



PERANCANGAN E-VOTING BERBASIS SMART CONTRACT MENGGUNAKAN KEAMANAN ALGORITMA KONSENSUS PROOF-OF-STAKE

Adi Gunawan Lase¹,
Mariska Putri Pratiwi²

¹Mahasiswa Program Studi Teknik Informatika, Universitas Putera Batam

²Dosen Program Studi Teknik Informatika, Universitas Putera Batam
email: pb200210106@upbatam.ac.id

ABSTRACT

The advancement of digital technology has created opportunities for efficiency in voting processes through e-voting system. However, the conventional e-voting systems are often vulnerable to cyber attacks and data manipulation. The main issue lies in the centralized architecture of these systems, which present significant security risks. This study explores the implementation of a more secured e-voting system built on blockchain technology, utilizing smart contracts on the Ethereum platform, that leverages the Proof-of-stake consensus with specific focus on vendor selection. By utilizing a decentralized architecture, the blockchain-based system eliminates single points of failure and distributes data across multiple nodes, significantly reducing the risk of manipulation or unauthorized access. This research concludes that the implementation of blockchain technology, especially that leverages the PoS consensus algorithm and smart contract on the Ethereum platform, can perform effectively and provide enhanced security compared to conventional e-voting systems.

Keywords: *blockchain, e-voting, ethereum, proof-of-stake, smart contract.*

PENDAHULUAN

Kemajuan teknologi digital pada era modern telah menghadirkan transformasi besar-besaran di banyak bidang kehidupan, tak terkecuali dalam sistem pemilihan umum. Sistem *e-voting* muncul sebagai solusi untuk meningkatkan efisiensi, akurasi, dan aksesibilitas dalam proses pemilihan. Menurut (Pramulia & Anggorajati, 2020), *e-voting* dapat mengurangi risiko kecurangan seperti pemalsuan identitas dan manipulasi hasil pemilihan. Selain itu, *e-voting* mampu menghemat waktu, biaya, dan usaha

serta mempercepat proses penghitungan suara (Jaya, Ariati, & Pratiwi, 2023).

Namun, sistem *e-voting* konvensional masih memiliki kelemahan terutama terkait dengan arsitekturnya yang tersentralisasi yang rentan terhadap serangan siber. Dalam sistem yang tersentralisasi, data tersimpan pada satu lokasi pusat, menciptakan titik lemah yang dapat dieksploitasi oleh penyerang (Christophorus Prasetyadi, Benny Mutiara, & Refianti, 2020). Dengan arsitektur yang tersentralisasi juga mempermudah bagi orang yang punya akses fisik ke sistem secara langsung



untuk melakukan manipulasi data (Farooq, Iftikhar, & Khelifi, 2022).

Teknologi *blockchain* hadir sebagai solusi potensial untuk mengatasi kelemahan ini. Dengan prinsip desentralisasi, setiap transaksi pada *blockchain* disimpan dalam blok-blok yang terkait satu sama lain melalui tautan kriptografi, dan diamankan serta disinkronisasikan oleh mekanisme konsensus sehingga menciptakan rantai data yang tidak dapat diubah dan jika ada penyusup yang melakukan modifikasi akan terdeteksi (Singh & Vardhan, 2020).

Penelitian ini bertujuan untuk mengeksplorasi implementasi sistem *e-voting* berbasis *blockchain* menggunakan *smart contract* pada platform *Ethereum*, yang menggunakan mekanisme konsensus *Proof-of-Stake (PoS)*. Studi kasus yang digunakan adalah pemilihan vendor di PT Bintan Teknologi Kreatif, memberikan konteks praktis untuk menguji efektivitas sistem dalam skenario dunia nyata.

TINJAUAN PUSTAKA

2.1 *E-voting*

E-voting (electronic voting) merupakan sistem pemungutan suara yang memanfaatkan teknologi digital untuk meningkatkan efisiensi, akurasi, dan aksesibilitas dalam proses pemilihan. Selain itu, sistem *e-voting* juga membuka potensi partisipasi yang lebih luas karena mengurangi hambatan dalam sisi aksesibilitas karena sistem ini bisa membantu pemilih untuk berpartisipasi dalam proses pemilihan dari lokasi mana pun, sehingga memudahkan pemilih yang berada jauh dari pusat pemungutan suara (G. Kalaiyarasi et al., 2020).

2.2 *Blockchain*

Menurut (Chaieb, Yousfi, Lafourcade, & Robbana, 2019), *blockchain* didefinisikan sebagai sistem catatan yang terdesentralisasi, di mana transaksi disimpan secara terdistribusi dalam sebuah jaringan dengan aman tanpa memerlukan kontrol dari sebuah entitas sentral.

Blockchain pertama kali diperkenalkan oleh Satoshi Nakamoto dalam sebuah paper yang ia publikasikan (Nakamoto, 2008), di mana ia menjelaskan tentang sebuah mekanisme pembayaran secara peer-to-peer tanpa membutuhkan campur tangan dari institusi apa pun.

2.3 *Smart contract*

Smart contract adalah kontrak yang berjalan secara otomatis dengan ketentuan yang telah diprogram sebelumnya di dalam *blockchain*, sehingga kontrak bisa berjalan tanpa membutuhkan pihak ketiga. Konsep *smart contract* awalnya dikembangkan untuk mengotomatisasi kontrak hukum yang mampu di implementasikan ke dalam perangkat lunak (Zou et al., 2021).

2.4 *Ethereum*

Ethereum adalah sebuah platform *blockchain* yang mengembangkan teknologi *blockchain* sebelumnya yang digunakan di *Bitcoin* dengan mendukung aplikasi yang lebih kompleks daripada sekedar transaksi keuangan. Aplikasi ini dikenal dengan nama *smart contract* (kontrak pintar), yang berjalan di atas *Ethereum Virtual Machine (EVM)*, yang merupakan lingkungan komputasi terdistribusi dan terdesentralisasi (Chen et al., 2020), yang memungkinkan pengguna untuk membuat aturan kontrak tertentu dari sebuah skrip program tanpa perlu adanya otoritas pusat.

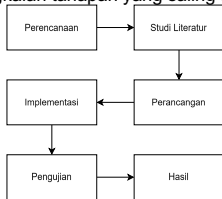
2.5 *Proof-of-stake*

Proof-of-stake adalah mekanisme konsensus di mana penciptaan blok baru dan validasi transaksi tergantung pada jumlah koin atau *stake* yang dipegang oleh *validator*. *Node* yang mempunyai jumlah *stake* lebih tinggi memiliki kemungkinan lebih tinggi untuk terpilih sebagai *validator* pada blok berikutnya. Ini secara signifikan mengurangi kebutuhan akan perangkat keras yang mahal dan konsumsi energi yang besar.

METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian terdiri dari serangkaian tahapan yang saling terkait:



Gambar 1. Desain Penelitian

(Sumber: Data olahan peneliti, 2024)

Definisi dari setiap tahapan desain penelitian tersebut adalah sebagai berikut:

a. Perencanaan

Tahap ini mencakup penentuan tujuan penelitian, yaitu pengembangan sistem *e-voting* yang aman, efisien, dan transparan menggunakan mekanisme konsensus *Proof-of-Stake (PoS)* pada platform *Ethereum* dengan studi kasus yang digunakan adalah pemilihan vendor di PT Bintang Teknologi Kreatif.

b. Studi literatur

Dilakukan pengumpulan dan analisis penelitian sebelumnya yang relevan dengan *e-voting*, *blockchain*, dan

Proof-of-stake untuk memahami teori dan konsep dasar yang mendasari penelitian.

c. Perancangan sistem

Menggunakan metode *Waterfall*, perancangan sistem melibatkan pembuatan diagram alur dan arsitektur sistem, termasuk desain *smart contract*, yang diilustrasikan melalui diagram UML.

d. Implementasi

Proses implementasi sistem meliputi pengembangan antarmuka pengguna dan *smart contract* pada platform blockchain *Ethereum*.

e. Pengujian

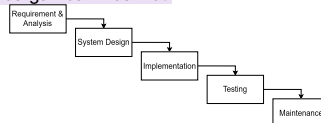
Metode *blackbox testing* diterapkan untuk menguji fungsionalitas sistem secara menyeluruh untuk memastikan bahwa seluruh elemen dari sistem beroperasi sesuai dengan yang telah direncanakan.

f. Hasil

Hasil penelitian adalah berupa sistem *e-voting* yang berbasis *blockchain* dan telah diuji untuk kemudian diimplementasikan untuk pemilihan vendor di PT Bintang Teknologi Kreatif.

3.2 Metode Perancangan Sistem

Sistem dikembangkan dengan metode *Waterfall*, yang mencakup tahapan seperti pada gambar 2 berikut:



Gambar 2. Alur metode *Waterfall*

(Sumber: Data olahan peneliti, 2024)

a. Requirement & analysis

Identifikasi kebutuhan, baik itu fungsional maupun non-fungsional dari sistem *e-voting* yang ingin dibuat.

b. System Design

Commented [SSSM1]: Gambar maupun tabel seharusnya di attach dalam penjelasan.
Mis. Mencakup tahapan seperti gambar 2 berikut.

Merancang arsitektur sistem, termasuk komponen *front-end*, *back-end*, dan *smart contract*.

c. *Implementation*

Implementasi dari rancangan sistem yang telah dibuat di tahap sebelumnya.

d. *Testing*

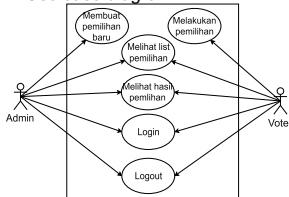
Pengujian sistem menggunakan metode *black box testing*. Pengujian ini bertujuan untuk memastikan seluruh fungsionalitas dari sistem beroperasi sesuai rencana.

e. *Maintenance*

Monitoring sistem untuk mendeteksi dan memperbaiki *bug* atau masalah yang muncul setelah pengujian, serta melakukan pembaruan sesuai kebutuhan.

3.2 Metode UML

3.2.1 Use case diagram



Gambar 3. Use case diagram

(Sumber: Data olahan peneliti, 2024)

Diagram ini efektif menggambarkan interaksi pengguna dengan sistem, membedakan peran dan akses admin dan voter, serta menyajikan gambaran singkat fungsi utama sistem pemilihan.

3.2.2 Activity Diagram

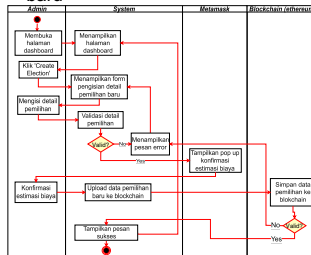
Diagram ini berfungsi untuk memodelkan urutan proses operasional sebuah sistem.

a. Activity diagram login



Gambar 4. Activity diagram login
(Sumber: Data olahan peneliti, 2024)

b. Activity diagram membuat pemilihan baru

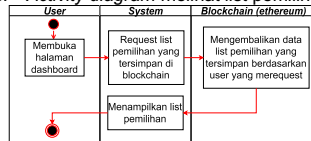


Gambar 5. Activity diagram membuat pemilihan baru

(Sumber: Data olahan peneliti, 2024)

Berdasarkan diagram ini, hanya admin yang mempunyai wewenang untuk melakukan pembuatan pemilihan baru.

c. Activity diagram melihat list pemilihan



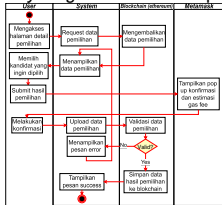
Gambar 6. Activity diagram melihat list pemilihan

(Sumber: Data olahan peneliti, 2024)

Berdasarkan diagram tersebut, list pemilihan tersimpan di *blockchain* dan

sistem hanya akan mengembalikan list pemilihan kepada user yang berhak.

d. *Activity diagram* melakukan pemilihan

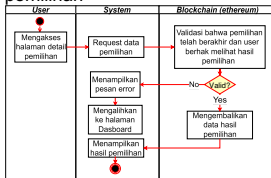


Gambar 7. *Activity diagram* melakukan pemilihan

(Sumber: Data olahan peneliti, 2024)

Diagram ini menjelaskan mengenai proses pemilihan oleh user. User bisa memilih kandidat yang telah ditentukan pada saat proses pembuatan pemilihan.

e. *Activity diagram* melihat hasil pemilihan

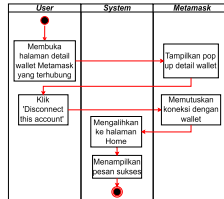


Gambar 8. *Activity diagram* melihat hasil pemilihan

(Sumber: Data olahan peneliti, 2024)

Diagram ini menggambarkan proses melihat hasil pemilihan, meliputi validasi untuk keamanan data, penanganan error yang efisien, dan fokus pada pengalaman pengguna.

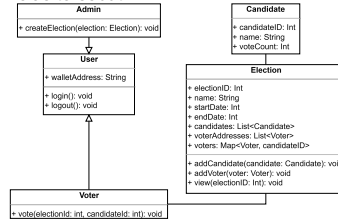
f. *Activity diagram* logout



Gambar 9. *Activity diagram* logout (Sumber: Data olahan peneliti, 2024)
Diagram ini menjelaskan proses logout oleh user. Metamask digunakan sebagai metode autentikasi user.

3.2.4 Class diagram

Class diagram menggambarkan struktur objek dalam suatu sistem dengan menampilkan kelas-kelas yang menyusun sistem tersebut serta hubungan antar kelas tersebut.



Gambar 10. *Class diagram*

(Sumber: Data olahan peneliti, 2024)

3.3 Metode Pengujian Sistem

Studi ini menerapkan metode pengujian *black box testing*. Pengujian ini dilaksanakan dengan memeriksa setiap komponen aplikasi guna memastikan seluruh fungsinya beroperasi sesuai rancangan yang ditentukan. Berikut adalah beberapa langkah dalam pengujian *black box testing* untuk sistem e-voting yang dibuat:

Tabel 1. Langkah pengujian sistem



No.	Fungsionalitas	Skenario Uji	Input	Output yang diharapkan
1	Login dengan MetaMask	Akses halaman login dan klik "Connect MetaMask".	Tombol "Connect MetaMask" diklik.	MetaMask pop-up muncul, user pilih wallet dan berhasil login
2	Pembuatan pemilihan baru oleh Admin	Admin mengisi detail pemilihan dan mengklik "Submit".	Detail pemilihan	Pemilihan baru berhasil dibuat dan muncul di dashboard.
3	Proses pemungutan suara oleh voter	Voter memilih kandidat dan klik "Submit".	Pilihan kandidat yang dipilih.	Suara berhasil tercatat di blockchain.
4	Melihat daftar pemilihan yang tersedia	User akses dashboard untuk melihat pemilihan yang tersedia.	User buka halaman dashboard.	Tampilkan pemilihan yang mendatang / sedang berlangsung.
5	Melihat hasil pemilihan yang telah selesai	User klik tombol "View" untuk melihat hasil pemilihan yang telah selesai.	Tombol "View" diklik pada pemilihan yang telah selesai.	Hasil pemilihan ditampilkan dengan grafik.

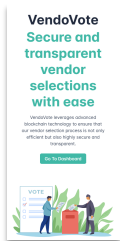
(Sumber: Data olahan peneliti, 2024)

HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Hasil dari penelitian ini merupakan implementasi rancangan antarmuka yang direncanakan pada tahap sebelumnya.

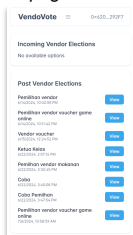
a. Home page



Gambar 11. Antarmuka home page (Sumber: Data olahan peneliti, 2024)
Home page adalah halaman pertama yang dilihat oleh pengguna ketika mereka mengakses aplikasi. Halaman ini

dirancang untuk memberikan kesan pertama yang kuat dan menggambarkan misi utama dari sistem e-voting.

b. Dashboard page



Gambar 12. Antarmuka dashboard (Sumber: Data olahan peneliti, 2024)
Dashboard adalah halaman yang bisa diakses setelah pengguna login. Halaman ini menampilkan pemilihan vendor yang sedang berlangsung dan mendatang.

Commented [SSSM2]: Ikuti sesuai template

Tabel 1. Jumlah Produk

No.	Jumlah Produksi	Jumlah Produk	Jumlah P
1	50	45	1 5
3			

Jurnal Comasie - Vol. 08 No. 01 (2023)

UPB
Universitas Putera Batam
LPPM
UNIVERSITAS PUTERA BATAM

Terbit online pada laman web jurnal : <http://ejournal.upbatam.ac.id/index.php/comasiejournal>

Jurnal Comasie
ISSN (Online) 2715-6265

2	55	50	2 5
3	45	40	3 5
4	50	45	2 5
5	55	45	2 10
6	45	35	2 10
7	55	45	2 5 10

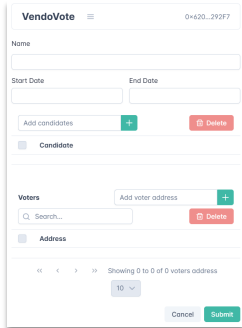
(Sumber: Data Penelitian, 2019)

Hasil penelitian yang dihasilkan oleh: **DAETA D**

serta memungkinkan akses cepat ke fitur-fitur utama.

c. *Create election page*

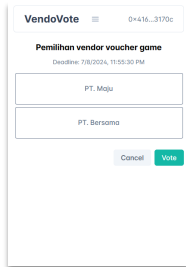
Halaman *create election* memungkinkan admin untuk membuat pemilihan vendor baru. Halaman ini hanya bisa diakses oleh admin dan dirancang untuk intuitif dan mudah digunakan.



Gambar 13. Antarmuka *create election* (Sumber: Data olahan peneliti, 2024)

d. *Vote page*

Halaman *vote* adalah tempat di mana pengguna dapat memberikan suara mereka dalam pemilihan vendor.

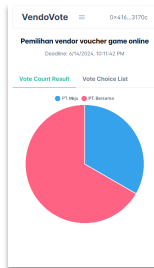


Tabel 2. Hasil pengujian sistem

Gambar 14. Antarmuka halaman *vote* (Sumber: Data olahan peneliti, 2024)

e. *View results page*

Halaman *view results* adalah halaman di mana pengguna dapat melihat hasil dari pemilihan vendor yang telah selesai.



Gambar 15. Antarmuka halaman *view results* (Sumber: Data olahan peneliti, 2024)

4.2 Pembahasan

Pada bagian ini menguraikan hasil pengujian dari sistem *e-voting* berbasis *blockchain* yang telah selesai dibuat. Pengujian dilakukan dengan menggunakan metode *black box testing* untuk memverifikasi apakah sistem telah beroperasi sesuai harapan atau tidak.



No.	Fitur	Skenario Uji	Hasil yang diharapkan	Hasil pengujian
1	Login menggunakan <i>metamask</i>	User klik "Connect <i>MetaMask</i> " di halaman login.	<i>MetaMask pop-up</i> muncul dan user berhasil login setelah melakukan konfirmasi.	Berfungsi dengan baik.
2	Pembuatan pemilihan baru oleh admin	Admin mengisi detail pemilihan dan mengklik tombol "Submit".	Pemilihan baru berhasil dibuat dan disimpan di <i>blockchain</i> .	Berfungsi dengan baik.
4	Melihat daftar pemilihan	Pengguna mengakses halaman <i>dashboard</i> untuk melihat daftar pemilihan.	Daftar pemilihan yang sedang berlangsung ditampilkan.	Berfungsi dengan baik.
3	Proses pemungutan suara oleh voter	Pengguna memilih kandidat dan mengklik tombol "Submit".	Suara berhasil dikirim dan dicatat di <i>blockchain</i> .	Berfungsi dengan baik.
5	Melihat hasil pemilihan	Pengguna klik tombol "View" untuk melihat hasil pemilihan yang selesai.	Hasil pemilihan ditampilkan dengan grafik hasil suara.	Berfungsi dengan baik.

Commented [SSM3]: Ikuti sesuai template penulisan tabel

(Sumber: Data Olahan Peneliti, 2024)

Hasil pengujian dengan metode *blackbox testing* menunjukkan bahwa semua fitur utama dalam sistem *e-voting* berbasis *blockchain* ini berfungsi dengan baik. Tidak ditemukan kesalahan atau masalah yang signifikan selama pengujian, sehingga dapat disimpulkan bahwa sistem telah berjalan dengan baik dan siap digunakan untuk proses pemilihan vendor.

SIMPULAN

Berdasarkan pada hasil penelitian dan pengujian yang dilaksanakan, berikut adalah kesimpulan yang dapat dirumuskan:

1. Implementasi *smart contract* pada platform *Ethereum* untuk membuat sebuah sistem *e-voting* menunjukkan bahwa proses pemilihan dapat dilakukan secara lebih efisien, dengan mengurangi risiko kesalahan manusia dan mempercepat perhitungan suara.
2. Teknologi *blockchain* dengan mekanisme konsensus *PoS* berhasil

meningkatkan keamanan dan transparansi dalam sistem *e-voting*. Setiap transaksi terekam secara desentralisasi sehingga sangat sulit untuk dimanipulasi atau diubah tanpa terdeteksi.

3. Hasil pengujian dengan metode *black box testing* mengindikasikan bahwa sistem yang dikembangkan dapat beroperasi dengan baik tanpa ditemukan kesalahan atau masalah yang signifikan. Hal ini menunjukkan bahwa sistem *e-voting* berbasis *blockchain* ini siap digunakan untuk pemilihan vendor di PT Bintang Teknologi Kreatif.

DAFTAR PUSTAKA

- Chaieb, M., Yousofi, S., Lafourcade, P., & Robbana, R. (2019). Verify-your-vote: A verifiable blockchain-based online



- voting protocol. *Lecture Notes in Business Information Processing*, 341, 16–30. Springer Verlag. https://doi.org/10.1007/978-3-030-11395-7_2
- Chen, T., Li, Z., Zhu, Y., Chen, J., Luo, X., Lui, J. C. S., ... Zhang, X. (2020). Understanding Ethereum via Graph Analysis. *ACM Transactions on Internet Technology*, 20(2). <https://doi.org/10.1145/3381036>
- Christophorus Prasetyadi, G., Benny Mutiara, A., & Refianti, R. (2020). Blockchain-based Electronic Voting System with Special Ballot and Block Structures that Complies with Indonesian Principle of Voting. In *IJACSA International Journal of Advanced Computer Science and Applications* (Vol. 11). Retrieved from www.ijacsa.thesai.org
- G. Kalaiyarasi, K. Balaji, T. Narmadha, & V. Naveen. (2020). E-Voting System In Smart Phone Using Mobile Application. *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*.
- Jaya, P., Ariati, N., & Pratiwi, M. P. (2023). SISTEM INFORMASI E-VOTING PEMILIHAN KEPALA DESA DI DESA KUANG DALAM TIMUR KABUPATEN OGAN ILIR. In *Prosiding Seminar Nasional Teknologi Komputer dan Sains* (Vol. 1).
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from www.bitcoin.org
- Pramulia, D., & Anggorojati, B. (2020). Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask. *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, 18–23. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICIMCIS51567.2020.9354310>
- Singh, N., & Vardhan, M. (2020). Computing Optimal Block Size for Blockchain based Applications with Contradictory Objectives. *Procedia Computer Science*, 171, 1389–1398. Elsevier B.V. <https://doi.org/10.1016/j.procs.2020.04.149>
- Zou, W., Lo, D., Kochhar, P. S., Le, X. B. D., Xia, X., Feng, Y., ... Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, 47(10), 2084–2106. <https://doi.org/10.1109/TSE.2019.2942301>

	<p>Biodata Penulis pertama, Adi Gunawan Lase, merupakan Mahasiswa Prodi Teknik Informatika Universitas Putera Batam. Email : pb200210106@upbatam.ac.id</p>
	<p>Biodata Penulis kedua, Mariska Putri Pratiwi, S.SI., M.IT. merupakan Dosen Prodi Teknik Informatika Universitas Putera Batam. Email : mrskaptrw@gmail.com</p>