JCENIM

ISSN 2986-1764
Volume 3, Nomor 1, Maret 2025

Sistem Pengamanan Data Perhitungan Surat Suara Berbasis Metode Penyimpanan Blockchain Bertingkat

Wahyu Santoso, Arta Kusuma Hernanda

Dept. Teknik Komputer Institut Teknologi Sepuluh Nopember Surabaya, Indonesia

Email: wahyusantoso1997@gmail.com, artakusuma@its.ac.id

Abstrak

Voting adalah suatu proses untuk mengekspresikan pendapat masyarakat dalam memilih pemimpin atau dalam pengambilan keputusan. Sistem voting konvensional tidak efisien dari segi biaya dan waktu, sehingga solusinya adalah e-voting. Namun, sebagian besar sistem e-voting masih menggunakan server terpusat, sehingga sistem dapat mengalami gangguan apabila server utama mengalami kerusakan atau diretas. Oleh karena itu, pada proyek akhir ini solusi yang digunakan adalah sistem terdistribusi dengan penyimpanan data blockchain. Sistem ini akan dirancang menggunakan metode penyimpanan blockchain multilevel untuk surat suara di TPS (klien) tingkat desa, kota, provinsi, dan negara guna mengurangi waktu validasi blockchain ketika terdapat data baru. Pada proyek ini, apabila blockchain disetujui oleh lebih dari 50% node dalam jaringan, maka blockchain tersebut dinyatakan valid. Selanjutnya, dengan 100000 surat suara, sistem dapat memvalidasi pengguna yang terdaftar untuk mengirimkan surat suara satu kali dengan 0 kesalahan dari 10 kali pengujian. Selain itu, sistem mampu melakukan rekapitulasi surat suara pemilihan dengan baik. Diharapkan sistem ini dapat mengamankan data pemilihan.

Keyword: *e-voting*, *blockchain*, *sistem terdistribusi*

Diterima Redaksi: 15-Pebruari-2025 Selesai Revisi: 01-Maret-2025 Diterbitkan Online: 15-Maret-2025
DOI: https://doi.org/10.59378/jcenim.v3i1.65

I. PENDAHULUAN

Teknologi e-voting dapat menghemat biaya dan waktu dibandingkan dengan sistem voting konvensional, namun masih memiliki beberapa permasalahan keamanan, salah satunya adalah penggunaan sistem jaringan terpusat dan terdesentralisasi, yang apabila server pada jaringan tersebut diretas oleh pihak tertentu, maka surat suara atau data dapat dimanipulasi.

Blockchain merupakan model sistem terdistribusi yang dapat menjaga keamanan dan integritas surat suara pemilihan. Konsepnya adalah setiap komputer atau node dalam jaringan saling terhubung satu sama lain. Surat suara disimpan ke dalam blockchain pada setiap node dalam jaringan, sehingga data yang tersimpan bersifat identik satu sama lain. Dengan kata lain, setiap node dalam jaringan memiliki salinan data. Apabila salah satu node dalam jaringan ingin mengubah data, maka perubahan tersebut harus diverifikasi oleh lebih dari 50% node dalam jaringan, dan apabila lolos proses verifikasi, maka seluruh salinan data dalam jaringan akan diperbarui sehingga tidak terdapat perbedaan data.

Pemilihan umum tingkat nasional diikuti oleh jumlah pemilih yang sangat besar sehingga diperlukan metode penyimpanan blockchain multilevel untuk mengurangi durasi validasi blockchain ketika terdapat data baru. Tingkatan tersebut meliputi desa, kota, provinsi, dan negara. Diharapkan sistem ini dapat menjadi solusi dalam menjaga keamanan dan integritas surat suara pemilihan, karena perubahan data pada jaringan blockchain tidaklah praktis untuk dilakukan, serta dapat menjamin ketersediaan data apabila server utama atau node mengalami gangguan.

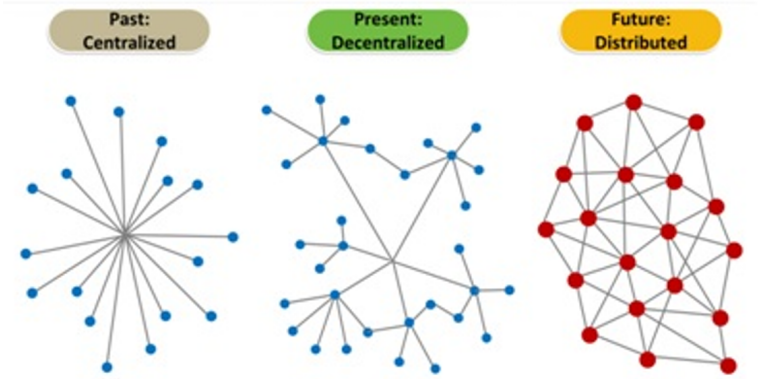
II. DASAR TEORI

A. Jaringan Terdistribusi Peer-to-Peer

Jaringan terdistribusi peer-to-peer (P2P) adalah suatu jaringan di mana setiap komputer (yang dapat disebut sebagai peer atau node) yang berada dalam jaringan saling terhubung satu sama lain tanpa adanya node pusat, atau dengan kata lain setiap komputer memiliki fungsi yang sama dalam menerima,

mengirim, dan memproses data. Jaringan P2P dapat berkembang secara luas dengan bergabungnya peer atau node baru ke dalam jaringan. Jalur komunikasi data pada jaringan P2P tidak mudah untuk dinonaktifkan karena jenis jaringan ini dapat mentransmisikan data melalui banyak jalur di antara banyak node yang tersedia dalam jaringan.

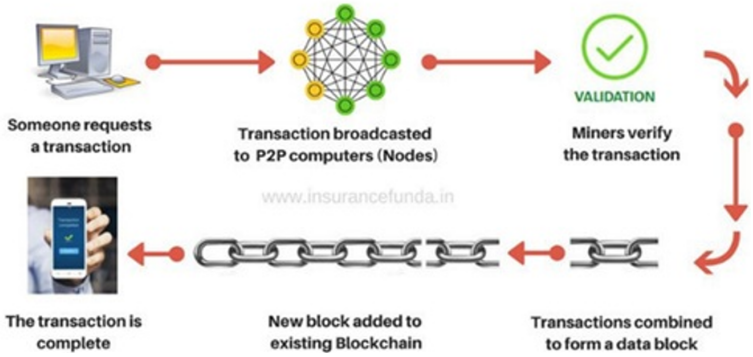
Jaringan ini tidak memerlukan kontrol terpusat maupun layanan terpusat. Pada jaringan ini, komunikasi data dapat melewati jalur node mana pun untuk mencapai tujuan, dengan kata lain apabila salah satu node mengalami gangguan, maka data dapat melewati jalur lain dan tetap mencapai tujuan. Hal ini sangat membedakan jaringan terdistribusi dengan jaringan terpusat dan terdesentralisasi, di mana apabila satu gerbang dari satu node dinonaktifkan, maka data tidak akan mencapai tujuan, sebagaimana dapat dilihat pada Gambar 1.



Gambar 1: Perbedaan dari 3 Jenis Jaringan

B. Blockchain

Blockchain adalah sebuah basis data terdistribusi yang digunakan untuk menangani pencatatan data yang terus bertambah, di mana catatan data tersebut disebut sebagai blok. Setiap blok memiliki penanda waktu dan kode unik yang terhubung dengan blok sebelumnya, sehingga setiap blok saling terhubung dan tidak dapat diubah. Blockchain biasanya dikelola oleh jaringan peer-to-peer yang secara kolektif mengikuti protokol untuk memvalidasi blok baru. Apabila terdapat perintah untuk menambahkan blok baru, maka setiap node dalam jaringan peer-to-peer akan terlebih dahulu memvalidasi blok tersebut, kemudian seluruh node akan memperbarui catatan datanya, sebagaimana ditunjukkan pada Gambar 2.



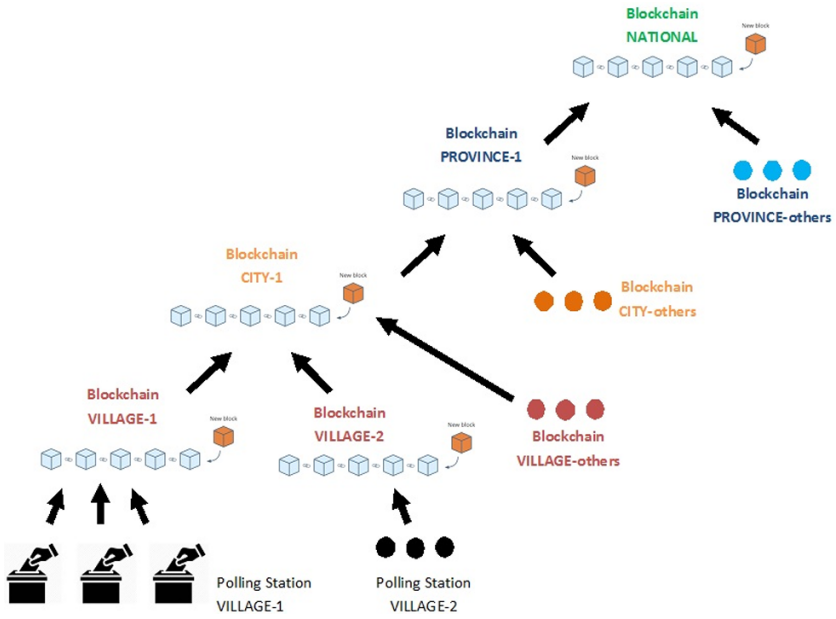
Gambar 2: Cara Kerja Blockchain

Blockchain memiliki beberapa jenis [1], yaitu Public Blockchain yang dapat diakses oleh semua orang seperti Bitcoin [3], kemudian Permissioned Blockchain yang dikendalikan oleh suatu organisasi namun dapat digunakan oleh publik, dan yang terakhir adalah Private Blockchain yang hanya dapat digunakan oleh organisasi tertentu. Jenis blockchain yang digunakan dalam Proyek Akhir ini merupakan kombinasi antara Permissioned Blockchain dan Private Blockchain.

III. PERANCANGAN DAN IMPLEMENTASI

A. Perancangan Sistem

Sistem dibangun menggunakan konsep blockchain multilevel, di mana surat suara pemilih disimpan di dalam blockchain pada setiap desa tempat pemilih terdaftar. Setelah pemilihan selesai, blockchain pada tingkat desa disimpan ke dalam jaringan blockchain pada tingkat kota, kemudian dari tingkat kota, blockchain disimpan ke tingkat provinsi dan selanjutnya ke tingkat nasional. Sistem multilevel ini dibuat untuk menangani lalu lintas yang tinggi ketika pemilihan berlangsung. Dengan demikian, jaringan blockchain hanya perlu menangani transaksi pada tingkat desa. Gambar 3 merupakan rancangan yang menggambarkan konsep dan cara kerja sistem.



Gambar 3: Cara Kerja Sistem

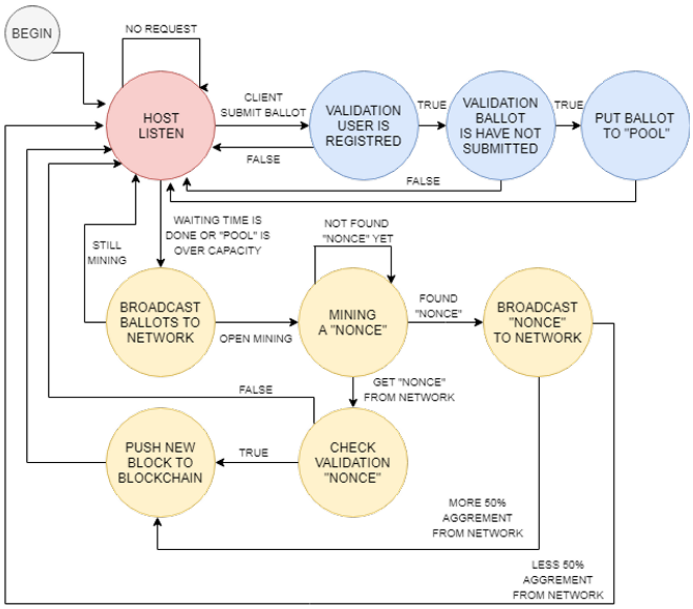
B. Perancangan Alur Kerja

Gambar 4 merupakan proses finite state machine (FSM) dari blockchain surat suara pada tingkat desa. Node sebagai host akan berada dalam kondisi mendengarkan. Apabila host menerima surat suara dari pemilih (klien), maka host akan memeriksa status surat suara tersebut di dalam jaringan, jika surat suara tersebut valid, maka surat suara akan dimasukkan ke dalam pool, yaitu wadah untuk menampung seluruh surat suara yang masuk sebelum disimpan ke dalam blockchain. Pada setiap durasi tertentu atau apabila pool telah melebihi kapasitas yang ditentukan, maka surat suara di dalam pool akan disiarkan ke seluruh node dalam jaringan untuk dilakukan proses mining, yaitu proses penyelesaian tantangan yang telah ditentukan oleh jaringan. Surat suara akan disimpan ke dalam sebuah blok baru dengan hashing yang diperoleh dari penyelesaian tantangan tersebut, kemudian blok tersebut dimasukkan ke dalam blockchain.

Sebelum sebuah blok baru dimasukkan ke dalam blockchain, blok tersebut harus disetujui sebagai blok yang valid oleh lebih dari setengah (50%) node dalam jaringan, karena blockchain tetap valid melalui pengambilan keputusan berdasarkan suara terbanyak dalam jaringan untuk menentukan penambahan blok baru yang sah. Oleh karena itu, jumlah node dalam suatu jaringan minimal adalah 3 node atau lebih (harus ganjil), untuk menghindari konflik karena keputusan validasi blok menjadi seimbang.

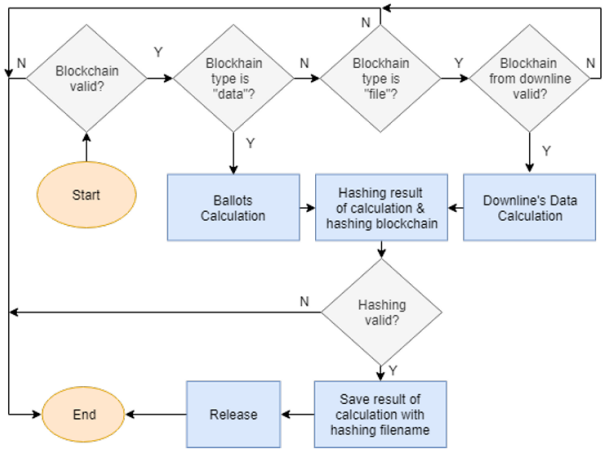
Setelah pemilihan selesai, jaringan pada tingkat paling bawah, yaitu tingkat desa, melakukan rekapitulasi surat suara dan mengirimkan hasilnya ke jaringan tingkat atas, yaitu tingkat kota. Selanjutnya, jaringan pada tingkat kota melakukan rekapitulasi hasil rekapitulasi dari setiap jaringan pada tingkat desa, demikian pula pada tingkat provinsi dan nasional.

Gambar 5 menggambarkan alur proses rekapitulasi surat suara pada tingkat desa (tipe “data”) atau tingkat atas (tipe “file”). Pada tingkat desa, surat suara di dalam blockchain direkapitulasi, kemudian hashing dari blockchain tersebut dikombinasikan dengan data rekapitulasi, dan hashing hasil rekapitulasi



Gambar 4: FSM dari Sistem

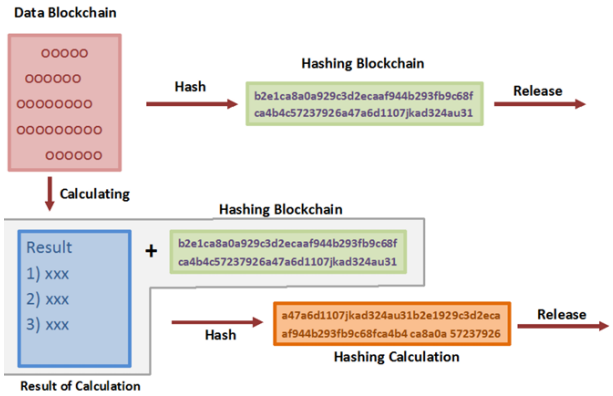
digunakan sebagai nama berkas untuk menyimpan data rekapitulasi pada tingkat desa. Pada tingkat atas, diperlukan pemeriksaan terlebih dahulu bahwa blockchain pada tingkat bawah dalam kondisi valid sebelum dilakukan rekapitulasi. Tingkat atas hanya menggabungkan seluruh data rekapitulasi dari tingkat bawah, kemudian proses selanjutnya sama seperti pada tingkat desa.



Gambar 5: Alur Kerja Perhitungan Surat Suara

C. Rilis Hasil Perhitungan Surat Suara

Blockchain dilakukan proses hashing sehingga diperoleh hashing blockchain. Selanjutnya blockchain direkapitulasi sehingga diperoleh hasil perolehan suara untuk setiap kandidat. Hasil rekapitulasi tersebut kemudian di-hash dengan hashing blockchain sehingga diperoleh hashing rekapitulasi. Hashing blockchain dan hashing rekapitulasi dikirimkan (dirilis) ke jaringan tingkat atas tanpa mengirimkan data master asli, melainkan hanya mengirimkan nama berkas berupa hashing. Hal ini dapat menghemat ruang memori pada node, karena apabila data master mengalami perubahan sebesar 1 bit saja, maka hasil rekapitulasi menjadi tidak valid akibat perbedaan nilai hashing. Gambar 6 menggambarkan alur rekapitulasi surat suara.



Gambar 6: Rilis Hasil Perhitungan Surat Suara

IV. PENGUJIAN

Pengujian pada Proyek Akhir ini meliputi pengujian fungsi sistem blockchain pada tingkat desa dan pada tingkat atas, serta pengujian kinerja dan efisiensi sistem.

A. Perangkat

Terdapat 3 komputer dengan spesifikasi yang berbeda.

1) PC1 - RAM 4 GB - CPU 2 core 1.8 GHz
2) PC2 - RAM 8 GB - CPU i5 4 core 1.8 GHz
3) PC3 - RAM 16 GB - CPU i7 4 core 3.5 GHz

B. Data Simulasi

Terdapat 100000 data (surat suara) dengan nomor identitas pemilih terdaftar dari 2000001 sampai 2100000 dan kata sandi adalah “secret”.

C. Validasi Blockchain

Pengujian ini dilakukan dengan memanipulasi data menggunakan 3 kombinasi node yang berbeda. Lihat Tabel 1.

Tabel 1: Validasi Blockchain

Node yang Dimanipulasi	Status Blockchain pada Node			Status Blockchain pada Jaringan
	1	2	3	
Tidak ada	Valid	Valid	Valid	Valid
1	Tidak Valid	Valid	Valid	Valid
2	Valid	Tidak Valid	Valid	Valid
3	Valid	Valid	Tidak Valid	Valid
1,2	Tidak Valid	Tidak Valid	Valid	Tidak Valid
1,3	Tidak Valid	Valid	Tidak Valid	Tidak Valid
2,3	Valid	Tidak Valid	Tidak Valid	Tidak Valid
1,2,3	Tidak Valid	Tidak Valid	Tidak Valid	Tidak Valid

Berdasarkan pengujian ini, sistem dapat melakukan validasi blockchain dengan baik, di mana blockchain dinyatakan valid apabila data pada setiap node bersifat identik. Pada kasus manipulasi data

pada satu node saja, blockchain menjadi tidak valid hanya pada node tersebut, sedangkan node lainnya tetap valid. Pada kasus manipulasi data pada lebih dari satu node, maka blockchain pada seluruh node menjadi tidak valid, karena hasil validasi blockchain kurang dari 50% node dalam jaringan.

D. Durasi Pengiriman Surat Suara

Pengujian dilakukan menggunakan 10, 20, dan 40 klien secara bersamaan pada setiap komputer, dengan tingkat kesulitan mining sebesar 3 dan 4. Hasil pengujian dapat dilihat pada Tabel 2 dan Tabel 3.

Tabel 2: Durasi Pengiriman Surat Suara (Tingkat Kesulitan Mining 3)

Kon. Klien	Total Durasi (detik)			Durasi Rata-rata (detik)		
	PC1	PC2	PC3	PC1	PC2	PC3
10	111987.56	36191.25	24637.67	11.19	3.61	2.46
20	101139.68	34916.06	23684.91	20.22	6.98	4.73
40	98780.30	31229.17	21924.27	39.51	12.49	8.76

Tabel 3: Durasi Pengiriman Surat Suara (Tingkat Kesulitan Mining 4)

Kon. Klien	Total Durasi (detik)			Durasi Rata-rata (detik)		
	PC1	PC2	PC3	PC1	PC2	PC3
10	149941.15	36043.26	25161.47	14.99	3.60	2.51
20	135709.54	31476.08	18467.56	27.14	6.29	3.69
40	122378.66	26039.48	14160.79	48.95	10.41	5.66

Berdasarkan pengujian yang ditunjukkan pada Tabel 2 dan Tabel 3, apabila semakin banyak klien yang mengirimkan surat suara secara bersamaan, maka durasi rata-rata yang dibutuhkan pemilih untuk mengirimkan surat suara menjadi lebih lama, namun total durasi yang dibutuhkan untuk keseluruhan pemilihan menjadi lebih cepat. Dari hasil tersebut, durasi yang dibutuhkan oleh PC1 setidaknya 5 kali lebih lama dibandingkan PC2, karena spesifikasi PC2 lebih baik daripada PC1. PC2 hanya membutuhkan waktu sekitar 6 jam untuk proses pemilihan, sehingga sistem dengan spesifikasi PC2 merupakan spesifikasi minimal yang diperlukan agar sesuai dengan waktu yang dibutuhkan pada pemilihan konvensional (untuk 100000 pemilih terdaftar).

E. Durasi Pembuatan Blok Baru

Pengujian dilakukan menggunakan 10, 20, dan 40 klien secara bersamaan pada setiap komputer, dengan tingkat kesulitan mining sebesar 3 dan 4. Blok baru dibuat apabila jumlah surat suara di dalam pool lebih dari 50 atau setiap 2 menit. Hasil pengujian dapat dilihat pada Tabel 4 dan Tabel 5.

Tabel 4: Durasi Pembuatan Blok Baru (Tingkat Kesulitan Mining 3)

Kon. Klien	Blok Dibuat			Durasi Rata-rata (dtk/blok)			Surat Suara Rata-rata (suara/blok)		
	PC1	PC2	PC3	PC1	PC2	PC3	PC1	PC2	PC3
10	1067	2113	2074	104.12	52.47	3.65	93.72	47.32	48.21
20	521	2096	2046	193.90	50.42	6.47	191.93	47.70	48.87
40	275	1961	1684	359.56	64.45	11.52	363.63	50.99	59.38

Berdasarkan pengujian yang ditunjukkan pada Tabel 4 dan Tabel 5, apabila jumlah klien simultan sangat banyak, maka blok yang dihasilkan menjadi sangat sedikit, karena durasi rata-rata yang dibutuhkan untuk memvalidasi dan membuat blok baru menjadi sangat lama, sehingga jumlah surat suara dalam setiap blok menjadi sangat banyak.

Tabel 5: Durasi Pembuatan Blok Baru (Tingkat Kesulitan Mining 4)

Konfigurasi Klien	Blok Dibuat			Durasi Rata-rata (dtk/blok)			Surat Suara Rata-rata (suara/blok)		
	PC1	PC2	PC3	PC1	PC2	PC3	PC1	PC2	PC3
10	968	1725	1820	154.15	85.75	59.26	103.36	57.97	54.94
20	499	1012	738	271.48	131.29	24.00	200.49	98.81	135.50
40	248	725	140	494.04	242.36	92.05	403.22	237.97	314.28

F. Perhitungan Surat Suara

Pada pengujian ini, perhitungan dilakukan dari tingkat desa hingga tingkat nasional. Sebanyak 3 kandidat dipilih secara acak dengan nomor 1, 2, dan 3.

Berikut merupakan perhitungan surat suara pada tingkat desa. Lihat Tabel 6.

Tabel 6: Perhitungan Surat Suara pada Tingkat Desa

Nama Desa	Nama Kota	Jumlah Surat Suara	Total Suara		
			1	2	3
Village-A	City-A	40000	19034	19044	1922
Village-B	City-A	100000	47770	47158	5072

Berikut merupakan perhitungan surat suara pada tingkat kota. Lihat Tabel 7.

Tabel 7: Perhitungan Surat Suara pada Tingkat Kota

Nama Kota	Nama Provinsi	Jumlah Surat Suara	Total Suara		
			1	2	3
City-A	Province-A	140000	66804	66202	6994
City-Others	Province-A	1000	339	633	28

Berikut merupakan perhitungan surat suara pada tingkat provinsi. Lihat Tabel 8.

Tabel 8: Perhitungan Surat Suara pada Tingkat Provinsi

Nama Provinsi	Nama Negara	Jumlah Surat Suara	Total Suara		
			1	2	3
Province-A	Indonesia	141000	67143	66835	7022
Province-Others	Indonesia	1000	614	195	191

Berikut merupakan perhitungan surat suara pada tingkat nasional. Lihat Tabel 9.

Tabel 9: Perhitungan Surat Suara pada Tingkat Nasional

Nama Negara	Jumlah Surat Suara	Total Suara		
		1	2	3
Indonesia	142000	67757	67030	7213

Berdasarkan pengujian ini, sistem dapat melakukan perhitungan surat suara dari blockchain dengan baik. Surat suara dikelompokkan dan dihitung sehingga diperoleh hasil perolehan suara untuk setiap kandidat.

V. KESIMPULAN

1) Sistem dapat melakukan validasi blockchain. Apabila blockchain disetujui oleh lebih dari 50% node dalam jaringan, maka blockchain dinyatakan valid, sedangkan apabila tidak lebih dari 50%, maka blockchain dinyatakan tidak valid.

2) Rata-rata total durasi pengiriman surat suara pada PC1 adalah 33 jam, pada PC2 adalah 9 jam, dan pada PC3 hanya 6 jam.

3) Rata-rata durasi yang dibutuhkan untuk membuat blok baru pada PC1 adalah 262.89 detik/blok, pada PC2 adalah 19.47 detik/blok, dan pada PC3 adalah 24.49 detik/blok.

4) Dan sistem mampu melakukan rekapitulasi surat suara pemilihan dengan baik.

Daftar Pustaka

[1] M. Gupta, *Blockchain For Dummies*. United States of America: John Wiley and Sons Inc., 2017.

[2] A. Rayendra, "Rancang bangun sistem e-voting dengan menggunakan teknologi blockchain," Master's thesis, Politeknik Negeri Padang, Padang, 2017.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin.org, 2009.

[4] M. Hajjar *et al.*, "An e-voting system for lebanese elections," *Journal of Theoretical and Applied Information Technology*, 2006.

[5] C. Zamora *et al.*, "Seles: An e-voting system for medium scale online elections," in *Proceedings of the 6th Mexican International Conference on Computer Science (ENC'05)*, 2005.

[6] C. Z. and A. Pilkjar, "E-voting in pakistan," Master's thesis, Department of Business Administration and Social Sciences, Lulea University of Technology, 2007.

[7] L. H. and V. M. Simarmata, "E-voting: Kebutuhan vs. kesiapan (menyongsong) e-demokrasi," Jawa Barat, 2011.