology, the voting data that has been carried *out cannot be changed, duplicated or deleted. So that it can improve the security of voting system. In addition, this technology can also maintain the confidentiality of the parties who carry out the voting. This application also helps the voting process to be easier in terms of management of related parties, voting, and tallying votes.*

From the research and testing systems that have been done, the application can help facilitate the implementation of voting. The blockchain technology that used is able to help store voting data that is transparent and accessible to the public. This technology also helps maintain the confidentiality of voters. The voting data also cannot be changed, duplicated or deleted. In addition, blockchain technology also helps verify and filter validated votes data.

Keywords: *Blockchain, e-voting system, vote data security.*

1. PENDAHULUAN

Electronic voting (*e-Voting*) pertama kali diperkenalkan oleh *David Shaumm* pada awal 1980. Sistem yang digunakan adalah dengan *cryptography-key* yang membantu para *voter* untuk tetap tidak terdeteksi. Estonia adalah negara yang pertama kali menggunakan *electronic voting* hanya menggunakan *internet* dan kartu tanda penduduk elektronik (*e-KTP*). Negara selanjutnya yang mengimplementasikan *electronic voting* adalah Norwegia. Sistem yang dibuat mirip seperti yang dimiliki Estonia, tetapi terpaksa tidak diteruskan karena banyak pihak yang takut akan keamanan dari sistem itu. Washington D. C. juga mengembangkan *electronic voting* pada tahun 2010. Tetapi banyak sekali masalah keamanan pada saat melakukan pengujian pada sistemnya. Sehingga proyek tersebut tidak pernah diimplementasikan. [1]

Blockchain merupakan teknologi dasar dari sebuah desain arsitektur *cryptocurrency Bitcoin* yang diciptakan oleh Satoshi Nakamoto pada tahun 2008. Ini merupakan bentuk dari *distributed database* yang mana berisi dari transaksi-transaksi yang disimpan dalam sebuah *block* data. Setiap *block* memiliki *hash* unik yang dihasilkan dari isi dari *block* itu sendiri. Setiap *block* menyimpan *hash* dari *block* sebelumnya sehingga membentuk sebuah rantai (*chain*) yang disimpan di setiap *node* dalam *Peer-to-peer network.*

Oleh karena itu, sistem dan aplikasi yang akan diciptakan ini akan menjawab beberapa kebutuhan pemungutan suara dengan implementasi dari teknologi *blockchain*. Sistem tersebut akan menjawab *transparency*, yaitu data yang disimpan bersifat terbuka untuk publik, sehingga meningkatkan keadilan dan kebenaran. *Anonymity*, yaitu hanya *voter* itu sendiri yang tahu informasi mengenai *vote* dan semua *ballot* yang terkumpul tidak ada hubungannya dengan *voter*. *Dependability*, yaitu setiap *vote* akan dihitung dan tidak dapat diganti, digandakan ataupun dihapus, serta mengeluarkan hasil yang dapat dipercaya. *Eligibility*, yaitu hanya *user* yang terverifikasi dan memiliki hak suara yang dapat membuat *ballot* dan melakukan *vote*. *Verifiability*, yaitu sistem bersifat terbuka untuk dapat diperiksa kebenarannya dari prosedur sistem hingga hasil yang dikeluarkan. [4]

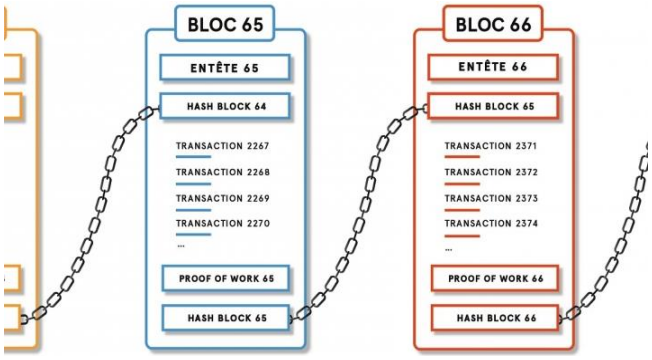
2. TINJAUAN PUSTAKA

Dalam penelitian yang dilakukan Azwanti, membahas mengenai permasalahan dimana setiap elemen masyarakat memiliki kegiatan dan kesibukkan yang berbeda-beda. Sehingga pemberian informasi mengenai pemungutan suara menjadi tidak tersampaikan dengan baik kepada masyarakat, dan menimbulkan masalah dimana pemungutan suara tersebut menjadi tidak transparan. Oleh karena itu, sistem pemungutan elektronik (*e-voting*) dirancang untuk mengurangi permasalahan dalam proses pemungutan suara sehingga dapat meminimumkan kecurangan, dan memberikan sebuah media penampung data pemungutan suara. [2]

Dalam penelitian Purwati, membahas mengenai masalah-masalah yang sering terjadi pada proses pemungutan suara antara lain: (1) Banyak data warga yang tidak tercatat dalam pemungutan suara. (2) Banyak warga yang melakukan kesalahan dalam pemberian hak suara, sehingga suara menjadi tidak sah. (3) Proses perhitungan suara berjalan dengan lambat. (4) Proses kecurangan yang dapat terjadi. Oleh karena itu, untuk menanggapi dan mengurangi permasalahan yang terjadi, dibuat sebuah sistem pemungutan suara secara *online* atau *e-voting*. [8]

2.1 *Blockchain*

Merupakan sebuah *list of record* yang disebut *blocks*, yang saling terhubung dan diamankan dengan metode *cryptography*. Setiap *block* memiliki *cryptographic-hash* yang berbeda. *Hash* tersebut dibentuk dari isi *block* itu sendiri. Isi *block* tersebut antara lain *timestamp*, beberapa transaksi, dan *hash* dari *block* sebelumnya sehingga membentuk sebuah rantai (*chain*) dari *blocks*. Ilustrasi struktur *blockchain* dapat dilihat melalui Gambar 1.



Gambar 1. Ilustrasi *blockchain* [6]

2.2 *Distributed database and decentralized system*

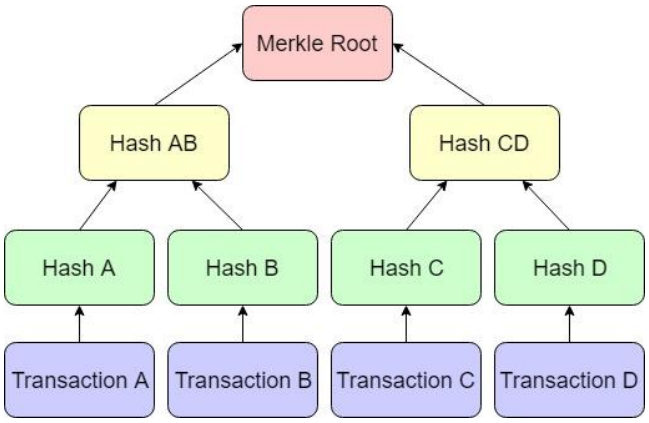
Distributed database merupakan sebuah metode penyimpanan dimana *storage device* tidak terpasang pada sebuah komputer, melainkan beberapa komputer. Beberapa komputer tersebut dapat terkoneksi pada sebuah *storage device* maupun beberapa *storage device* yang berbeda, yang dihubungkan melalui *network*. Metode ini membuat *database* menjadi transparan terhadap *users* yang memakainya.

Decentralized system merupakan desain sistem yang terdiri dari beberapa komputer yang disebut *nodes* dalam sebuah jaringan dan memiliki kewenangan untuk mengatur fungsi sendiri untuk mencapai *goal* dari sistem pusat. Setiap *node* dapat memiliki sistem sendiri dan menjalankan fungsi tertentu untuk memberi kontribusi pada sistem global (*main system*). [3] Ilustrasi perbedaan sistem *centralized*, dan *decentralized* dapat dilihat pada Gambar 2.

Gambar 2. Ilustrasi Sistem [7]

2.3 *Merkle Tree*

Merupakan sebuah struktur data *tree* dimana setiap *leaf node* menyimpan *hash* dari isi datanya dan *node* lain (*non-leaf node*) menyimpan *hash* dari *child nodes* yang dia miliki. Metode ini efektif untuk meningkatkan keamanan dari struktur penyimpanan data yang besar, karena mampu melakukan verifikasi dari setiap *node* yang ada dalam *tree*. [5] Ilustrasi struktur *merkle tree* dapat dilihat pada Gambar 3.



Gambar 3. Ilustrasi Merkle Tree

2.4 Multichain (*Blockchain Platform*)

Multichain merupakan sebuah *tools* untuk membantu pengguna dalam membangun dan menjalankan aplikasi *blockchain*. *Tools* ini dapat membantu dalam mengelola satu atau lebih *blockchain* yang dijalankan pada sebuah komputer. Multichain yang telah berjalan pada sebuah komputer akan menjadi sebuah *node*. Multichain dapat mengatur *behavior* dari *blockchain* hingga

hubungan antar *node* pada *blockchain network*. *Tools* ini juga mampu melakukan *proof-of-work consensus* yang dijalankan pada *blockchain node*, yang sering dikenal dengan istilan *mining block*.

Multichain juga menyediakan fungsi yang dapat dipanggil oleh pengguna untuk mengelola *blockchain* dari aplikasi lain ataupun dari luar *node*. Fungsi yang disediakan adalah JSON-RPC API *call*. Fungsi ini dapat dipanggil dengan menggunakan metode HTTP *POST* dengan autentikasi HTTP *Basic*. Dari fungsi ini, pengguna dapat mengelola *blockchain* dari aplikasi yang sedang dibangun sesuai dengan kebutuhan.

2.5 *Voting Values on e-Voting*

Electronic Voting yang dibuat haruslah mendukung dengan sifat pemungutan suara secara umum. Berikut sifat dan kebutuhan pemungutan suara elektronik secara umum yang telah dilakukan dalam penelitian sebelumnya.

Dalam penelitian yang dilakukan oleh Ayed tahun 2017, sistem pemungutan suara elektronik harus memiliki nilai *authentication*, *anonymity*, *accuracy*, dan *verifiability*. *Authentication* berarti hanya beberapa orang yang terdaftar yang dapat melakukan *vote*. *Anonymity* berarti identitas *voter* tidak boleh terhubung dengan *ballot* yang dibuat. *Accuracy* berarti *ballot* harus terhitung, dan tidak boleh diganti, digandakan atau dihapus. *Verifiability* berarti sistem seharusnya dapat diverifikasi apakah semua *vote* telah terhitung dengan benar atau tidak.

Dalam penelitian yang dilakukan oleh Lee, James, Ejeta, dan Kim pada tahun 2016, pemungutan suara elektronik memiliki kebutuhan penting seperti *robustness*, *anonymity* dan *transparency*. *Robustness* berarti sistem haruslah tahan terhadap perubahan data. *Anonymity* berarti *voter* melakukan *vote* dengan rahasia dan tidak diketahui identitasnya. *Transparency* berarti data yang disimpan bersifat transparan dan terbuka untuk publik.

Dalam penelitian yang dilakukan oleh Liu dan Wang pada tahun 2017, pemungutan suara elektronik yang diusulkan membutuhkan nilai *public verifiability*, *individual verifiability*, *dependability*, *consistency*, *auditability*, *anonymity*, dan *transparency*. *Public verifiability* berarti seluruh pihak terkait dapat memeriksa prosedur dan hasil yang dikeluarkan. *Individual verifiability* berarti *voter* yang melakukan pemungutan suara dapat memeriksa prosedur yang dilakukan dan *vote* yang dia lakukan apakah sudah masuk dan terhitung atau tidak. *Dependability* berarti sistem yang dibuat memiliki ketahanan terhadap serangan dari luar. *Consistency* berarti setiap suara yang disimpan memiliki data yang sama dan menghasilkan hasil yang sama. *Auditability* berarti seluruh prosedur yang tersimpan dapat diaudit. *Anonymity* berarti hanya *voter* itu sendiri yang tahu informasi dari *ballot*-nya, dan setiap *ballot* yang telah tersimpan tidak ada berkaitan dengan seseorang. *Transparency* berarti seluruh prosedur berisfat terbuka untuk publik.

3. DESAIN SISTEM

3.1 Analisa sistem

Sifat yang dimiliki oleh *blockchain* ini sangat mendukung dalam pencapaian sistem pemungutan suara elektronik yang transparan dan dapat diverifikasi kebenarannya. Sehingga sistem yang disusun dapat memiliki nilai sebagai berikut.

Transparency. Blockchain merupakan *public ledger*, dimana setiap orang dapat melihat atau bahkan menggandakan data yang ada pada *blockchain*.

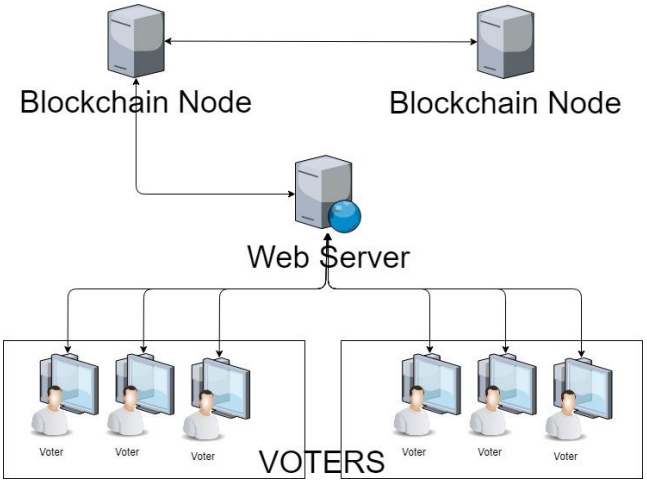
Dependability. Blockchain merupakan *block-block* yang terhubung dengan teknik kriptografi dan memiliki sistem *decentralized* dimana setiap *block* terdistribusi ke seluruh *node*. Karena itu, untuk mengubah sebuah data pada *blockchain* memiliki tingkat kesulitan yang sangat tinggi dan hampir tidak mungkin. Oleh karena itu, setiap *vote* pasti akan dapat dihitung tanpa *vote* tersebut digandakan, diubah, ataupun dihapus.

Eligibility. Hanya *user* yang terverifikasi dan memiliki hak untuk dapat melakukan *vote*. Untuk dapat menambahkan *block* pada *blockchain*, maka dibutuhkan transaksi yang sah. Transaksi dinyatakan sah apabila terdapat *digital signature* pada transaksi tersebut. Hal tersebut dapat dilakukan hanya oleh *user* yang memiliki sepasang kunci yang terverifikasi oleh *blockchain*.

Verifiability. *Blockchain* merupakan *public ledger* dan setiap transaksi yang dilakukan dapat dilihat kebenarannya dari detail transaksi tersebut.

Anonymity. Hanya *voter* itu sendiri yang dapat melihat isi dari *vote* tersebut. Protokol yang direncanakan ini menggunakan *multi-signature* untuk *digital signature*, dimana alamat pengirim dari *vote* merupakan alamat *virtual* yang disusun dan dimiliki oleh beberapa *user*. Sehingga *voter* yang melakukan *vote* tidak dapat diketahui secara langsung.

3.2 Arsitektur sistem

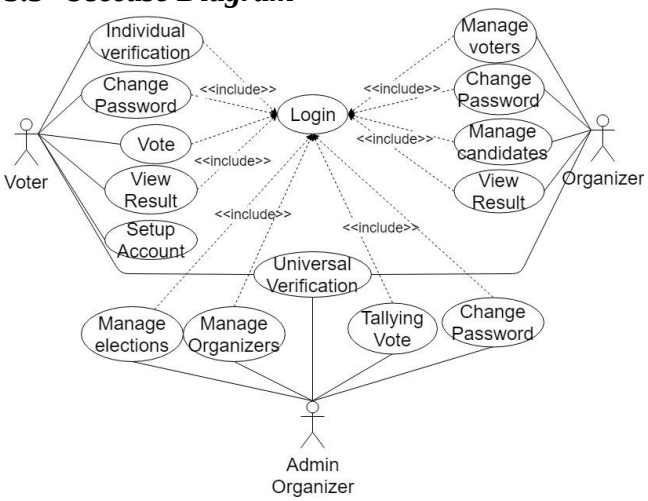


Gambar 4. Arsitektur Sistem

Dari Gambar 4 menjelaskan mengenai rancangan sistem arsitektur yang akan diterapkan pada Pemilu Raya Universitas Kristen Petra. Dalam sistem arsitektur ini memiliki komponen berupa *Blockchain Node*, *Webserver* dan *Client Computer*. Komponen *client computer* merupakan komputer yang dipakai pada tempat pemilihan umum untuk dipakai dalam melakukan pemungutan suara. Komputer *client* tersebut mengakses halaman *web* pada *webserver*. Segala data dan interaksi aplikasi *web* antara komputer client dan *webserver* menggunakan HTTP atau HTTP *method*. Komponen *webserver* merupakan aplikasi *web* yang menyediakan layanan untuk *voter* maupun *organizer* dalam melakukan proses pemungutan suara. *Webserver* menggunakan sebuah komputer (*centralized*) untuk mengatur semua aktivitas yang dilakukan dari komputer *client* (*voter*). *Webserver* juga terhubung dengan sebuah *database* lokal untuk menyimpan data yang dibutuhkan dalam pemungutan suara seperti data *election*, data *user* (*voter*, *candidate*, *organizer*) dan data pendukung lainnya. *Webserver* juga terhubung dengan sebuah *blockchain node* untuk melakuan *API call*. Komponen *blockchain node* tersebut menyediakan *API*

call dengan *JSON RPC method*. Komponen ini merupakan sebuah komputer dalam *peer-to-peer network* dari *blockchain*. *JSON RPC API call* tersebut dipakai oleh *webserver* untuk mengelola *blockchain* dalam memenuhi kebutuhan pemungutan suara. *Ballot* yang dihasilkan oleh *voter* (komputer *client*) akan disimpan ke dalam *blockchain* pada *blockchain node* oleh *webserver*.

3.3 *Usecase Diagram*



Gambar 5. *Usecase diagram*

Usecase diagram pada Gambar 5 mendeskripsikan aktor-aktor yang berperan dalam sistem yaitu *Admin Organizer*, *Organizer*, dan *Voter*. Setiap aktor tersebut memiliki fungsi dan peran yang berbeda-beda sesuai dengan kebutuhannya. Yang pertama adalah aktor *Organizer* (pihak penyelenggara), terdiri dari *usecase manage voters, change password, universal ballot verification, manage candidates*, dan *view result*. Yang kedua adalah aktor *Admin Organizer* (pihak admin dari penyelenggara), terdiri dengan *usecase change password, universal ballot verification, view result, manage elections, manage organizers,* dan *tallying vote*. Yang ketiga adalah aktor *Voter* (pihak yang melakukan pemungutan suara), terdiri dari *usecase view result, setup account, change password, vote,* dan *individual ballot verification*.

3.4 Desain Aplikasi

Desain *interface* dari *website application* disesuaikan dengan hak akses yang ada, yaitu *Admin Organizer*, *Organizer*, dan *Voter*. Setiap desain aplikasi yang ditujukan pada setiap hak akses memiliki perbedaan sesuai dengan fungsi dan kebutuhan. Desain aplikasi untuk *admin organizer* memiliki fungsi untuk mengelola pemungutan suara (*election*), mengelola data penyelenggara (*organizer*), dan mengelola data hak akses dari para *organizer* yang menjalankan pemungutan suara. Desain *interface* untuk *admin organizer* terdiri dari halaman *change password, view result, manage elections, manage organizers,* dan *manage access right.* Desain aplikasi untuk *organizer* memiliki fungsi untuk mengelola data *voter*, dan mengelola data *candidate* yang mengikuti pemungutan suara. Desain *interface* untuk *organizer* terdiri dari halaman *change password, view result, manage voters* dan *manage candidates*. Sedangkan desain aplikasi untuk *voter* memiliki fungsi untuk melakukan pemungutan suara, melihat dan memeriksa suara yang sudah dilakukan. Desain *interface* untuk *voter* terdiri dari halaman *change password, view result, vote* dan *individual ballot verification*. Selain itu, terdapat halaman yang dapat diakses oleh semua *user* antara lain halaman *login, register, setup account,* dan *universal ballot verification*. Halaman *login, register* dan *setup account* memiliki fungsi untuk membantu *user* dalam mengelola akun pada saat awal mengakses aplikasi. Halaman *universal ballot verification* memiliki fungsi untuk memeriksa suara yang sudah masuk ke dalam sistem.

4. HASIL IMPLEMENTASI

4.1 Simulasi

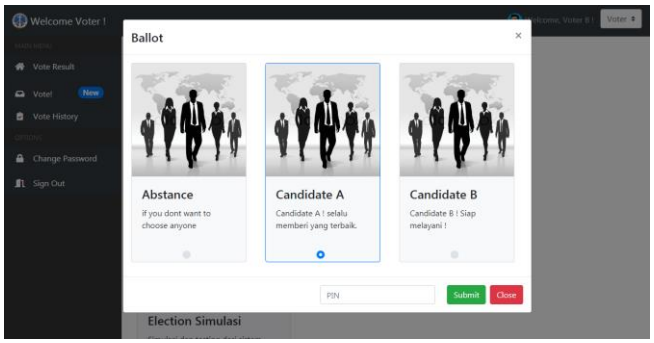
Sistem yang telah ada dilakukan pengujian dengan skenario tertentu, yakni sebuah pemungutan suara yang diikuti oleh beberapa *voter*. Pemungutan suara tersebut juga diselenggarakan oleh beberapa *organizer* dan diikuti oleh 2 *user* sebagai *candidate*. Pemungutan suara diselenggarakan dengan beberapa tahap, yaitu tahap persiapan, tahap pemungutan suara, tahap pemeriksaan suara dan tahap perhitungan suara.

4.1.1 Tahap Persiapan

Tahap persiapan dimulai dengan menambah sebuah pemungutan suara (*election*) ke dalam sistem. Lalu menambahkan 10 data *organizer* yang menyelenggarakan *election*. Selanjutnya, salah seorang *organinzer* tersebut menambahkan 2 data *candidate* yang mengikuti *election* dan 20 data *voter* yang berpartisipasi dalam *election* tersebut. Setiap *voter* yang akan mengikuti *election* dapat melakukan *setup account* terlebih dahulu untuk membuat *username*, *password*, dan *passphrase* yang akan digunakan untuk melakukan *vote*.

4.1.2 Tahap Pemungutan Suara

Tahap pemungutan suara dapat dimulai dengan menekan tombol *start election*. Pada tahap ini, *voter* dapat datang ke tempat pemungutan suara dan melakukan verifikasi kehadiran dengan kartu identitas. *Organizer* yang melakukan verifikasi kepada *voter* dapat meng-*update* kehadiran *voter* di dalam sistem. Dari 20 *voter* yang terdaftar akan dibuat 16 *voter* untuk dapat melakukan *vote* dengan valid, 4 *voter* tidak melakukan *vote* dan 2 *vote* tidak valid yang berasal dari luar *election* (*fraud*). Contoh *ballot* dapat dilihat pada Gambar 6.



Gambar 6. *Ballot*

Sedangkan, *vote* yang tidak valid dilakukan melalui *console*. Kondisi *vote* yang tidak valid yang dilakukan adalah *ballot* kosong yang sudah dibuat untuk *user* tertentu diberi *digital signature* oleh *user* yang bukan pemilik dari *ballot* tersebut. *Vote* yang tidak valid akan langsung ditolak oleh sistem.

Dilakukan juga 2 *vote* yang berasal dari luar sistem. *Vote* pertama adalah *vote* yang berisikan *multi-signature address* yang valid tetapi tidak tercatat oleh sistem. Yang kedua, *vote* yang dilakukan langsung tanpa *multi-signature address* dan dikirimkan ke

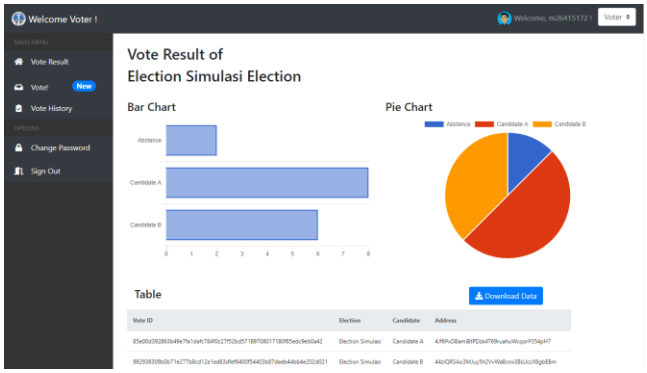
election address. Kedua *vote* tersebut dapat masuk ke dalam *blockchain*, namun dianggap tidak valid dan tidak akan terhitung menjadi hasil *election*.

4.1.3 Tahap Pemeriksaan Suara

Setelah pemungutan suara selesai, *election* dapat diakhiri dengan menekan tombol *stop election*. Pada tahap ini, diberikan waktu untuk sistem dapat memproses semua *vote*, memasukkan ke dalam *blockchain* dan validasi oleh *blockchain*. *Voter* juga dapat melakukan verifikasi *vote* yang sudah dilakukan melalui halaman *vote history*.

4.1.4 Tahap Perhitungan Suara

Pada tahap perhitungan suara, *admin organizer* dapat melakukan perhitungan suara yang sudah masuk melalui tombol *count votes*. Sistem akan melakukan perhitungan *vote* yang valid, dan disimpan ke dalam *database*. Hasil *vote* tersebut dapat dilihat melalui halaman *vote result* ketika *login*. Perhitungan *vote* seharusnya menghasilkan total 16 *vote* valid. Hasil pemungutan suara dapat dilihat pada Gambar 7.



Gambar 7. Hasil Pemungutan Suara

4.2 Analisa Sistem

4.2.1 Ballot valid

Ballot dalam sistem adalah sebuah *multi-signature address* pada *blockchain* yang terdiri dari 3 *address* yaitu dari *voter*, *organizer*, dan *blockhain node*. Selain itu, *ballot* tersebut juga telah diisikan sejumlah aset untuk dikirimkan ke alamat *blockchain* dari *election*. Kondisi tersebut merupakan *ballot* kosong dan siap diisikan oleh data *candidate* yang dipilih oleh *voter*. Sedangkan *ballot* yang valid adalah sebuah transaksi pada *blockchain* yang berisikan *multi-signature address* sebagai alamat pengirim, *election address* sebagai alamat penerima, berisi data *vote*, dan *digital signature* dari 3 *address* pada *multi-signature address* tersebut.

4.2.2 Transparency

Sistem yang dibuat mempunyai nilai *transparency*, berarti data yang ada pada sistem bersifat transparan dan dapat diverifikasi kebenarannya oleh publik. Ini berarti data dari *vote* yang tersimpan dalam *blockchain* dapat dibaca oleh publik.

Dalam sistem yang dibuat, konfigurasi *blockchain* sudah disesuaikan agar setiap orang yang ingin memiliki data *blockchain* tersebut dapat terhubung dengan *node* yang tersedia. Selain itu, terdapat fitur *universal ballot verification* yang berfungsi membantu dalam mencari data tertentu dalam *blockchain*. Setelah *election* selesai, juga terdapat fitur untuk mengunduh data *vote* yang berhasil terhitung dari *blockchain* secara publik.

4.2.3 Anonimity

Sistem yang dibuat mempunyai nilai *anonymity*, berarti isi dari setiap *vote* yang dilakukan oleh *voter* hanya diketahui oleh *voter* itu sendiri dan *ballot* yang ada berhubungan dengan *voter* tersebut. Ini berarti dari *ballot* yang ada tidak dapat diketahui siapa yang melakukan *vote* tersebut.

Dari sistem yang dibuat, setiap *voter* menggunakan *multi-signature address* sebagai alamat dari transaksi atau *vote* yang dilakukan. Penggunaan *multi-signature address* tersebut berfungsi untuk menghindari penggunaan alamat *blockchain* langsung milik *voter*. Sehingga untuk setiap *vote* yang dilakukan tidak terlihat siapa yang melakukan *vote* tersebut.

4.2.4 Dependability

Sistem yang dibuat mempunyai nilai *dependability*, berarti setiap *vote* yang dilakukan akan dihitung dan tidak dapat diubah, digandakan ataupun dihapus, serta mengeluarkan hasil yang sesuai dengan *vote* yang dilakukan. Ini berarti semua *vote* yang valid dan masuk ke dalam sistem, akan ikut dihitung untuk mengeluarkan hasil yang sesuai.

Dari sistem yang dibuat, ketika *user* melakukan *vote* yang valid akan langsung dimasukkan ke dalam *memory pool* dari *blockchain* untuk ditambahkan ke dalam sebuah *block*. Dan setiap *vote* yang sudah masuk ke dalam *blockchain* tidak dapat diubah, digandakan atau dihapus, karena untuk menambahkan sebuah *block* baru dibutuhkan komputasi tinggi untuk *proof-of-work consensus* dan setiap data saling terhubung dengan enkripsi tertentu yang merupakan sifat alami dari *blockchain*. Selain itu, perhitungan suara akan dilakukan dengan menyaring *vote* valid yang terdaftar dalam sistem. Sehingga, *vote* yang dilakukan oleh *voter* melalui aplikasi pasti akan terhitung dalam sistem.

4.2.5 Eligibility

Sistem yang dibuat mempunyai nilai *eligibility*, berarti hanya *user* yang terverifikasi dan memiliki hak suara yang dapat melakukan *vote*. Ini berarti *vote* hanya dapat dilakukan oleh orang yang sudah terverifikasi kebenarannya, dan tidak dapat diwakilkan.

Dalam sistem yang dibuat, setiap *user* memiliki *account* sendiri sebagai hak akses untuk masuk ke dalam sistem. Setiap *voter* yang akan melakukan *vote* sudah diberi kewenangan dan hak akses untuk masuk ke dalam sistem yang diatur oleh *organizer*. Selain itu, setiap *voter* yang akan melakukan *vote* juga memiliki sepasang *key* dari *blockchain* sebagai identitas dan hak suara dalam mengikuti *election*. *Voter* juga perlu untuk menunjukkan diri dan identitas pribadi kepada *organizer* untuk dapat melakukan *vote*. Sehingga, tidak dapat diwakilkan oleh siapapun.

4.2.6 Verifiability

Sistem yang dibuat mempunyai nilai *verifiability*, berarti *user* dapat memeriksa sendiri kebenaran dari *vote* yang dilakukan berhasil masuk ke dalam *blockchain* dan menyimpan data yang sesuai. Ini berarti *user* dapat memeriksa sendiri, apakah *vote* yang pernah dilakukan tetap memiliki data yang sama atau tidak dan telah masuk serta terhitung ke dalam *blockchain* atau tidak.

Dari sistem yang dibuat, setiap *user* diberi fitur untuk melakukan pengecekan dari *vote* yang sudah pernah dia buat. Ketika melakukan *vote*, data *vote* yang dilakukan oleh *voter* akan langsung disimpan dan dienkripsi oleh sistem, dengan tujuan agar *voter* dapat memeriksa kembali apakah data *vote* yang pernah dilakukan pertama kali dan dimasukkan ke dalam *blockchain*

berubah atau tidak. Selain itu, setelah melakukan perhitungan suara, data *vote* dapat diunduh dan dilakukan pencarian dari berdasarkan *vote ID* yang pernah dilakukan, apakah *vote* sudah masuk dan terhitung atau tidak.

4.2.7 Tallying Votes

Perhitungan dalam *blockchain* dilakukan dengan memilah *vote* valid dan tidak. *Vote* yang valid adalah *vote* yang dilakukan sekali, dan alamat pengirim tercatat ke dalam sistem. Selain itu, *vote* yang valid juga merupakan *vote* yang sudah termasuk ke dalam sebuah *block* dan dianggap *valid* oleh *blockchain*. Setiap *vote* yang memenuhi hal-hal tersebut akan dibaca dan disimpan ke dalam *database*.

4.3 Perbandingan dengan *e-Voting* tanpa *Blockchain*

4.3.1 Ballot Valid

Sistem pemungutan suara elektronik yang tidak memakai blockchain akan memberi definisi sendiri mengenai ballot yang dikatakan valid oleh pembuat sistem. Pemberian definisi pastinya akan hanya bergantung dengan kemampuan sistem yang dibuat dan hanya dapat divalidasi kebenarannya oleh sistem tersebut. Sehingga bila sistem tersebut mengalami masalah, ballot yang dikatakan valid dapat berubah. Sedangkan sistem e-Voting dengan blockchain, pemberian definisi ballot yang valid melibatkan program dari luar sistem tersebut yaitu blockchain. Sehingga bila sistem mengalami masalah, ballot yang dikatakan valid tidak akan berubah dan validasi tetap dapat dilakukan oleh blockchain.

4.3.2 Transparency

Sistem pemungutan suara elektronik yang tidak memakai *blockchain*, akan kesulitan untuk memberikan *transparency* terhadap data yang disimpan. *Database* yang digunakan membutuhkan akses dan autentikasi untuk dapat membaca data tersebut. Selain itu, pemberian akses akan memberikan banyak sekali celah untuk membaca data-data rahasia dan terjadinya perubahan data. Sedangkan sistem *e-Voting* dengan *blockchain*, penyimpanan data *vote* dilakukan pada *blockchain* dan dapat diakses secara publik. *Blockchain* memungkinkan data untuk dibaca tanpa perlu autentikasi, dan terjadi perubahan data.

4.3.3 Anonymity

Sistem pemungutan suara elektronik yang tidak memakai *blockchain* akan kesulitan untuk membuat *voter* tidak dapat diketahui identitasnya ketika melakukan *vote*. Bila tidak diberi identitas pada *ballot*, maka *voter* tidak dapat melakukan verifikasi pada *vote* yang telah dilakukan. Bila diberi identitas pada *ballot*, maka *vote* tersebut tidak rahasia, karena sifat data yang transparan terhadap publik. Bila memberi enkripsi, maka akan kesulitan untuk dilakukan perhitungan *vote*. Sedangkan sistem *e-Voting* dengan *blockchain* memudahkan sistem untuk melakukan *vote* tanpa diketahui identitasnya. *Blockchain* memiliki metode *multi-signature address* yang dapat membuat alamat identitas virtual untuk melakukan *vote*, tetapi terhubung dengan *voter* sehingga dapat dilakukan verifikasi. Perhitungan suara pun dapat dilakukan karena *blockchain* bersifat transparan dan dapat dibaca secara publik.

4.3.4 Dependability

Sistem pemungutan suara elektronik tanpa *blockchain* akan kesulitan untuk menyimpan data yang dapat diakses publik tetapi tidak dapat diubah. Penggunaan *database* pada umumnya memiliki masalah umum seperti duplikasi data. Selain itu, *database* yang sering dipakai juga dapat memiliki risiko untuk data *vote* dapat diubah, digandakan ataupun dihapus oleh siapapun karena bersifat transparan. Sedangkan sistem *e-Voting* dengan *blockchain* dapat mengatasi masalah tersebut. *Blockchain* dengan kriptografi yang diterapkan, dapat memungkinkan data untuk tersimpan permanen. Sehingga data tersebut tidak dapat diubah, digandakan ataupun dihapus.

4.3.5 Eligibility

Sistem pemungutan suara elektronik tanpa *blockchain* akan sulit untuk menentukan pengguna atau *voter* yang berhak melakukan pemungutan suara. Dikarenakan pemberian hak akan dilakukan berdasarkan sistem tersebut. Jadi apabila sistem tersebut mengalami masalah, pemberian hak dapat dilakukan pada pihak asing dan dimanfaatkan untuk kepentingan pihak tertentu. Sehingga hasil pemungutan suara tidak akurat. Sedangkan sistem *e-Voting* dengan *blockchain* dapat membantu sistem dalam memberikan hak pilih terhadap *voter* tertentu. Karena *blockchain* merupakan program dari luar sistem dan memiliki sistem sendiri untuk melakukan autentikasi terhadap data yang dimasukkan pada *blockchain*.

4.3.6 Verifiability

Sistem pemungutan suara elektronik tanpa *blockchain* akan kesulitan untuk melakukan verifikasi dengan *vote* yang dilakukan oleh *voter*. Dikarenakan data *vote* bersifat transparan dan dapat diakses oleh publik, proses verifikasi akan sulit untuk dilakukan karena berbanding terbalik dengan sifat rahasia (*anonymity*). Bila tidak diberi identitas pada *ballot*, maka *voter* tidak dapat melakukan verifikasi pada *vote* yang telah dilakukan. Bila diberi identitas pada *ballot*, maka *vote* tersebut tidak rahasia, karena sifat data yang transparan terhadap publik. Bila memberi enkripsi, maka akan kesulitan untuk dilakukan perhitungan *vote*. Sedangkan sistem *e-Voting* dengan *blockchain* dapat memudahkan proses verifikasi. *Voter* dapat melakukan *vote* dengan rahasia tanpa diketahui identitasnya dan dapat melakukan verifikasi pada *vote* yang telah dilakukannya apakah tetap sama atau tidak.

4.3.7 Tally Votes

Proses perhitungan suara juga memiliki masalah yang sama dengan definisi *ballot* yang valid. Sistem pemungutan suara elektronik tanpa *blockchain* akan kesulitan untuk melakukan perhitungan suara, dikarenakan pemeriksaan *ballot* yang valid untuk dihitung dan dimasukkan ke dalam hasil akhir. Pemberian definisi untuk *ballot* yang valid untuk dapat terhitung di hasil akhir akan bergantung dengan sistem itu sendiri. Sehingga bila terjadi masalah pada sistem, akan mempengaruhi perhitungan *ballot* yang dikatakan valid, dan pada akhirnya mempengaruhi hasil akhir. Sedangkan sistem *e-Voting* dengan *blockchain* dapat membantu memberikan definisi serta verifikasi pada *ballot* yang dikatakan valid. Sehingga perhitungan hasil tetap dapat dilakukan tanpa perubahan pada definisi *ballot* yang valid dan tidak mempengaruhi hasil akhir.

4.4 Kuesioner

Untuk mengetahui penilaian pengguna terhadap program yang telah dibuat, dilakukan penelitian dan pengujian dengan penggunaan program ini melalui kuesioner yang diberikan kepada 18 mahasiswa. Dari hasil kuesioner yang telah disebarkan, maka detail penilaian mahasiswa terhadap penggunaan program yang telah dibuat dapat dilihat pada Tabel 1.

Table 1. Detail Penilaian Mahasiswa

Pertanyaan	1	2	3	4
Aplikasi mudah untuk digunakan.	0	2	9	7
Aplikasi mudah untuk dipahami.	0	2	9	7
Tampilan aplikasi keseluruhan.	0	2	5	11
Kejelasan informasi tersedia.	0	2	11	5
Kemudahan melakukan pemungutan suara.	0	1	8	9
Fitur yang ada sudah baik.	0	2	6	10
Aplikasi menjawab kebutuhan.	0	0	9	9
Keseluruhan aplikasi.	0	0	10	8

*Keterangan Penilaian : 1 = kurang; 2 = sedang; 3 = baik; 4 = baik sekali;

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil pengujian sistem yang telah dilakukan, dapat diambil beberapa kesimpulan antara lain :

- Teknologi *blockchain* dengan Multichain *tools* dapat membantu sistem *e-voting* dalam menyimpan data yang transparan dan dapat diakses oleh publik.
- Teknologi *blockchain* dengan Multichain *tools* dapat membantu sistem *e-voting* dalam melakukan *vote* tanpa diketahui identitasnya.
- Teknologi *blockchain* dengan Multichain *tools* dapat membantu sistem *e-voting* untuk menyimpan data *vote* yang tidak dapat diubah, digandakan, atau dihapus.
- Teknologi *blockchain* dengan Multichain *tools* dapat membantu sistem *e-voting* dalam memberikan hak pada *voter* untuk dapat melakukan *vote*.
- Teknologi *blockchain* dengan Multichain *tools* dapat membantu *voter* untuk dapat melakukan verifikasi kebenaran dari *vote* yang dilakukan.
- Teknologi *blockchain* dengan Multichain *tools* dapat membantu sistem *e-voting* untuk memilah data *vote* yang valid dan yang tidak valid.
- *Ballot* yang valid adalah *ballot* yang memiliki hal berikut
    - Tanda tangan (digital, alamat pengirim) dari seorang *organizer*, *voter* yang melakukan *vote* dan *node* tempat *ballot* itu dikirimkan, sebagai bukti keabsahan *ballot* tersebut.
    - Alamat penerima sebagai tempat pemungutan suara dari *ballot* tersebut ditujukan.
    - Sebuah aset sebagai hak pilih atau sarana *voter* untuk memilih dan mengirimkan *ballot*.
    - Data berupa *candidate* yang dipilih oleh *voter* dengan format tertentu sebagai tanda pemilihan yang sah (pencoblosan).
    - Status valid (di *blockchain*) sebagai tanda *ballot* tersebut sah dan sudah diterima dalam sistem pemungutan suara.
- Berdasarkan hasil kuesioner yang diberikan kepada mahasiswa, 55,6 % pengguna menilai baik mengenai keseluruhan aplikasi, dan 44,4 % pengguna menilai baik sekali mengenai keseluruhan aplikasi.
- Berdasarkan nilai rata-rata hasil kuesioner yang diberikan kepada mahasiswa, penilaian terhadap keseluruhan aplikasi adalah 3,44 (baik).

5.2 Saran

Saran yang dapat diberikan untuk penyempurnaan dan pengembangan program lebih lanjut antara lain :

- Sistem dibuat dengan *blockchain node* publik yang sudah *online* seperti *Bitcoin* atau *Ethereum*.
- Mekanisme sistem dapat dibuat *online* tanpa perlu datang ke tempat pemilihan umum.
- Aplikasi dibuat dalam *mobile application* dengan autentikasi ke nomor telepon.

6. REFERENSI

[1] Ayed, A. B. 2017. *A Conceptual Secure Blockchain-Based Electronic Voting System*. International Journal of Network Security & Its Applications, 9(3): 1-9.doi:10.5121/ijnsa.2017.9301

[2] Azwanti, N. 2017. *Perancangan E-Voting berbasis Web*. Jurnal Komputer Terapan, 3(2): 119-132.

[3] Conte de Leon, Daniel & Q. Stalick, Antonius & Jillepalli, Ananth & A. Haney, Michael & Sheldon, F.T. 2017. *Blockchain: properties and misconceptions*. Asia Pacific Journal of Innovation and Entrepreneurship. 11: 286-300. doi:10.1108/APJIE-12-2017-034.

[4] Liu, Y., & Wang, Q. 2017. *An E-voting Protocol Based on Blockchain*. IACR Cryptology ePrint Archive, 2017, 1043.

[5] Noizat, P. 2015. *Chapter 22 - Blockchain Electronic Vote*. Chuen, D. L.K. (Ed.) Handbook of Digital Currency (pp 453-461). San Diego: Academic Press.

[6] Pinsard, L. 2018. *Deploy Your First Ethereum Smart Contract on a Blockchain!* Retrieved from https://blog.theodo.fr/2018/01/deploy-first-ethereum-smart-contract-blockchain/

[7] *Public, Private and Consortium Blockchains*. 2019. Retrieved from https://www.draglet.com/blockchain-services/blockchain-technology/private-or-public-blockchain/

[8] Purwati, N. 2015. *Perancangan Sistem E-Voting Untuk Pemilihan Kepala Daerah (Pilkada)*. Jurnal Bianglala Informatika 3(1): 18-27.