|  |
| --- |
| **CM07** |

**PROPOSAL SKRIPSI**

**IMPLEMENTASI BLOCKCHAIN PADA SISTEM PEMUNGUTAN SUARA ELEKTRONIK DENGAN METODE KONSENSUS *PROOF-OF-AUTHORITY***



**Disusun Oleh**

**Basilius Bias Astho Christyono**

**00000013536**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS TEKNIK DAN INFORMATIKA**

**UNIVERSITAS MULTIMEDIA NUSANTARA**

**TANGERANG**

**2020HALAMAN PERSETUJUAN**

**PROPOSAL SKRIPSI**

**IMPLEMENTASI BLOCKCHAIN PADA SISTEM PEMUNGUTAN SUARA ELEKTRONIK DENGAN METODE KONSENSUS *PROOF-OF-AUTHORITY***

**Basilius Bias Astho Christyono**

**00000013536**

**Disetujui untuk diangkat sebagai topik penelitian pada tahun ajaran bersangkutan.**

**Tangerang, …………………….. 2020**

**Menyetujui,**

|  |
| --- |
| **Dosen Pembimbing I,**  **(…..………………….)**  **Dosen Pembimbing II,**  **(…..………………….)** |

|  |  |  |
| --- | --- | --- |
| **Tim Skripsi I,**  **(…..………………….)** | **Tim Skripsi II,**  **(…..………………….)** | **Tim Skripsi III,**  **(…..………………….)** |

# JUDUL: IMPLEMENTASI BLOCKCHAIN PADA SISTEM PEMUNGUTAN SUARA ELEKTRONIK DENGAN METODE KONSENSUS *PROOF-OF-AUTHORITY*

## 1. Latar Belakang Masalah

Indonesia adalah negara demokrasi terbesar ketiga di dunia. Pemilihan adalah sarana bagi orang Indonesia untuk memberikan suara kepada para pemimpin dan perwakilan rakyat yang dipilih. Pemilu yang ada masih menggunakan metode konvensional, di mana masyarakat yang memiliki hak pilih datang ke tempat pemungutan suara pada saat pemilihan berlangsung. Mereka mencoblos atau mencontreng gambar kandidat di kertas yang ada kemudian memasukkannya ke dalam kotak suara yang telah disediakan. Setelah proses pemungutan suara selesai, kemudian dilakukan proses penghitungan suara dengan membuka kembali kotak dan menghitung satu persatu kertas suara.

Proses konvensional ini memiliki beberapa kelemahan, diantaranya:

* Dapat terjadi kesalahan seperti kertas salah cetak, tidak sengaja basah dan sobek, data pemilih yang tidak benar ataupun tidak sesuai, hingga pemilih ganda.
* Lambatnya proses tabulasi hasil perhitungan suara misalnya dari daerah yang lokasinya sulit untuk dijangkau akibat lemahnya infrastruktur.
* Tidak ada salinan terhadap kertas suara. Jika terjadi kerusakan terhadap kertas suara, panitia sudah tidak mempunyai alat bukti lagi, lalu akan menyebabkan sulitnya penghitungan suara akibat ketidakpercayaan terhadap hasil penghitungan suara.
* Bersarnya anggaran yang diperlukan untuk melaksanakan pemungutan suara, mulai dari biaya cetak, gaji panitia dan pengawas, hingga transportasi.

Kerumitan dan berbagai kendala dalam pelaksanaan membuat proses pemilihan umum tidak berjalan dengan baik serta kurang dari segi efektifitas maupun efisiensi. Disisi lain, perkembangan teknologi telah banyak memberikan manfaat signifikan karena memberikan berbagai kemudahan baik dari segi akses maupun biaya. Pemanfaatan teknologi informasi dalam pelaksanaan pemilihan umum akan memacu efektivitas dan efisiensi pelaksanaannya dari yang tadinya konvensional bergeser kepada model pemungutan suara secara elektronik.

Teknologi *e-voting* dapat menjadi pilihan yang baik untuk saat ini dalam menjalankan salah satu pilar utama demokrasi yaitu pemilihan umum. Apalagi terdapat kekurangan dalam penerapan secara konvensional yang sudah terjadi selama ini. Sebenarnya, sistem pemungutan suara secara elektronik ini sudah sangatlah sering digunakan seperti survei, ujian, petisi, hingga pemilu.

Dalam setiap demokrasi, keamanan pemilu adalah masalah keamanan nasional. Bidang keamanan komputer telah selama satu dekade mempelajari kemungkinan sistem pemilihan elektronik, dengan tujuan meminimalkan biaya pemilihan umum nasional, sambil memenuhi dan meningkatkan kondisi keamanan pemilihan. Mengganti skema kertas tradisional dengan sistem pemilihan yang baru sangatlah penting untuk membatasi penipuan dan membuat proses pemungutan suara dapat dilacak dan diverifikasi.

Beberapa negara maju dan berkembang juga menerapkan teknologi *e-voting*, seperti India, pemilu India adalah sebuah perhelatan demokrasi paling besar di dunia, pada hari pemilu, setiap pemilih harus membawa kartu pemilih, setelah diperiksa oleh panitia pemungutan suara, dan sesuai dengan data daftar pemilih tetap, pemilih diizinkan untuk memilih pada mesin elektronik yang disediakan. Selain di India, beberapa negara yang sudah menerapkan sesuai dengan *e-voting map 2015* yang dikeluarkan *Competence Center for Electronic Voting and Participation* diantaranya, kategori *legally binding electronic voting with voting machines* yaitu: Australia, Brazil, Canada, Prancis, India, Jepang, Kazakhstan, Peru, Russia, Amerika, Arab Saudi, Venezuela, kategori *legally binding internet voting* yaitu: Austria, Australia, Canada, Estonia, Prancis Jepang, Switzerland, kategori *Planning trials, non-legally binding e-voting* yaitu: Argentina, Azerbaijan, Belarus, Bulgaria, Chile, Republik Czech, Finlandia, Greece, Italia, Latvia, Lithuania, Mexico, Nepal, Nigeria, Norwegia, Polandia, Portugal, Romania, Slovakia, Slovenia, Afrika Selatan, Spanyol, Korea Selatan, Swedia.

Mesin pemilihan elektronik telah dianggap cacat, oleh komunitas keamanan, terutama berdasarkan masalah keamanan fisik. Siapapun yang memiliki akses fisik ke mesin tersebut dapat menyabotase mesin, sehingga memengaruhi semua suara yang diberikan pada mesin tersebut. Salah satu potensi untuk menyelesaikan permasalahan keamanan seperti ini adalah dengan menggunakan *blockchain*.

Teknologi *blockchain* digunakan untuk menyimpan daftar transaksi layaknya buku besar akuntansi. *Blockchain* memungkinkan data untuk disimpan secara terdesentralisasi yang berarti seluruh riwayat transaksi tersebut disebarkan ke semua penggunanya, jadi seluruh pengguna yang masing-masing terhubung dalam jaringannya akan memiliki salinan dari daftar transaksi.

Penggunaan *blockchain* sebagai sarana penyimpanan data sangatlah jauh berbeda dengan cara penyimpanan *database* pada umumnya misalnya SQL di mana menggunakan sistem *server* yang terpusat dan setiap pengguna mengakses database yang sama. Dengan *database* seperti SQL tersebut, setiap pengguna bisa menambah / membuat, mengubah, bahkan menghapus data sesuai kebutuhan sedangkan dalam *blockchain*, yang bentuknya riwayat transaksi, pengguna hanya bisa menambah data ke dalam buku besar tetapi tidak dapat mengubah ataupun menghapus data yang sudah tercatat.

Cara untuk merusak *database* yang berada pada sistem terpusat yaitu dengan melakukan peretasan ke dalam sistem tersebut, namun untuk *blockchain* pada umumnya, peretas memerlukan jumlah *computing power* yang jauh melebihi mayoritas pengguna yang ada karena dalam penentuan buku besar mana yang akan dianggap sah adalah dengan membandingkan buku besar yang dimiliki pengguna dan seluruh pengguna lain lalu menghitung jumlah terbanyak yang identik, dengan begitu akan sangat kecil kemungkinannya untuk memanipulasi transaksi yang ada.

## 2. Rumusan Masalah

Membangun sistem pemungutan suara elektronik yang memenuhi persyaratan hukum legislator telah menjadi tantangan sejak lama. Teknologi ledger terdistribusi adalah kemajuan teknologi yang menarik di dunia teknologi informasi.

Berdasarkan latar belakang yang telah dipaparkan maka rumusan masalah adalah sebagai berikut:

1. Bagaimana mekanisme mendistribusikan data pemungutan suara melalui sistem *e-voting* menggunakan jaringan *Blockchain* secara *peer-to-peer*?
2. Bagaimana cara sistem melakukan konsesus terhadap data yang terdistribusi di setiap *node* dalam jaringan dan menentukan data mana yang valid terverifikasi?

## 3. Batasan Masalah

Penelitian ini mengevaluasi kerangka kerja blockchain dan penerapannya sebagai layanan untuk sistem pemilihan elektronik terdistribusi dimana lebih menitikberatkan pada persebaran data dan proses validasinya dengan melakukan konsensus sehingga penelitian yang dilakukan akan dibatasi menjadi berikut ini:

1. Bahasa yang akan digunakan yaitu JavaScript agar dapat berjalan secara *cross-platform* (*mobile, desktop,* dan terutama *web*).
2. Menggunakan alat, *library* dan *framework* Go-Ethereum dan Web3JS.
3. Jaringan yang akan digunakan untuk *testing* adalah jaringan lokal.
4. Sistem berjalan dengan asumsi kondisi ideal dimana pada saat aplikasi berjalan tidak terdapat gangguan maupun serangan misalnya *Man-in-the-middle attack*.
5. Jenis *Blockchains* yang digunakan adalah *Private Blockchain* dengan metode konsensus *Proof-of-Authority* untuk menentukan pihak mana sajakah yang dapat menulis blok baru sebagai *validator* ke dalam buku besar *blockchain* (misalnya lembaga atau organisasi yang sudah terbukti integritasnya).

## 4. Tujuan Penelitian

Penelitian ini bertujuan untuk membangun sistem pemungutan suara elektronik dengan menggunakan *blockchain* sebagai layanan untuk pemilihan elektronik. Dengan kondisi server yang terdesentralisasi melalui jaringan *blockchain* secara *peer-to-peer*, diharapkan akan meningkatkan kepercayaan umum terhadap data yang tersimpan karena setiap server dan bahkan orang biasapun dapat ikut terhubung ke dalam jaringan lalu menyimpan salinan dari rantai data buku besar secara utuh serta dapat dengan mudah untuk melakukan audit terhadap data untuk menentukan mana data yang *valid* dan terverifikasi.

## 5. Manfaat Penelitian

Selain meningkatkan keamanan dalam penyimpanan data dan mengurangi biaya *hosting* pemilihan nasional karena *server* hanya akan digunakan untuk pendataan daftar pemilih tetap. Dari sifat *blockchain* sendiri menawarkan anonimitas, otonomi, keadilan, kerahasiaan, dan transparansi dimana sifat ini sesuai dengan asas pemilu di Indonesia yaitu langsung, umum, bebas, rahasia, jujur dan adil.

Dari sisi pengguna juga meningkatkan kemudahan untuk menyalurkan hak suara pemilihan tanpa perlu repot datang ke tempat pemungutan suara karena dapat dilakukan kapan saja dan dimanapun selama periode masih berlangsung.

## 6. Telaah Literatur

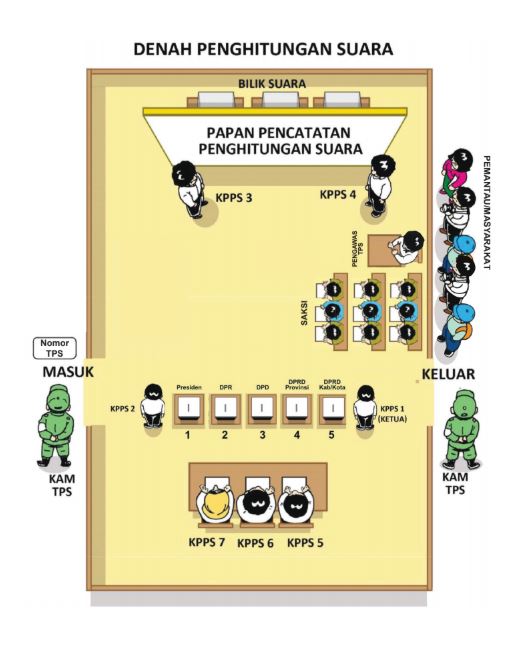
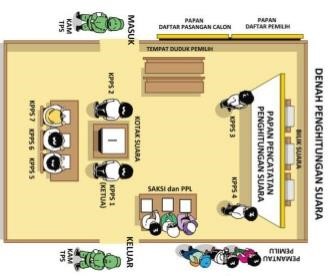
Pemilihan Umum adalah proses memilih seseorang untuk mengisi jabatan tertentu yang diselenggarakan seharusnya sesuai dengan asas langsung, umum, bebas, rahasia, jujur, dan adil dalam Negara Kesatuan Republik Indonesia berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia tahun 1945.

Berikut ini merupakan beberapa contoh mekanisme pemungutan suara yang sudah terdapat dan sering terjadi di Indonesia:

1. Tradisional yaitu datang ke tempat pemungutan suara

Contoh paling mudah dan sangat terlihat adalah pemilihan umum kepala pemerintahan. Hingga saat ini, proses pemungutan suara dilakukan secara *onsite* di mana para pemilih datang ke tempat pemungutan suara sesuai yang tertera pada daftar pemilih tetap, melakukan verifikasi dengan menyerahkan surat undangan hak pilih (seperti model C-6) ataupun dengan tanda pengenal lainnya, lalu menunggu giliran untuk memilih pada ruangan yang disediakan.

Gambar 1. Komponen denah tempat pemungutan suara (KPU RI, 2019)

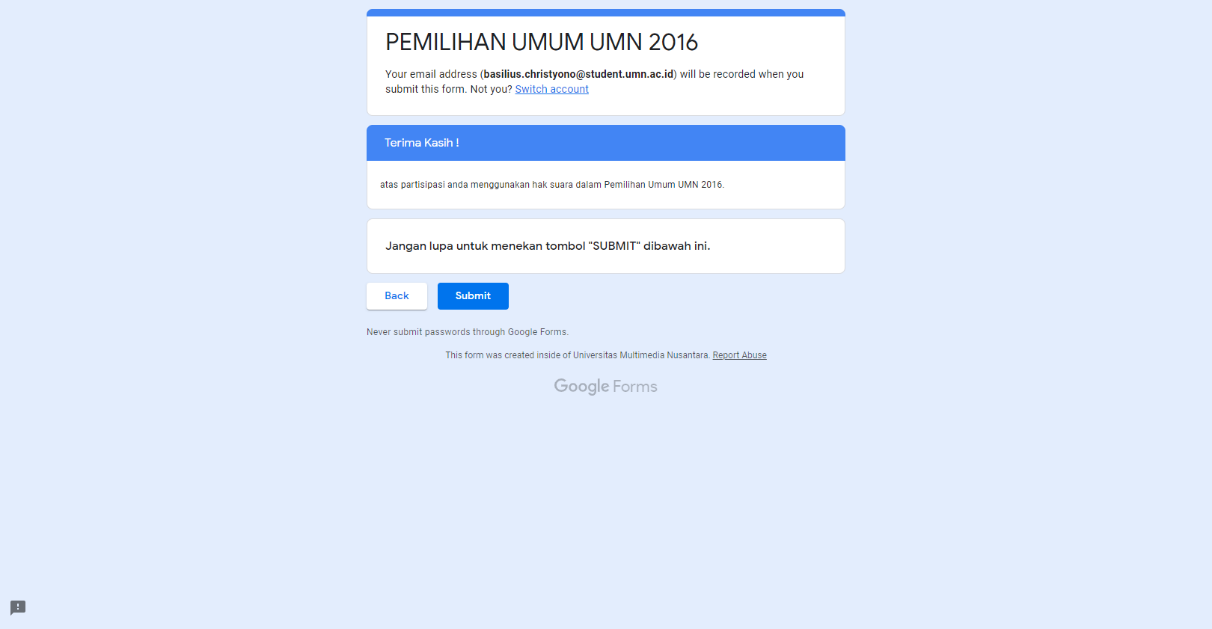
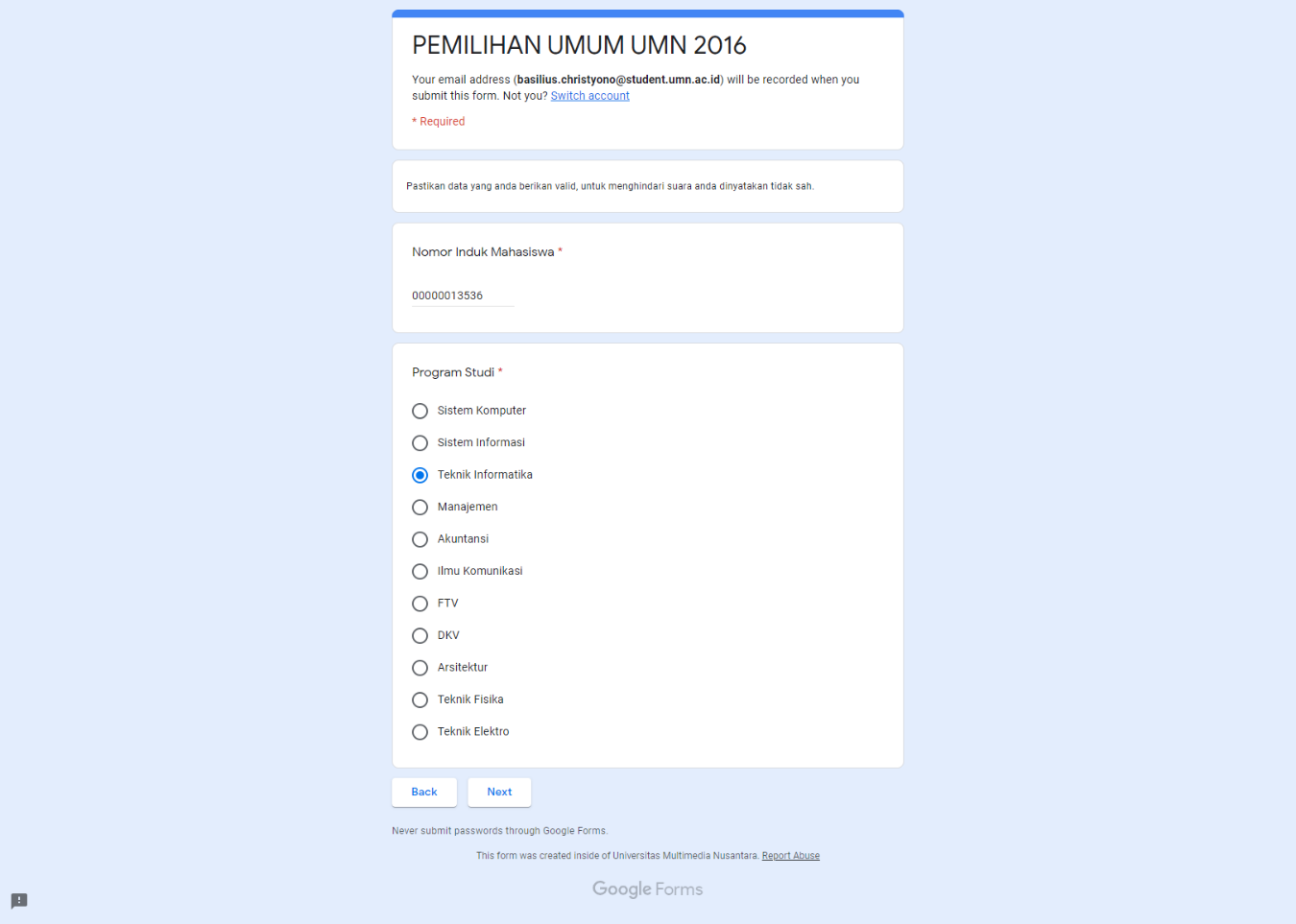


1. Elektronik dengan *server* terpusat

Beberapa pemungutan suara yang sering kita temui dengan sistem seperti ini yaitu misalnya survei, ujian, petisi, bahkan pemilihan ketua kelas hingga organisasi lembaga dalam kampus. Cara ini memang memiliki keuntungan efisien dan lebih hemat biaya, namun siapapun yang memiliki akses ke *server* tersebut dapat melihat atau mungkin juga mengubah data.

Sebagai contoh yang ada di lingkungan sekitar misalnya pemilihan ketua himpunan yang ada di lingkungan kampus Universitas Multimedia Nusantara. Pada pemilihan ini, sistem yang digunakan sudah dilakukan secara elektronik yaitu dengan menggunakan Google *Form* yang nantinya data hasil akan tersimpan ke dalam Google *Sheet* hanya dengan persyaratan sebagai berikut:

* Pemilihan dilakukan menggunakan akun surel khusus yang dimiliki oleh masing-masing mahasiswa
* Hanya mahasiswa aktif yang suaranya akan dianggap sah
* Setiap akun hanya dapat satu kali memilih
* Setiap akun memilih kandidat dari daftar program studinya, apabila sesuai, maka akan dianggap sebagai suara yang sah



Gambar 2. Cara pengisian surat suara (KPU UMN, 2016)

Penggunaan *Google Form* selain memudahkan dalam penggunaan, juga cepat dalam proses persiapan hingga pembuatan, hanya saja sistem ini kurang tepat apabila digunakan untuk pemungutan suara yang bersifat rahasia yang bahkan pembuatnya saja tidak boleh tahu apa yang dipilih oleh pengguna karena cara ini biasanya digunakan untuk mengumpulkan data yang sifatnya informatif dan memungkinkan untuk digunakan sebagai keperluan statistik misalnya kuisioner.

Setelah pengguna memberikan suaranya, akan ada periode rekapitulasi suara di mana seluruh data surat suara yang masuk akan di cek untuk menentukan apakah akun pemilih tersebut merupakan mahasiswa aktif dan memilih sesuai dengan jurusannya sebagai suara sah kemudian dilakukan penghitungan suara.

Hingga saat ini penggunaan *blockchain* pada umumnya digunakan hanya terbatas pada *cryptocurrency*. Maka pada penelitian kali ini, peneliti akan merancang sistem pemungutan suara elektronik yang menggunakan *blockchain* dengan *server* yang terdesentralisasi sehingga memungkinkan pemilih untuk dapat memberikan hak suaranya kapanpun dan di manapun selama periode pemungutan berlangsung.

**6.1. *Blockchain***

*Blockchain* dapat diartikan sebagai struktur data yang memungkinkan kita membuat buku digital dari data dan berbagi data dalam jaringan secara terdesentralisasi. Setiap blok yang terkandung dalam teknologi blockchain selalu dikaitkan dengan satu blok sebelum dan satu blok sesudahnya.

Saat ini ada beberapa jenis blockchain (Laurence Tiana, 2017), yaitu:

* *Public Blockchains*

*Blockchain* publik, seperti Bitcoin, adalah jaringan terdistribusi besar yang dijalankan secara terbuka bagi siapa saja untuk berpartisipasi ditingkat manapun dan biasanya bersifat *open-source* yang dikelola oleh komunitas mereka.

* *Permissioned Blockchains*

*Blockchain* dengan izin, seperti Ripple, mengontrol peran yang dapat dimainkan individu dalam jaringan. Mereka masih tergolong cukup besar. Untuk jenis ini biasanya sudah tidak lagi *open-source*.

* *Private Blockchains*

*Blockchain* secara tertutup, cenderung lebih kecil. Keanggotaan mereka dikendalikan dengan ketat. Jenis *blockchain* ini disukai oleh suatu lembaga atau organisasi tertentu yang memiliki anggota tepercaya dan mendistribusikan informasi rahasia.

Ketiga jenis *blockchain* menggunakan kriptografi agar memungkinkan setiap peserta di jaringan tertentu dapat mengelola buku besar dengan cara yang aman tanpa perlu otoritas pusat untuk menegakkan aturan.

Selain itu, ada manfaat yang dimiliki blockchain (Ernest Adam K., 2014) yang dapat digunakan dalam mendesain sistem yaitu:

1. *Security*

Dengan menggunakan enkripsi asimetris. Kunci yang dihasilkan adalah dalam bentuk dua pasang kunci publik dan privat yang terkait secara matematis.

Kunci publik akan dipublikasikan dalam sistem dan kunci pribadi hanya diakses oleh pengguna. Hanya orang yang memiliki kunci pribadi yang dapat menggunakan akun.

1. *Accuracy*

Dalam pemilihan setiap pengguna akan diverifikasi oleh pemverifikasi dan mendaftar sehingga pengguna yang dapat memilih adalah pengguna yang terverifikasi.

1. *Transparency*

Semua surat suara dalam sistem disimpan di blockchain sehingga pengguna dapat melihat berapa banyak suara yang dimiliki masing-masing kandidat. Selain itu sistem ini dapat dan mudah diaudit.

1. *Autonomy*

Hal besar yang mengikuti sistem pemungutan suara ini adalah bahwa memiliki keuntungan di bidang sistem desentralisasi.

1. *Anonymity*

Sistem pemungutan suara yang digunakan adalah anonim sehingga pengguna merasa aman tetapi masih dapat memeriksa apakah suara yang dipilih memasuki sistem.

1. *Forgiveness*

Setiap pengguna yang telah memberikan suara dimungkinkan untuk membuat perubahan selama periode pemilihan.

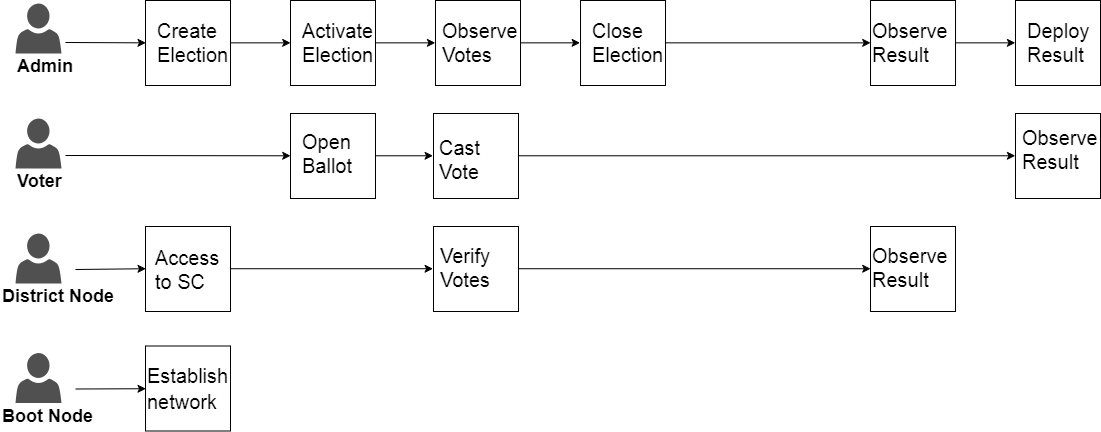
1. *Fairness*

Setiap pengguna dapat memilih sesuai keinginan mereka.

1. *Efficiency*

Target yang diharapkan dari sistem ini adalah untuk meminimalkan biaya yang digunakan untuk operasi.

Masuk ke dalam, teknologi baru ini bekerja melalui empat fitur utama (Cachin C. dan Vukolić M., 2017) yaitu:

1. Buku besar ada di banyak lokasi berbeda: Tidak ada titik kegagalan dalam pemeliharaan buku besar yang didistribusikan.
2. Adanya kontrol terdistribusi atas siapa yang dapat menambahkan transaksi baru ke buku besar.
3. Setiap blok baru yang diusulkan untuk buku besar harus merujuk ke versi buku besar sebelumnya, menciptakan rantai yang tidak dapat diubah dari mana *blockchain* mendapatkan namanya, dan dengan demikian mencegah gangguan dengan integritas entri sebelumnya.
4. Mayoritas *node* jaringan harus mencapai konsensus sebelum blok entri yang diusulkan menjadi bagian permanen dari buku besar.

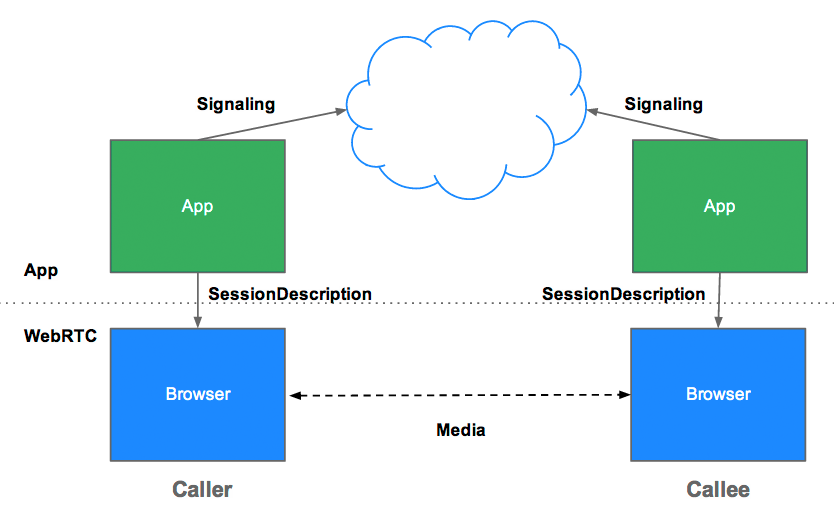
Gambar 3. Proses Pemilihan (*Blockchain-Based E-Voting System*, 2018)

**6.2. WebSocket**

Sebelumnya, teknologi P2P (*peer-to-peer*) seperti aplikasi obrolan *desktop* dapat melakukan sesuatu yang tidak bisa dilakukan pada *browser*. WebSocket pada dasarnya memungkinkan aplikasi *web* membuat komunikasi P2P dengan menggunakan SDP (*Session Description Protocol*).

Untuk berkomunikasi dengan rekan lain melalui *browser web*, setiap *browser* harus memenuhi kriteria berikut ini:

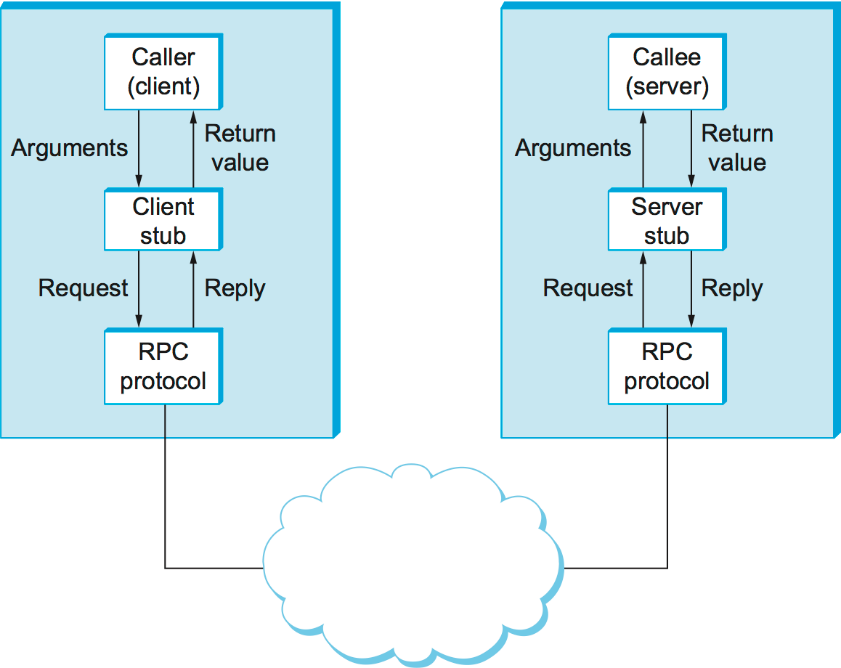
1. Saling setuju untuk memulai komunikasi
2. Tahu cara menemukan lokasi (*IP Address*) satu sama lain
3. Melewati keamanan dan perlindungan *firewall*
4. Mengirimkan semua komunikasi secara *real-time*



Gambar 4. *Javascript Session Establishment Protocol* (WebRTC, 2012)

**6.3. RPC (*Remote Procedure Call*)**

RPC adalah suatu protokol yang menyediakan suatu mekanisme komunikasi antar proses yang mengijinkan suatu program untuk berjalan pada suatu komputer tanpa terasa adanya eksekusi kode pada sistem yang jauh (*remote system*), hal ini berbeda dengan REST. Protokol ini juga mendukung adanya prosedur callback dan select subroutine pada sisi *server*. Setiap *service* pada *network* adalah susunan dari *program* *remote*, dan setiap *program* *remote* mengimplementasi *procedure* *remote*. Semua prosedur berikut parameternya dan hasilnya di dokumentasikan secara spesifik pada protokol suatu program. *Protokol Message* RPC didefinisikan dengan menggunakan deskripsi data *eXternal Data Representation* (XDR) yang meliputi struktur, enumerasi dan *union*.

Gambar 5. *Remote Procedure Call* (https://book.systemsapproach.org, 2019)

**6.4. *Proof-of-Authority Consensus***

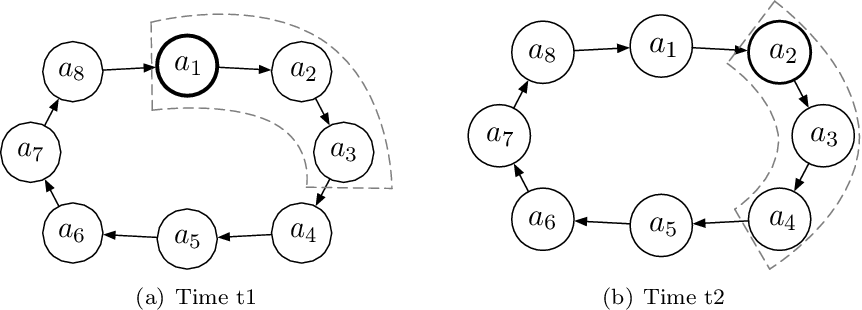
*Proof-of-Authority* (PoA) adalah sebuah algoritma konsensus berbasis reputasi yang merupakan sebuah solusi praktis dan efisien untuk jaringan *blockchain*. PoA memiliki struktur yang mirip dengan *Delegated Proof of Stake* (DPoS), di mana jumlah *validator* sangat terbatas. Perbedaannya adalah bahwa dalam DPoS mereka dipilih oleh masyarakat / *node*, yaitu semua pemegang *token*, sedangkan di PoA mereka dipilih setelah pemeriksaan menyeluruh, biasanya dari entitas yang mengendalikan proyek blockchain ataupun dari kelompok tertentu yang dapat dipercaya.

Algoritma konsensus PoA menggunakan nilai identitas, yang berarti *validator* menggunakan reputasinya untuk dapat membuat atau menulis blok data baru kedalam rantai. Maka dari itu *blockchain* PoA diamankan dengan *node* validasi yang terpilih sebagai entitas yang dapat dipercaya. Model bergantung pada jumlah blok validator yang terbatas dan ini membuat sistem yang lebih dapat berskala. Blok dan transaksi diverifikasi oleh peserta yang sudah di setujui, yang berlaku sebagai moderator sistem.

Ada beberapa mekanisme yang digunakan untuk membuat sebuah blok baru yaitu sebagai berikut:

* *Authority Round* (atau disebut juga *AuRa*)

1. "*Block Leader*" dipilih secara acak dari daftar *validator.*
2. Pemimpin blok tersebut kemudian mencoba membuat blok baru dari daftar transaksi yang ada (disebut juga *block proposal*), lalu mendistribusikannya kepada seluruh *validator* lainnya.
3. Seluruh *validator* menerima proposal dari blok tersebut sebagai *block acceptance.*
4. Jika seluruh *validator* lainnya (kecuali pemimpinnya) menerima blok yang sama, maka blok tersebut dinyatakan diterima dan akan di distribusikan ke dalam jaringan sebagai blok permanen. Jika tidak menerima blok yang sama, seluruh *validator* akan ambil *voting* untuk menentukan apakah blok yang dikirimkan dari pemimpin ini dianggap tidak sah dan berbahaya atau tidak.
5. Jika pemimpin blok dianggap sebagai aktor jahat oleh mayoritas *validator* lain, mereka ditendang keluar dan kehilangan hak untuk membuat blok. Kalau tidak, proses pembuatan blok akan diulang dari awal dengan memilih pemimpin yang baru.



Gambar 6. *Validator* yang dapat mengusulkan blok baru (DPoS, 2018)

* *Clique* (*epochs*)

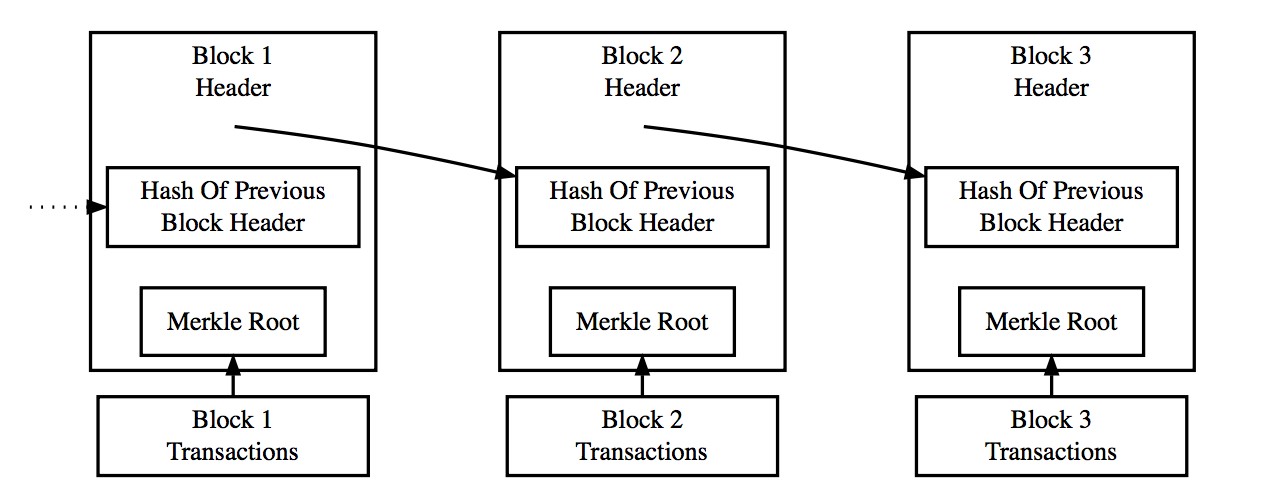
Dalam *Clique*, sebuah blok dapat diusulkan tidak hanya oleh pemimpin blok, tetapi juga oleh sejumlah *validator* lainnya (setengah dari jumlah seluruh *validator* - 1).

Sebagai contoh, katakanlah jumlah *validator* ada 8 dan terdaftar sebagai angka 1 hingga 8. Formula di atas memberi informasi bahwa maksimal tiga *validator* dapat mengajukan / membuat blok baru.

1. Untuk blok pertama, 1 adalah pemimpin blok, dan *validator* 2 dan 3 juga dapat mengusulkan blok.
2. Blok yang dibuat oleh pemimpin blok memiliki prioritas di atas yang lain, tetapi jika karena alasan apapun pemimpin blok gagal untuk mengusulkan yang lain akan tetap mengusulkan dan blok yang diusulkan pertama akan dianggap menang.
3. Setelah blok di *commit* ke blockchain secara permanen, *clique* akan berubah di periode pembuatan blok berikutnya, selanjutnya 2 adalah pemimpin blok dan *validator* 3 dan 4 juga dapat mengusulkan blok.
4. Proses ini berulang sampai semua *validator* menjadi pemimpin blok, dan berputar lagi dari awal.

**6.5. Kriptografi Antar Blok**

*Hashing* merupakan salah satu teknik kriptografi dalam menghitung nilai unik (D Eastlake, T Hansen, 2001) yang dapat diibaratkan sebagai sidik jari dari sebuah data dan merupakan sebuah identitas dari suatu blok data yang digunakan untuk menghubungkan blok baru dengan blok sebelumnya. Contohnya *Secure Hash Algorithms* (SHA).

Gambar 7. Ilustrasi *blockchain* (<http://www.blockchain.org>)

**6.6. Kriptografi Transaksi Data Pemilih**

*Elliptic Curve Digital Signature Algorithm* (ECDSA) adalah sebuah tanda tangan digital yang digunakan untuk mengautentikasi konten secara digital (Johnson D., Menezes A., Vanstone S, 1992) sebagai cara untuk mengetahui keaslian kontent ataupun kepemilikan

Algoritma ini akan menghasilkan kunci yang saling terkait secara matematis.

* *Private Key*: Nomor rahasia, hanya diketahui oleh orang yang membuatnya. Kunci pribadi pada dasarnya adalah nomor yang dibuat secara acak.
* *Public Key*: Nomor yang terkait dengan kunci pribadi, tetapi tidak perlu dirahasiakan. Kunci publik dapat dihitung dari kunci pribadi, tetapi tidak sebaliknya. Kunci publik dapat digunakan untuk menentukan apakah tanda tangan asli (dengan kata lain, diproduksi dengan kunci yang tepat) tanpa memerlukan kunci pribadi untuk diungkapkan.
* *Signature*: Nomor yang membuktikan bahwa operasi penandatanganan berlangsung. Tanda tangan secara matematis dihasilkan dari hash sesuatu yang akan ditandatangani, ditambah dengan kunci pribadi. Lalu dengan adanya kunci publik, algoritma matematika dapat digunakan pada tanda tangan untuk menentukan bahwa itu awalnya dihasilkan dari hash dan kunci pribadi, tanpa perlu mengetahui kunci pribadi.

## 7. Metodologi Penelitian

1. Pendataan peserta pemilih

Calon Pemilih membuat sepasang kunci publik dan privat kemudian mengirimkan nomor kunci publik tersebut beserta informasi pribadi yang valid dan bersifat unik, misalnya berdasarkan data kartu identitas, kepada pihak penyelenggara pemungutan suara sebagai pendaftaran untuk ikut serta dalam pemungutan suara, dan untuk kunci privatnya disimpan masing-masing untuk digunakan saat melakukan pemilihan.

1. Perancangan sistem jaringan *blockchain*

*Instance Node* merupakan sebuah perangkat yang memulai membuat jaringan *blockchain* pertama kali (disebut sebagai *seed / bootnode*) memiliki nomor IP yang statis dengan port tertentu dimana perangkat ini yang akan pertama kali dihubungi oleh *client node* untuk mencari seluruh IP *node* lainnya yang sedang aktif.

*Node* ini juga akan membuat sebuah *genesis block.* Karena *blockchain* hanya mencatat riwayat transaksi sebagai buku besar transaksi kegiatan pengguna seperti mengirim dan menerima koin atau riwayat eksekusi *smart contract*.

1. Perancangan metode konsensus

Dari seluruh *node* yang terhubung ke dalam jaringan *blockchain*, tidak hanya *Instance Node* dan pemilih saja yang terhubung, tetapi lembaga atau organisasi juga dapat bergabung (tentunya harus mendaftar terlebih dahulu), misalnya lembaga hitung cepat pemilu, namun karena bukan kategori pemilih, maka tidak memiliki hak untuk melakukan transaksi pemilihan kandidat dan hanya dapat melakukan *mining* blok baru. Pihak penyelenggara pemungutan suara berhak menentukan siapa saja yang bisa menjadi *validator* untuk dapat membuat blok baru dan mendistribusikannya ke dalam jaringan *blockchain*.

1. Perancangan *User Interface* Aplikasi Pengguna

* Halaman penyimpanan kunci publik dan privat
* Halaman registrasi untuk ikut serta dalam pemilihan
* Halaman pemilihan / pemungutan suara
* Halaman riwayat pemilihan / hasil penghitungan suara kandidat

1. Pengujian Sistem
2. Pembuatan *genesis block* sebagai langkah awal pengaturan jaringan blockchain untuk menentukan siapa yang berhak menulis atau membuat blok baru dan mendistribusikannya ke dalam jaringan.
3. Uji jaringan *blockchain* dimana setiap node harus bisa terhubung satu sama lain dan analisa data dari rantai masing-masing *node* untuk menentukan rantai mana yang dianggap valid.
4. Pengujian Aplikasi
5. Uji registrasi pemilih dimana pemilih membuat sepasang kunci publik dan privat (jika belum punya akun).
6. Melihat riwayat pemilihan yang telah dilakukan oleh pemilik akun.
7. Melihat hasil pemungutan suara masing-masing kandidat.

## 8. Spesifikasi Sistem

Ketika dimulai untuk pertama kalinya, program tidak mengetahui alamat IP dari setiap *node* penuh yang aktif. Untuk menemukan beberapa alamat IP dari *node lainnya*, mereka meminta satu atau lebih nama DNS (disebut *seed* DNS / IP *Tracker*).

Maka dari itu, dibutuhkan setidaknya satu perangkat yang menjadi *Node* awal saat *booting* dengan kondisi selalu online dengan IP yang statis tidak berubah untuk mempercepat menemukan dan berkomunikasi antar node lainnya dengan spesifikasi seperti server standar pada umumnya..

Beberapa perangkat keras yang digunakan adalah sebagai berikut:

1. Laptop pribadi dengan prosesor Intel i7-7700HQ, RAM 16GB.
2. Beberapa komputer dengan spesifikasi standar sebagai *node server.*
3. Beberapa telepon pintar dengan spesifikasi standar.

Beberapa perangkat lunak yang digunakan adalah sebagai berikut:

1. Visual Studio Code / IntelliJIDEA sebagai *text editor*.
2. NodeJS, Geth, dan beberapa Javascript *library* lainnya.

**9. Rencana Waktu Penelitian**

Tabel 1. Rencana waktu penelitian

| Kegiatan | Minggu ke- | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| Pendataan peserta pemilih |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perancangan system jaringan *blockchain* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perancangan metode konsensus |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perancangan *User Interface* Aplikasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengujian Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengujian Aplikasi Pengguna |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Dokumentasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**10. Daftar Pustaka**

Republik Indonesia. 1945. Undang-Undang Dasar Tahun 1945. MPR, Jakarta.

Republik Indonesia. 2011. Undang-Undang No 15 Tahun 2011. DPR, Jakarta.

Republik Indonesia. 2017. Undang-Undang No 7 Tahun 2017. DPR, Jakarta.

A. Barnes, C. Brake and T. Perry. 2016. Digital Voting with the Use of Blockchain Technology Team Plymouth Pioneers. Plymouth University.

“Blockchain vs Centralized Databases”. Multichain, [daring] Tersedia di: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases [Diakses 12 Mei 2019]

“WebRTC Architecture”, [daring] Tersedia di: https://webrtc.org/architecture [diakses 12 Mei 2019]

E-Voting.cc. 2015. Competence Center for Electronic Voting and Participation, [daring] Tersedia di: https://www.e-voting.cc/en/it-elections/world-map/ [Diakses 12 Mei 2019].

Sos.ca.gov. 2007. Top-to-Bottom Review | California Secretary of State, [online] Tersedia di: https://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ [Diakses 12 Mei 2019].

Nicholas Weaver. 2016. Secure the Vote Today, [daring] Tersedia di: https://www.lawfareblog.com/secure-vote-today [Diakses 12 Mei 2019].

Nakamoto Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, [daring] Tersedia di: https://bitcoin.org [diakses 12 Mei 2019].

Stefano De Angelis, dkk. 2018. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain, [daring] Tersedia di: https://pdfs.semanticscholar.org/17b8/4f0e092401b88b2505c145890d1d0db91219.pdf [diakses 12 Mei 2019].

Ankaa W., dan Dimaz. 2017. Blockchain dari Bitcoin untuk Dunia. Jasakom, Jakarta.

Laurence, Tiana. 2017. 2009. Blockchain for Dummies. John Wiley & Sons, New Jersey.

Ernest, Adam Kaleb. 2014. The Key To Unlocking The Black Box: Why The World Needs A Transparent Voting DAC, [daring] Tersedia di https://followmyvote.com/wp-content/uploads/2014/08/The-Key-To-Unlocking-The-Black-Box-Follow-My-Vote.pdf [diakses 12 Mei 2019].

Hjálmarsson, Friðrik Þ., dan Hreiðarsson, Gunnlaugur K. 2018. Blockchain-Based E-Voting System, [daring] Tersedia di: <https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf> [diakses 12 Mei 2019].

Cachin, C., dan Vukolić, M. 2017. Blockchain Consensus Protocols in the Wild, [daring] Tersedia di: <http://arxiv.org/abs/1707.01873> [diakses 12 Mei 2019].

Meter, C. 2017. Design of Distributed Voting Systems. [daring] Tersedia di: <http://arxiv.org/abs/1702.02566> [Diakses 12 Mei 2019].

“Penjelasan Mengenai Proof of Authority”, [daring] Tersedia di: <https://www.binance.vision/id/blockchain/proof-of-authority-explained> [diakses 12 Mei 2019].

Accredited Standards Committee X9. 2005. Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*.* [daring] Tersedia di: https://web.archive.org/web/20160304101319/http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf [diakses 12 Mei 2019].

D Eastlake, P Jones. 2001. US Secure Hash Algorithm 1 (SHA1)*.* [daring] Tersedia di: http://www.hjp.at/(st\_a)/doc/rfc/rfc3174.html [diakses 12 Mei 2019].

Johnson, D., Menezes, A., Vanstone, S.. 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA)*.* [daring] Tersedia di: https://link.springer.com/journal/10207 [diakses 12 Mei 2019].

**LEMBAR PENILAIAN**

**PROPOSAL SKRIPSI**

JUDUL : Implementasi Blockchain Pada Sistem Pemungutan Suara Elektronik Dengan Metode Konsensus *Proof-Of-Authority*

NAMA : Basilius Bias Astho Christyono

NIM : 00000013536

Hasil Penilaian (centang salah satu)

□ Ditolak □ Diterima dengan revisi □ Diterima

Catatan Penilai (fokus pada substansi isi topik penelitian yang diajukan)

Tim Skripsi I,

**(…..………………….)**

**LEMBAR PENILAIAN**

**PROPOSAL SKRIPSI**

JUDUL : Implementasi Blockchain Pada Sistem Pemungutan Suara Elektronik Dengan Metode Konsensus *Proof-Of-Authority*

NAMA : Basilius Bias Astho Christyono

NIM : 00000013536

Hasil Penilaian (centang salah satu)

□ Ditolak □ Diterima dengan revisi □ Diterima

Catatan Penilai (fokus pada substansi isi topik penelitian yang diajukan)

Tim Skripsi II,

**(…..………………….)**

**LEMBAR PENILAIAN**

**PROPOSAL SKRIPSI**

JUDUL : Implementasi Blockchain Pada Sistem Pemungutan Suara Elektronik Dengan Metode Konsensus *Proof-Of-Authority*

NAMA : Basilius Bias Astho Christyono

NIM : 00000013536

Hasil Penilaian (centang salah satu)

□ Ditolak □ Diterima dengan revisi □ Diterima

Catatan Penilai (fokus pada substansi isi topik penelitian yang diajukan)

Tim Skripsi III,

**(…..………………….)**