Analisis Penerapan Blockchain dalam Kegunaannya dalam Sistem Pemilu (*E-Voting*) Indonesia

Muhammad Farhan (18219015)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 18219015@std.stei.itb.ac.id

Pemilihan umum (pemilu) adalah proses penting dalam sistem demokrasi, namun seringkali dihadapkan pada berbagai permasalahan. Salah satu permasalahan utama adalah kurangnya kepercayaan publik terhadap integritas dan transparansi dalam pemilihan. Digitalisasi telah menjadi upaya untuk mengatasi masalah tersebut, namun juga membawa permasalahan baru. Salah satu permasalahan utama dalam digitalisasi pemilihan politik adalah keamanan data dan privasi pemilih. Ancaman terhadap keamanan data dan kemungkinan terjadinya manipulasi dapat merusak integritas pemilihan. Selain itu, partisipasi pemilih juga menjadi masalah, dengan beberapa kelompok mungkin sulit mengakses atau memahami teknologi yang digunakan. Di sinilah teknologi blockchain dapat menjadi solusi potensial. Namun, penggunaan teknologi blockchain dalam pemilihan politik juga memunculkan permasalahan, seperti skalabilitas, keamanan jaringan, dan kerangka hukum yang memadai. Penting bagi pihak yang terlibat dalam pemilihan politik untuk memahami dan mengatasi permasalahan ini untuk memastikan pemilihan yang adil, aman, dan terpercaya.

Keywords: pemilu, politik, permasalahan, kepercayaan publik, integritas, transparansi, digitalisasi, keamanan data, privasi, manipulasi, partisipasi pemilih, teknologi blockchain, skalabilitas, keamanan jaringan, kerangka hukum.

I. Pendahuluan

Proses pemilu di Indonesia menghadapi sejumlah tantangan yang mempengaruhi integritas dan efisiensinya. Salah satu masalah yang sering muncul adalah terkait dengan teknologi dan infrastruktur. Meskipun telah dilakukan upaya untuk memperbaiki infrastruktur teknologi, masih ada daerah di Indonesia yang mengalami keterbatasan akses internet dan jaringan telekomunikasi yang memadai. Hal ini dapat menghambat penggunaan teknologi dalam proses pemilu, seperti dalam pengiriman data dan penghitungan suara. Terlebih lagi, masalah teknologi juga melibatkan keandalan sistem informasi yang digunakan dalam pemilu, termasuk kerentanan terhadap serangan siber dan manipulasi data.

Selain itu, masalah yang sering muncul dalam pemilu di Indonesia adalah terkait dengan keamanan. Terdapat tantangan dalam menjaga keamanan dan mencegah manipulasi suara, baik dari pihak internal maupun eksternal. Ancaman seperti *money politics*, intimidasi, dan kecurangan dalam penghitungan suara masih menjadi perhatian serius dalam proses pemilu. Dalam beberapa kasus, terdapat laporan kecurangan dan ketidakadilan dalam proses pemilu, yang dapat merusak kepercayaan publik terhadap hasil pemilu dan mengganggu stabilitas politik.

Tantangan lain dalam pemilu di Indonesia adalah terkait dengan transparansi dan pengawasan. Proses pemilu yang transparan dan adil adalah prasyarat penting dalam membangun kepercayaan publik. Namun, terdapat kekhawatiran bahwa pengawasan pemilu tidak cukup efektif dan independen. Dalam beberapa kasus, pengawas pemilu menghadapi kendala dalam mengakses data dan informasi yang diperlukan untuk melakukan pengawasan yang lebih baik. Ketidaktransparan ini dapat menciptakan keraguan dan ketidakpuasan terhadap integritas pemilu.

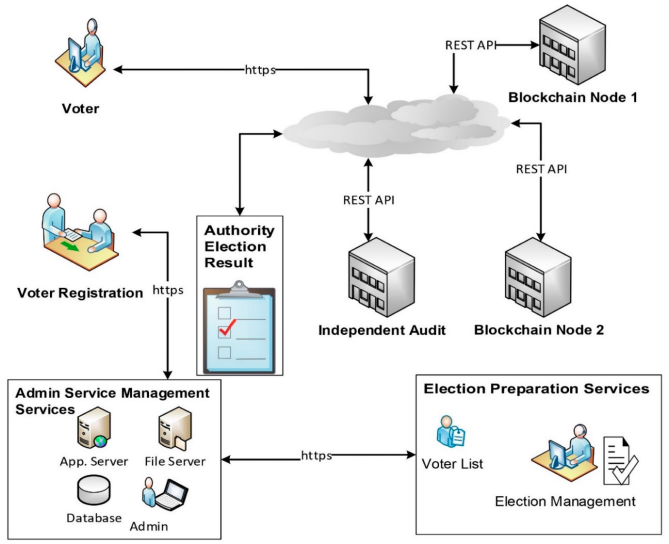
Dengan memahami permasalahan dalam pemilu di Indonesia, penting untuk mencari solusi yang tepat untuk meningkatkan integritas, keamanan, dan transparansi proses pemilu. Implementasi teknologi yang tepat, peningkatan infrastruktur, peningkatan pengawasan independen, serta edukasi dan partisipasi aktif masyarakat dapat membantu mengatasi permasalahan dalam pemilu dan memperkuat demokrasi di Indonesia.

II. Landasan Teori

A. *E-Voting*

Pemungutan suara elektronik (disebut juga *e-voting*) berasal dari kata electronic voting yang mengacu pada penggunaan teknologi informasi pada pelaksanaan pemungutan suara. Pilihan teknologi yang digunakan dalam implementasi dari *e-voting* sangat bervariasi, seperti penggunaan kartu pintar untuk otentikasi pemilih yang bisa digabung dalam e-KTP, penggunaan internet sebagai sistem pemungutan suara atau pengiriman data, penggunaan layar sentuh sebagai pengganti kartu suara, dan masih banyak variasi teknologi yang bisa digunakan. Dalam perkembangan pemikiran penggunaan perangkat telepon seluler untuk memberikan suara bisa menjadi pilihan karena sudah menggabungkan (konvergensi) perangkat komputer dan jaringan internet dalam satu perangkat tunggal.

Kondisi penerapan dan teknologi *e-voting* terus berubah seiring perkembangan teknologi informasi yang sangat cepat. Kendala-kendala *e-voting* yang pernah terjadi di berbagai negara yang pernah dan sedang menerapkannya menjadi penyempurnaan *e-voting* selanjutnya. Salah satu segi positif dari penerapan *e-voting* saat ini adalah makin murahnya perangkat keras yang digunakan dan makin terbukanya perangkat lunak yang digunakan sehingga biaya pelaksanaan *e-voting* makin murah dari waktu ke waktu dan untuk perangkat lunak makin terbuka untuk diaudit secara bersama. Salah satu konsep penerapan perangkat lunak adalah melalui Indonesia Goes Open Source (IGOS) dengan diperkenalkannya aplikasi e-demokrasi pada tahun 2007.[1]



Gambar II.1. Sistem *e-voting*

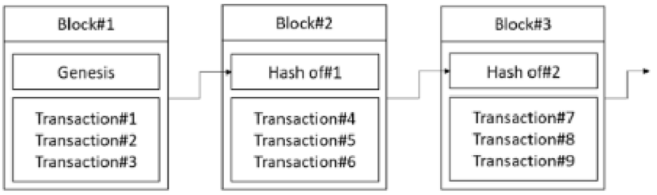
Sumber: *e-voting*

B. Blockchain

Blockchain adalah teknologi yang mengubah cara transaksi dan pertukaran data dilakukan secara digital. Konsep dasar dari blockchain adalah bahwa informasi atau transaksi yang terjadi dicatat dalam blok-blok yang saling terhubung dan terenkripsi. Setiap blok memiliki referensi terhadap blok sebelumnya, membentuk rantai yang tak terputus. Salah satu keunggulan utama blockchain adalah keamanannya yang tinggi. Setiap transaksi yang dicatat dalam blockchain tidak dapat diubah atau dihapus, sehingga mencegah manipulasi data. Ini membuat blockchain menjadi alat yang efektif dalam mengamankan transaksi keuangan, data pribadi, dan informasi sensitif lainnya [2].

Selain itu, blockchain juga menawarkan transparansi yang tinggi. Karena setiap transaksi dicatat dalam blok yang dapat diakses oleh semua pihak yang terlibat, maka informasi mengenai transaksi tersebut menjadi terbuka dan dapat dipertanggungjawabkan. Hal ini dapat membantu mencegah penipuan atau kecurangan, karena setiap perubahan atau manipulasi data akan terlihat secara jelas dalam blockchain. Keaslian dan integritas data juga dapat diverifikasi dengan mudah oleh semua pihak yang memiliki akses ke blockchain [3].

Selain aplikasi dalam transaksi keuangan, blockchain juga telah digunakan dalam berbagai bidang lainnya seperti logistik, rantai pasok, pemilu, dan sertifikasi dokumen. Teknologi ini memberikan potensi untuk meningkatkan efisiensi, mengurangi biaya, dan mengurangi ketergantungan pada pihak ketiga. Namun, meskipun memiliki potensi yang besar, blockchain juga memiliki beberapa tantangan yang perlu diatasi, seperti skalabilitas, regulasi, dan masalah keberlanjutan energi [4].



Gambar II.2. Ilustrasi blockchain

Sumber: blockchain

C. RSA

RSA (Rivest-Shamir-Adleman) adalah salah satu algoritma kriptografi kunci publik yang paling terkenal. Algoritma RSA digunakan untuk enkripsi dan dekripsi data serta untuk membuat dan memverifikasi tanda tangan digital. Algoritma ini didasarkan pada kesulitan memfaktorkan bilangan bulat besar menjadi faktor-faktor primanya [5].

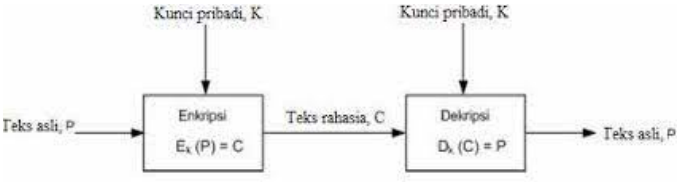
Proses RSA dimulai dengan pembuatan pasangan kunci, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi pesan, sementara kunci pribadi digunakan untuk mendekripsinya. Kunci publik dapat diberikan kepada siapa saja, sedangkan kunci pribadi harus dijaga dengan baik oleh pemiliknya.Berikut adalah langkah-langkah proses RSA secara rinci:

1. Pembuatan Kunci:
   A. Pilih dua bilangan prima acak yang besar, misalnya p dan q.
   B. Hitung nilai n = p * q, yang merupakan modulus.
   C. Hitung nilai phi(n) = (p - 1) * (q - 1), yang merupakan fungsi Euler dari n.
   D. Pilih bilangan bulat acak e, di mana 1 < e < phi(n) dan e saling prima dengan phi(n). e akan menjadi kunci publik.
   E. Hitung nilai d, yang merupakan invers perkalian modulo e terhadap phi(n) (d * e mod phi(n) = 1). d akan menjadi kunci pribadi.

2. Enkripsi Pesan:
   A. Ambil pesan yang akan dienkripsi dalam bentuk bilangan bulat, misalnya m.

B. Hitung ciphertext (c) dengan rumus c = m^e mod n. Ciphertext ini dapat dikirimkan ke penerima pesan.

3. Dekripsi Pesan:
   A. Terima ciphertext (c).
   B. Hitung plaintext (m) dengan rumus m = c^d mod n. Plaintext ini adalah pesan asli yang dikirimkan.



Gambar II.3. Ilustrasi enkripsi dan dekripsi menggunakan RSA

D. Hashing

Hashing dalam kriptografi merujuk pada proses mengubah data yang tidak terduga menjadi nilai tetap yang disebut hash atau nilai hash [6]. Fungsi hash kriptografis digunakan untuk menghasilkan nilai hash yang unik untuk setiap input yang berbeda. Tujuan utama hashing adalah memastikan integritas data dan menyembunyikan informasi asli yang di-hash. Berikut adalah langkah-langkah proses hashing kriptografi secara rinci:

1. Ambil data yang akan di-hash, misalnya sebuah pesan atau file.

2. Gunakan fungsi hash kriptografis, seperti SHA-256 (Secure Hash Algorithm 256-bit), MD5 (Message Digest Algorithm 5), atau SHA-3 (Secure Hash Algorithm 3), untuk mengolah data.

3. Fungsi hash akan menghasilkan nilai hash dengan panjang tetap, terlepas dari panjang data aslinya. Misalnya, SHA-256 menghasilkan nilai hash 256-bit.

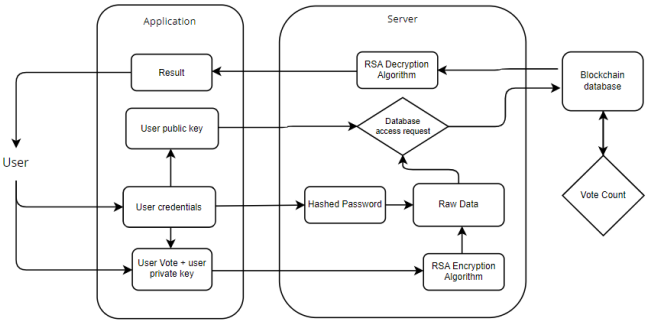
4. Nilai hash yang dihasilkan akan memiliki beberapa karakteristik penting:

   - Unik: Setiap input yang berbeda akan menghasilkan nilai hash yang unik. Namun, kemungkinan terjadinya tumpang tindih nilai hash (collision) sangat kecil.
   - Tidak dapat dikembalikan: Nilai hash tidak dapat dikembalikan menjadi data aslinya.
   - Deterministik: Data yang sama akan menghasilkan nilai hash yang sama.

5. Nilai hash dapat digunakan untuk memverifikasi integritas data. Jika terdapat perubahan pada data asli, nilai hash yang dihasilkan akan berbeda.

Hashing kriptografis penting dalam banyak aplikasi keamanan, seperti verifikasi kata sandi, penandatanganan digital, dan deteksi perubahan data. Namun, penting untuk menggunakan fungsi hash yang aman dan teruji, mengingat kemajuan teknologi yang dapat mengurangi keamanan hashing.

III. SKEMA RANCANGAN



Gambar III.1. Algoritma sistem *e-voting*

Dalam sistem yang dikembangkan, data pemilihan yang dienkripsi menggunakan RSA dan lalu di hashing akan disimpan pada database, data *credential* pengguna seperti password juga akan di hash dan disimpan pada database, data credential lainnya seperti nama, *email*, NIK, dan tanggal lahir juga akan disimpan pada *database* blockchain. Perlu ditinjau ulang bahwa unsur penyimpanan data pada blockchain dalam sistem ini menggunakan perantara *third party database* yang berbasis *blockchain* sehingga unsur kriptografi *blockchain* tidak akan terlalu dibahas. Namun, permasalahan pemilihan *database* apa dan algoritma kriptografi paling efisien untuk digunakan agar data transaksi dapat dimanfaatkan sebaik mungkin akan tetap dibahas.

Untuk mengakses sistem, pengguna diperlukan untuk memasukkan data diri (*credential*) berupa nama, *email*, *password*, NIK, dan tanggal lahir terlebih dahulu. Setelah itu, *public* dan *private key* akan terbuat dan akan dilakukan *tracking* pada setiap pergantian sesi sehingga *user* dapat memiliki public key yang dapat mengakses proses dekripsi pada *server*. *Private key* akan digunakan untuk mengenkripsi hasil voting user dengan metode kriptografi RSA + *hex* sebagai *digital sign*. Hasil voting tersebut akan disimpan pada *database blockchain* beserta *credential* dari user (*password* yang telah di-*hashed*, nama, NIK, *email*, dan tanggal lahir, serta alamat) agar dapat dilakukan *mapping* pada pengambilan data dengan memanfaatkan akun pengguna (*email* dan *password*).

Suara untuk calon yang dipilih oleh user akan langsung dimasukkan ke dalam blockchain database sebagai *polling* calon tersebut dan tidak dapat diganti karena *voting* dari user akan unik sesuai dengan *credential user* (Nama, NIK, tanggal lahir, alamat) itu sendiri seperti halnya *digital sign*. Ini dapat dibuktikan bila *credential* dari *user* akan dilakukan mapping pada *database*, bila hasil *mapping*-nya ada dan hanya 1, maka

sistem akan melakukan pengecekan validnya pemungutan suara dari *polling* calon dengan melakukan *decryption* RSA dari *ciphertext/digital sign* (kombinasi *credential user* dan calon yang dipilih). Bila hasil *hashing* dari proses *decryption* RSA menggunakan *public key* dari *user* sama dengan hasil hashing dari kombinasi *credential user* dan calon, maka suara dari hasil pemungutan suara tersebut adalah calon yang bersangkutan. Namun pada aspek *blockchain*-nya sendiri *user* juga memiliki tingkat keamanan dari datanya sendiri sehingga dapat dipastikan bahwa data dari user tersebut tidak dapat diubah sehingga akan menambah aspek keamanan dalam sistem.

NIK	Nama	Tanggal Lahir	Alamat	Email	Password	Vote
Integer	String	Date	String	String	Text	Text

Gambar III.2. *Logical user database table*

Diatas merupakan *logical database* dari tabel *user*, untuk *database table* caleg dan cawapres, penulis masih belum mendapatkan informasi yang akurat mengenai data apa saja yang perlu diadakan, namun dapat diperkirakan adalah sebagai berikut:

NIK	Nama	Tanggal Lahir	Alamat	Jabatan	Partai	Nomor Urut
Integer	String	Date	String	String	String	Integer

Gambar III.3. *Logical* caleg, capres, & cawapres *database table*

Hasil voting dari *user* akan diakumulasikan berdasarkan polling pada tiap-tiap kandidat yang disimpan pada *database* sesuai dengan nomor urut votingan pengguna. Hasil akumulasi ini akan diumumkan pada saat prosesi pemilu selesai termasuk juga semua pengecekan keautentikan dari suara pemilih dalam polling kandidat.

IV. Analisis dan Pembahasan

Untuk melakukan pembahasan, mari kita gunakan sebuah *test case* untuk dijalankan pada algoritma sistem *e-voting*. Untuk pembangkitan kunci akan diberikan spesifikasi sederhana terlebih dahulu yaitu:

- p = 32817341
- q = 98651089
- phi = 3237466296265920

Dari pembangkitan kunci *public* dan *private* RSA didapat:

- public key = (252718507312223, 3237466427734349)
- private key = (1296970992100127, 3237466427734349)

Pesan (plaintext) yang akan dienkripsi menggunakan algoritma RSA adalah nama + NIK + tanggal lahir + calon yang dipilih. Untuk memasukkan data nama, NIK, dan tanggal lahir, terlebih dahulu pengguna harus membuat akun berupa *email* dan *password* yang disimpan sistem. Akun ini akan dilakukan mapping dengan data yang disimpan pada database. Data diri (*credential*) yang ada sebagai contoh adalah sebagai berikut:

- Nama: Muhammad Farhan
- NIK: 1234567890123456
- Tanggal Lahir: 1 September 2001
- Alamat: Sekeloa, Bandung
- No urut calon presiden dan wapres: 1
- No urut calon DPR: 3
- No urut calon DPD: 10
- No urut calon DPRD Provinsi: 7
- No urut calon DPRD Kabupaten: 3

Hasil dari enkripsi pesan berupa ciphertext RSA yang kemudian dilakukan *hex* untuk mengenkripsi data hasil pemilihan menjadi *digital sign* untuk masing-masing calon yang dipilih oleh pengguna. Hasil pemilihan pengguna berupa *digital sign* berdasarkan contoh pemilihan diatas adalah sebagai berikut:

- Presiden dan wapres:
  067e6f1ccbe2f70aa93001021104077bb23b02f121001be
  b6c81602b08697a3513bb0c06ea209cd49c4a00000004
- DPR:
  01cfa596bcfac30bafc8e93f093b06e260792b28630aa0ce
  756d97a80b8d61d8ab4d9f1bdb4046f0db4100000004
- DPD:
  00ab4872138ff7079db19161ac07045742905d4ecd015b3
  488cf00ed02edc54719f8bb01791bef55a1f100000004
- DPRD Provinsi:
  0a0a7aea9d7e76056b6347e89ac40dd3348c33a4e300d57
  17b7640fc07cdef1f11d4d4000d018883baa900000004
- DPRD Kabupaten:
  06dfcd4dda6abf058ae480b14f0b0749bb326e146600a10
  0acbff1ea073a24cb3fc44b011f39072b566b00000004

Hasil dari *digital sign* ini akan dimasukkan pada polling masing-masing calon yang dipilih dalam *blockchain database*. Untuk mengecek keautentikan dari hasil pemungutan suara maka dapat dilakukan *decryption* RSA + hashing yang sudah disinggung pada bagian sebelumnya. Dengan menggunakan kunci publik yang sudah di bangkitkan didapatkan bahwa hasil dari proses dekripsi adalah sebagai berikut:

- Presiden dan wapres:
  \xd8\x9d\xeb\xfcC2{\x0f\x04GM\xd2"\xfc\x91lP\x89\xa
  7\xa0\xe568/\x9d0KYD\x1bz\xc3
- DPR:
  \x10B\xda\x90\\S#\xa1\x02\xe3[\xdd\xec4A\xc7\xbe;B\x
  0e\x13\x9b\x16\x0b\xea\x07u\x9c\xe0\x8e\x9d1
- DPD:
  \x97\x00\x85\xf8A\x14U5A\x8fu6\xb6\xce\xdb\x82\xc0
  MEB\xa8:V{\x85W\xb7\xea\x9e\xa6\x8f\xf3
- DPRD Provinsi:
  v\xcf\x01\xad\x13#\x8bF\xb4\xb6\x90\xe6OWf\xf0\x13

A\xde\xafDd+\x974\xaa\xe84.&<\x00

- DPRD Kabupaten: \x88\x1a\xad\xe5M\xeb\xb4\x7f(\x17+\xb9\x89\x8e\x10\x18\xf7bNc\x1b\x96\xbd(\xcc\xb8;)\x15\xd3\xb2x

Hasil dekripsi adalah berupa bytes yang nantinya akan dikonversi menjadi nilai *hash*. Nilai hash dari proses dekripsi akan dibandingkan dengan nilai hash dari data pengguna yang bersangkutan (data diri/*credentials* dan votingnya). Apabila sama maka hasil voting autentik dan bila tidak maka terjadi kesalahan atau pengubahan data dan dapat dilakukan traceback pada pengubahan data tersebut untuk ditindaklanjuti ke ranah hukum.

Peninjauan lainnya berupa aspek penyimpanan data pada *database blockchain* juga perlu dibahas. Untuk mengakses database seorang user harus memiliki 2 aspek penting yaitu *email*, *password*. Setelah login, public dan private key user akan dibangkitkan dan akan langsung dimasukkan pada database blockchain. Setelah itu user akan diarahkan pada halaman pemilihan oleh aplikasi dan akan dimintai data pemilihan seperti yang sudah disebutkan sebelumnya, data tersebut akan disimpan pada *database blockchain*. Pemilihan *database blockchain* yang tepat serta algoritma penyimpanan data yang efisien perlu dipertimbangkan karena akan mempengaruhi lama respon dari *database* karena semakin panjang data yang perlu diinput pada *database* akan semakin lama juga proses komputasinya. Tidak ada pengukuran pasti mengenai lama waktu proses *read and write* pada *database* berbasis *blockchain* namun terdapat sebuah gambaran general pada beberapa contoh database. Ada beberapa opsi dari database *blockchain* yang dapat diintegrasikan pada sistem, diantaranya adalah:

Database	Waktu Rata-Rata Read	Waktu Rata-Rata Write
Ethereum	Beberapa detik	Sekitar 15 detik hingga beberapa menit
Hyperledger Fabric	Beberapa detik	Beberapa detik
Corda	Hitungan detik	Hitungan detik
BigchainDB	Hitungan milidetik hingga detik	Beberapa detik
Quorum	Beberapa detik	Beberapa detik

Tabel IV.1. Rata-rata waktu *read and write* beberapa *blockchain database*

Database blockchain yang akan digunakan juga memerlukan tingkat keamanan yang tinggi karena data bersifat rahasia sehingga tidak hanya memerlukan kemampuan komputasi yang cepat tetapi juga memerlukan kemampuan sekuritas yang tinggi. Beberapa database yang dapat ditinjau dari sisi keamanan serta kompleksitasnya dalam pengintegrasian dengan sistem adalah sebagai berikut:

Database	Tingkat Keamanan	Tingkat Kompleksitas
Ethereum	Tinggi	Tinggi
Hyperledger Fabric	Tinggi	Sedang
Corda	Tinggi	Sedang
BigchainDB	Sedang	Rendah
Quorum	Tinggi	Tinggi

Tabel IV.2. Tingkat keamanan dan kompleksitas *database blockchain*

Tingkat Keamanan:

- Tinggi: Database memiliki tingkat keamanan yang tinggi dengan mekanisme kriptografi yang kuat dan algoritma konsensus yang terdistribusi.
- Sedang: Database memiliki tingkat keamanan yang cukup baik, tetapi mungkin memiliki beberapa fitur yang mengurangi tingkat keamanan dibandingkan dengan tingkat keamanan yang tinggi.
- Rendah: Database memiliki tingkat keamanan yang lebih rendah, mungkin dengan fitur yang lebih sederhana dan kurangnya lapisan keamanan yang kuat.

Tingkat Kompleksitas:

- Tinggi: Database memiliki tingkat kompleksitas yang tinggi dalam hal arsitektur, algoritma konsensus, dan konfigurasi yang rumit.
- Sedang: Database memiliki tingkat kompleksitas yang moderat, dengan arsitektur dan algoritma yang relatif mudah dipahami dan dikonfigurasi.
- Rendah: Database memiliki tingkat kompleksitas yang rendah, dengan desain yang lebih sederhana dan alat yang lebih mudah digunakan.

Perlu diingat bahwa tingkat keamanan dan kompleksitas dapat bervariasi tergantung pada implementasi, konfigurasi, dan penggunaan yang tepat dari masing-masing *database*

blockchain sehingga perlu dipertimbangkan ulang dan matang-matang mengenai pemilihan *database blockchain* yang akan diintegrasikan dengan sistem.

V. Kesimpulan

E-Voting merupakan salah satu pengembangan teknologi yang diperlukan untuk pemilihan suara yang bersifat langsung, umum, bebas, jujur, adil. Selain itu dengan adanya pengintegrasian dengan teknologi *blockchain*, terdapat tambahan sekuritas, transparansi, dan juga integritas dari data yang disimpan sehingga tidak akan ada pengubahan data yang dilakukan pihak ke 3 sehingga tidak perlu meragukan integritas dari data yang ada. Dengan adanya sistem yang disarankan pada makalah ini, diharapkan terdapat tambahan opsi/pertimbangan sistem *e-voting* untuk pemilu kedepannya. Namun perlu dipertimbangkan dengan matang untuk sistem yang akan diterapkan karena akan banyak data sensitif yang perlu digunakan dalam sistem dan pengelolaan data tersebut perlu dilakukan dengan efisien serta seaman mungkin pada setiap proses transaksi data tersebut dalam sistem.

References

[1] IGOS Center Tawarkan Aplikasi Pemilu dan Pilkada Murah Meriah

[2] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System

[3] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.

[4] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio.

[5] Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

[6] National Institute of Standards and Technology (NIST). (2015). Secure Hash Standard (SHS).

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 Mei 2023

Muhammad Farhan 18219015