

**PEMUNGUTAN SURAT SUARA ELEKTRONIK
MENGUNAKAN *BLOCKCHAIN* DAN *DIGITAL IDENTITY***



Oleh:

Nama : Raka Adi Nugroho

NIM : 19206050006

**PROGRAM STUDI INFORMATIKA
PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA**

2023

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Raka Adi Nugroho
NIM : 19206050006
Jenjang : Magister
Program Studi : Informatika

Menyatakan bahwa naskah tesis ini secara keseluruhan adalah hasil penelitian / karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya

Yogyakarta, 23 Januari 2023

Yang menyatakan,



Raka Adi Nugroho

NIM: 19206050006

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan di bawah ini:

Nama : Raka Adi Nugroho

NIM : 19206050006

Jenjang : Magister

Program Studi : Informatika

Menyatakan bahwa naskah tesis ini secara keseluruhan benar-benar bebas dari plagiasi. Jika di kemudian hari terbukti melakukan plagiasi, maka saya siap ditindak sesuai dengan ketentuan hukum yang berlaku

Yogyakarta, 23 Januari 2023

Yang menyatakan,



Raka Adi Nugroho

NIM: 19206050006



PENGESAHAN TUGAS AKHIR

Nomor : B-281/Un.02/DST/PP.00.9/01/2023

Tugas Akhir dengan judul : PEMUNGUTAN SURAT SUARA ELEKTRONIK MENGGUNAKAN BLOCKCHAIN DAN DIGITAL IDENTITY

yang dipersiapkan dan disusun oleh:

Nama : RAKA ADI NUGROHO, S.Kom
Nomor Induk Mahasiswa : 19206050006
Telah diujikan pada : Rabu, 25 Januari 2023
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR



Ketua Sidang

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.
SIGNED

Valid ID: 63d3772c69ed3



Penguji I

Dr. Agung Fatwanto, S.Si., M.Kom.
SIGNED

Valid ID: 63d4bfd6c776



Penguji II

Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom.
SIGNED

Valid ID: 63d66692a2813



Yogyakarta, 25 Januari 2023

UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi
Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 63d72cc506da6

NOTA DINAS PEMBIMBING

Kepada Yth.,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga
Yogyakarta

Assalamu'alaikum wr. wb.

Setelah melakukan bimbingan, arahan, dan koreksi terhadap penulisan tesis yang berjudul:

**PEMUNGUTAN SURAT SUARA ELEKTRONIK
MENGUNAKAN BLOCKCHAIN DAN DIGITAL IDENTITY**

Yang ditulis oleh:

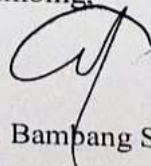
Nama : Raka Adi Nugroho
NIM : 19206050006
Jenjang : Magister
Program Studi : Informatika

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Magister Informatika UIN Sunan Kalijaga untuk diujikan dalam rangka memperoleh gelar Magister Informatika.

Wassalamu'alaikum wr. wb.

Yogyakarta, 14 Desember 2022

Pembimbing,



Dr. Ir. Bambang Sugiantoro, S.Si., M.T.

NIP: 197701032005011003

ABSTRACT

Blockchain technology is increasingly being used for various applications, including voting systems. Blockchain-based voting ensures the integrity and transparency of voting data, and digital identity is used to ensure that only eligible voters can participate. This research discusses the use of blockchain technology for voting systems with a focus on integration with Digital Identity. Using Algorand as the blockchain layer-1 network and OREID as the digital identity provider, the combination of blockchain and digital identity provides a strong solution for fair and secure elections. The research focuses on architecture design, including the creation of smart contracts, application development, and system architecture testing. The research results in a blockchain-based architecture that can be integrated with digital identity platforms. This approach not only improves the security and transparency of the voting process, but also makes the user experience easier.

Keywords: *Blockchain, Proof of Stake, Voting, Algorand, Digital Identity*

ABSTRAK

Teknologi *blockchain* semakin banyak digunakan untuk berbagai aplikasi, termasuk *voting system*. *Voting* berbasis *blockchain* memastikan integritas dan transparansi dari data pemilihan, serta identitas digital digunakan untuk memastikan bahwa hanya pemilih yang berhak yang dapat berpartisipasi. Penelitian ini membahas tentang penggunaan teknologi *blockchain* untuk *system voting* dengan fokus pada integrasi dengan *Digital Identity*. Menggunakan *Algorand* sebagai *layer-1* jaringan *blockchain* dan juga *OREID* sebagai penyedia *digital identity*, kombinasi dari *blockchain* dan identitas digital menyediakan solusi yang kuat untuk pemilihan yang adil dan aman. Penelitian berpusat pada rancangan arsitektur, termasuk pembuatan *smart contract*, pengembangan aplikasi dan pengujian arsitektur sistem. Dari penelitian ini dihasilkan arsitektur berbasis *blockchain* dapat diintegrasikan dengan *platform digital identity*. Pendekatan ini tidak hanya meningkatkan keamanan dan transparansi dari proses *voting*, tetapi juga membuat pengalaman pengguna yang lebih mudah.

Kata kunci: *Blockchain, Proof of Stake, Voting, Algorand, Digital Identity*

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan yang Maha Esa, atas berkat dan rahmat yang diberikan Nya sehingga penulis dapat menyelesaikan penelitian ini. Tentunya selama penulisan dan penelitian yang dilakukan banyak pihak yang membantu dan memberikan dukungan, oleh karenanya penulis ingin mengucapkan terimakasih kepada:

1. Bapak Brojo Suwignyo & Ibu Eni Indriyaningsih kedua orang tua yang sangat supportive & doa terbaik pada setiap keputusan yang penulis ambil,
2. Kitami Akromunisa & Sabrina Almira Seruni sebagai Istri, Anak dan Keluarga yang selalu mendukung,
3. Bapak Dr. Bambang Sugiantoro selaku dosen pembimbing thesis yang telah dengan ilmu dan kesabaran beliyau serta doa selama penyusunan laporan ini,
4. Bapak Dr. Agung Fatwanto, S.Si., M.Kom. selaku dosen penguji 1,
5. Ibu Dr. Ir. Shofwatul ‘Uyun, S.T., M.Kom. selaku dosen penguji 2,
6. Bapak / Ibu Dosen Magister Informatika yang telah memberikan fasilitas dan pengalaman terbaiknya dalam proses pengajaran,
7. Rekan-rekan seperjuangan di magister informatika 2019.

Penulis menyadari karya tulis ini masih jauh dari kata sempurna, Untuk itu kritik dan saran diharapkan untuk kemajuan penelitian tentang *voting*

system yang lebih baik lagi kedepannya, atau bahkan dapat diterapkan langsung pada proses pemilu. Akhir kata, semoga penelitian ini dapat bermanfaat bagi pembaca



DAFTAR ISI

PERNYATAAN KEASLIAN	II
PERNYATAAN BEBAS PLAGIASI.....	III
PENGESAHAN TUGAS AKHIR	IV
NOTA DINAS PEMBIMBING	V
<i>ABSTRACT</i>.....	VI
ABSTRAK.....	VII
KATA PENGANTAR	VIII
DAFTAR ISI.....	X
DAFTAR TABEL	XIII
DAFTAR GAMBAR	XIV
DAFTAR LAMPIRAN.....	XV
DAFTAR SINGKATAN	XVI
BAB I PENDAHULUAN	17
A. LATAR BELAKANG MASALAH	17
B. RUMUSAN MASALAH.....	19
C. TUJUAN	19
D. MANFAAT PENELITIAN	20
BAB II KAJIAN PUSTAKA DAN LANDASAN TEORI.....	21
A. KAJIAN PUSTAKA	21
B. LANDASAN TEORI.....	25

1. <i>Blockchain</i>	25
2. <i>Digital Identity</i>	33
3. <i>E-Voting</i>	33
BAB III METODE PENELITIAN.....	36
A. IDENTIFIKASI MASALAH DAN MOTIVASI	36
B. MENDIFINISKAN SOLUSI.....	36
C. PERANCANGAN DAN PENGEMBANGAN	36
D. DEMONSTRASI.....	37
E. EVALUASI.....	37
F. KOMUNIKASI.....	37
BAB IV HASIL DAN PEMBAHASAN.....	38
A. PERANCANGAN SISTEM	38
1. <i>Identifikasi Sistem</i>	38
2. <i>Perancangan Sistem</i>	39
3. <i>Diagram Alir</i>	41
4. <i>Vote Smart Contract</i>	42
5. <i>Rancangan Antar Muka</i>	43
B. PENGUJIAN DAN EVALUASI.....	44
1. <i>Membuat Voting</i>	45
2. <i>Membuat Akun Voters</i>	46
3. <i>Pengiriman Asset dan Registrasi Voter ke Smart Contract</i>	47
4. <i>Proses Voting</i>	48
5. <i>Perhitungan Hasil Voting</i>	49
6. <i>Skenario Edge-case</i>	49
PENUTUP	51

A. KESIMPULAN	51
B. SARAN	51
DAFTAR PUSTAKA	52
LAMPIRAN-LAMPIRAN.....	54
DAFTAR RIWAYAT HIDUP.....	69



DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	23
Tabel 4.1 Daftar Partisipan.....	39
Tabel 4.2 <i>Vote Smart Contract</i>	42
Tabel 4.3 Daftar Halaman Web.....	44
Tabel 4.4 Akun Penyelenggara.....	44
Tabel 4.5 Performa <i>Create Projek Voting</i>	45
Tabel 4.6 Performa Pengiriman Asset Hak Pilih.....	47
Tabel 4.7 Skenario <i>Edge-case</i>	49

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi <i>Blockchain</i>	25
Gambar 4.1 Arsitektur Sistem <i>E-Voting</i>	40
Gambar 4.2 Diagram Alir <i>Voter</i>	41
Gambar 4.3 Diagram Alir Penyelenggara	42
Gambar 4.4 <i>Project Voting Application Detail</i>	46
Gambar 4.5 <i>Smart Contract</i> di Jaringan <i>Algorand</i>	46
Gambar 4.6 Akun <i>Algorand Voter</i>	46
Gambar 4.7 <i>Asset</i> Pada Akun <i>Voter</i>	48
Gambar 4.8 <i>Log Voting</i>	48
Gambar 4.9 Rekapitulasi <i>Voting</i>	49

DAFTAR LAMPIRAN

Lampiran 1 <i>Sourcode Smartcontract</i>	54
Lampiran 2 <i>Sourcecode Create Asset Vote</i>	62
Lampiran 3 <i>Sourcecode Transfer Asset</i>	65
Lampiran 4 Halaman <i>Voting Creator</i>	67
Lampiran 5 Halaman <i>Voter</i>	67
Lampiran 6 Halaman Hasil.....	68
Lampiran 7 Halaman <i>OREID Login</i>	68



DAFTAR SINGKATAN

ID	<i>Identity / Identitas</i>
PoS	<i>Proof of Stake</i>
Pemilu	Pemilihan Umum
KPU	Komisi Pemilihan Umum
LUBER JURDIL	Langsung, Bebas, Rahasia, Jujur, dan Adil
PoW	<i>Proof of Work</i>
E-Voting	<i>Electronic Voting</i>
ZKP	<i>Zero-Knowledge Proof</i>
PPoS	<i>Pure Proof of Stake</i>
KPU	Komisi Pemilihan Umum
API	<i>Application Programming Interface</i>
BE	<i>Backend</i>
FE	<i>Frontend</i>
SC	<i>Smart Contract</i>

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB I PENDAHULUAN

A. Latar Belakang Masalah

Pemilu (Pemilihan Umum) adalah “proses untuk memilih pemimpin atau wakil pemimpin melalui suara rakyat yang diberikan secara langsung atau tidak langsung” (Kamus Besar Bahasa Indonesia, 2016). Pemilu digunakan dalam sistem pemerintahan demokrasi untuk memilih pemimpin atau wakil pemimpin melalui suara rakyat yang diberikan secara langsung atau tidak langsung. Pemilu diadakan secara teratur dan dapat dibagi menjadi dua jenis yaitu pemilu legislatif dan pemilu presiden. Pada lingkup yang lebih kecil pemilu digunakan untuk memilih kandidat untuk sebuah posisi pada organisasi tertentu, dikarenakan kita tinggal di negara yang menganut demokrasi maka sangatlah wajar jika sering menemukan kasus-kasus pemilu dari ruang terkecil di sekitar kita.

Teknologi telah membantu dalam berbagai hal, termasuk dalam proses pemilu. Menurut sebuah studi yang dilakukan oleh The International Foundation for Electoral Systems (IFES), "Teknologi dapat membantu dalam meningkatkan transparansi, efisiensi, dan aksesibilitas dalam proses voting" (IFES, 2019). Beberapa contoh teknologi yang digunakan dalam proses voting saat ini adalah sistem voting elektronik, aplikasi voting berbasis *smartphone*, dan teknologi *blockchain*. Keberadaan teknologi ini dapat membantu dalam meningkatkan efisiensi dalam proses *voting*, meningkatkan transparansi dalam hasil *voting*, dan meningkatkan aksesibilitas bagi

pemilih yang berada di berbagai lokasi bahkan daerah yang terpencil.

Meskipun teknologi telah membantu proses *voting*, Namun, masalah yang sering dihadapi dalam sistem voting tradisional adalah masalah keamanan, transparansi, dan keabsahan suara. Keamanan *voting* dapat terganggu melalui pemalsuan suara, manipulasi hasil *voting*, atau penyalahgunaan suara, bahkan rekapitulasi suara yang tidak transparan. Transparansi dalam voting dapat terganggu jika tidak adanya mekanisme untuk memantau proses *voting* dan hasil *voting*. Keabsahan suara dapat terganggu jika tidak adanya mekanisme untuk memverifikasi identitas pemilih.

Untuk mengatasi masalah-masalah tersebut, teknologi *blockchain* dan *digital identity* dianggap sebagai solusi potensial. *Blockchain* dapat menyediakan sistem distribusi terdesentralisasi yang dapat mencegah pemalsuan suara dan manipulasi hasil voting. *Blockchain* juga dapat menyediakan mekanisme untuk memantau proses voting dan hasil voting secara transparan. *Digital identity* dapat digunakan untuk verifikasi identitas pemilih dan mencegah penyalahgunaan suara.

Blockchain dapat menjadi solusi dalam proses *voting*. *Blockchain* adalah teknologi yang memungkinkan untuk menyediakan sistem distribusi terdesentralisasi yang transparan. Hal ini dapat meningkatkan keamanan dan mengurangi risiko pemalsuan suara atau manipulasi hasil voting. "*Blockchain* dapat digunakan untuk menyimpan data suara secara terdesentralisasi dan membuat data tersebut tersedia untuk semua pihak yang berkepentingan" (Ethereum, 2019). Selain itu, *blockchain* juga dapat digunakan untuk

memvalidasi identitas pemilih dan mencegah penyalahgunaan suara. Beberapa contoh implementasi voting berbasis blockchain yang sudah dilakukan adalah pemilu di West Virginia, Rusia dan Denmark.

Blockchain dan *digital identity* dapat digabungkan sebagai solusi dalam proses voting. *Blockchain* dapat digunakan untuk menyimpan data suara secara terdesentralisasi dan transparan serta memvalidasi data suara. Sedangkan *digital identity* digunakan untuk verifikasi identitas pemilih. "Menggabungkan teknologi *blockchain* dan *digital identity* dalam proses *voting* dapat meningkatkan keamanan dan transparansi dalam proses *voting* serta memvalidasi identitas pemilih yang benar" (Blockchain Research Institute, 2018). Selain itu, penggunaan *digital identity* dapat membantu dalam mencegah penyalahgunaan suara dan meningkatkan keabsahan suara.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan pada bagian sebelumnya, terkait permasalahan yang ada pada *E-Voting* berbasis blockchain, maka rumusan masalah dalam penelitian tesis ini adalah sebagai berikut:

1. Apakah *digital identity* dapat diterapkan sebagai tanda pengenal pada voting berbasis *blockchain*?
2. Bagaimana arsitektur voting berbasis *blockchain* dan *digital identity*?

C. Tujuan

Tujuan penelitian ini dapat diuraikan sebagai berikut:

1. Merancang arsitektur *Voting System* berbasis *blockchain* dan melakukan integrasi dengan *digital identity*
2. Melakukan pengujian arsitektur *Voting System*

D. Manfaat Penelitian

Dari uraian tujuan penelitian, harapannya penelitian ini dapat memberikan gambaran penerapan *blockchain* dan *digital identity* pada *voting system*.



PENUTUP

A. Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan terkait perancangan arsitektur sistem *e-voting* dengan mengimplementasikan teknologi *blockchain* dan mengintegrasikan dengan *platform digital identity*, maka dapat ditarik kesimpulan sebagai berikut:

1. Penggunaan digital identity (OREID) yang digunakan sebagai contoh *platform digital identity* dapat diintegrasikan dengan teknologi *blockchain Algorand*.
2. Arsitektur penggunaan *blockchain Algorand* dan *digital identity* dengan OREID yang dirancang pada penelitian ini dapat berjalan dengan normal, dimana proses transaksi data dapat dilakukan secara *end-to-end*.

B. Saran

Untuk penelitian lebih lanjut sangat disarankan jika kedepannya Indonesia memiliki *Platform Digital Identity* yang mandiri, sehingga *usecase* pemungutan suara berbasis *blockchain* dapat dilakukan dan *verifiable* untuk *voter* dengan data diri warga Indonesia, selain itu bagian lain seperti keamanan data dan proses pengiriman asset dapat dioptimalkan kembali, sehingga untuk kasus dengan pemilih yang banyak proses inisialisasinya tidak membutuhkan waktu yang lama.

DAFTAR PUSTAKA

- Kamus Besar Bahasa Indonesia*. (2016).
- IFES*. (2019).
- Ethereum*. (2019).
- Blockchain Research Institute. (2018).
- Don, & Alex, T. (2016). *Blockchain Revolution*.
- Schneier, B. (1996). *Applied Cryptography*.
- Antonopoulos, A. M. (2014). *Mastering Bitcoin*.
- A survey on Proof of Stake (PoS) consensus: Current trends and future directions*. (2020). IEEE.
- The Role of Smart Contracts in Blockchain Technology*. (2018).
Springer.
- Jain, S., & Bhatia, R. (2018). *Digital Identity: Concepts, Methodologies, Tools, and Applications*. IGI Global.
- Kshetri, N. (2019). *Blockchain-based identity management systems: Promise and challenges*. *Journal of Business Research*.
- Micali, S., Nayak, G., & Zeldovich, N. (2019). *The Algorand Protocol*. MIT Laboratory for Computer Science Technical Report.
- Micali, S., Chiesa, A., Tromer, E., & Virza, M. (2019). *Algorand: Scaling Byzantine Agreements for Cryptocurrencies*.
Proceedings of the ACM Symposium on the Theory of Computing.
- Friðrik, Þ. H., & Gunnlaugur, K. H. (2019). *Blockchain Based E-Voting System*.

- Dyah, A. P., Adhitya, B., & Kasyful, A. (2019). *Implementasi Permissioned Blockchain Berbasis Hyperledger Sebagai Penjamin Integritas Data Pada Sistem E-Vote*.
- Francesco, F., Maria, I. L., Filippo, E. P., & Andrea, P. (2018). *Crypto-Voting, a blockchain based e-voting system*.
- Satria Wibowo, D. F. (2019). *Perancangan dan Implementasi Teknologi Blockchain Pada Sistem Pencatatan Hasil Rekapitulasi PEMILU Berdasarkan Formulir C1 Pindaian KPU*.
- Dang, D. K. (2020). *Blockchain-based e-voting: a review of existing solutions*.
- IFES. (2019). *The International Foundation for Electoral Systems*.
- Micali, S., Chen, J., Gorbunov, S., & Vlachos, G. (2018). ALGORAND AGREEMENT Super Fast and Partition Resilient Byzantine Agreement. Retrieved from Algorand: <https://www.algorand.com/smart-contracts-defi>