

SISTEM PENGUNDIAN PELAJAR MENGGUNAKAN BLOCKCHAIN

Siti Nursyazana Abdul Wahab

Khairul Azmi Abu Bakar

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Pengundian elektronik atau e-voting telah digunakan dalam pelbagai bentuk sejak tahun 1970-an dengan asasnya yang memberi banyak faedah berbanding sistem berasaskan kertas seperti peningkatan kecekapan dan mengurangkan kesilapan. Walau bagaimanapun, ia tetap menjadi cabaran untuk mencapai penggunaan sistem secara meluas terutama berkaitan dengan peningkatan ketahanan sistem terhadap kemungkinan risiko kesalahan. *Blockchain* adalah teknologi masa kini yang menjanjikan peningkatan ketahanan keseluruhan sistem e-voting. Fakta telah menunjukkan teknologi *Blockchain* mempunyai kebolehgunaan dan ketahanan yang tinggi terhadap penggoda, jadi dengan menggunakan teknologi ini, rekod atau transaksi tidak dapat ditukar dan selamat. Selain itu, dengan menggunakan rangkaian *Blockchain* dapat mengurangkan beban rangkaian sistem. Kajian ini menunjukkan usaha untuk memanfaatkan faedah dari *Blockchain* seperti asas kriptografi dan ketelusan untuk mencapai skema yang berkesan untuk e-voting. Skema yang dicadangkan sesuai dengan syarat asas untuk e-voting dan mencapai pengesahan dari hujung ke hujung (*end-to-end*). Kajian ini membentangkan penilaian mendalam mengenai skema tersebut yang berjaya menunjukkan keberkesanannya dalam mencapai skema e-voting yang dapat disahkan secara menyeluruh.

1 PENGENALAN

Pilihan raya adalah asas kepada sistem demokrasi yang membolehkan orang awam menyatakan pandangan mereka dalam bentuk undi. Oleh kerana undi merupakan sesuatu yang penting dalam masyarakat, proses pengundian perlulah tulus dan boleh dipercayai dan dalam masa yang sama memastikan kredibiliti calon. Sistem pengundian yang digunakan di universiti memerlukan pengundi pergi ke tempat pengundian secara fizikal dan memberikan undi mereka dengan menggunakan kertas undi yang mengandungi nama pengundi dan maklumat lain. Sistem secara manual ini memerlukan calon untuk mendaftarkan diri dengan jawatankuasa Pemilihan Majlis Universiti.

Usaha yang berterusan telah diambil untuk memastikan kecekapan dan ketahanan sistem pengundian. Pengundian secara elektronik atau e-voting memainkan peranan yang penting dalam isu ini. Sistem pengundian secara elektronik telah diperkenalkan untuk menggantikan dan

meningkatkan tahap kecekapan dan ketuluan dalam proses pengundian. Melalui pendekatan ini, proses pengundian akan lebih selamat dan lebih cekap.

2 PENYATAAN MASALAH

Proses pengundian secara manual sangat membebankan pengundi di mana mereka perlu beratur panjang sebelum memberikan undi mereka dengan menggunakan kertas undi. Hal ini menyebabkan 10-15 % pengundi yang layak mengundi tidak mengundi. Sistem pengundian secara manual juga tidak begitu tulus kerana pengiraan undi dilakukan secara manual oleh manusia dimana peluang untuk melakukan kesalahan sangat tinggi dan jumlah undi kemungkinan dislah kira.

Oleh kerana itu, projek ini bertujuan untuk mengatasi masalah tersebut dan juga mengatasi masalah keselamatan sistem pengundian secara elektronik.

3 OBJEKTIF PROJEK

Objektif utama projek :

1. Mengkaji protokol pengundian elektronik dari perspektif keselamatan.
2. Untuk mekanisme privasi, pengesahan, integriti, pengulangan untuk sistem e-voting
3. Rangka protokol pengundian elektronik umum yang menyediakan privasi, ketelusan, integriti, dengan ketepatan, pengesahan dan pengundian elektronik yang dipercayai dan sebagai tambahan kepada keperluan untuk pengundian elektronik.
- 4.

4 METHOD KAJIAN

Projek ini menggunakan *Rational Unified Process* (RUP) sebagai model proses asas untuk mengembangkan sistem berasaskan web e-voting ini. RUP adalah kerangka proses pengembangan perisian berulang yang dibuat oleh *Rasional Software Corporation*, suatu divisyen dari IBM sejak 2003. RUP bukanlah suatu proses tunggal dengan aturan yang konkrit, melainkan suatu kerangka proses yang dapat diadaptasi dan dimaksudkan untuk disesuaikan oleh pertubuhan pemaju dan pasukan projek perisian yang kan memilih elemen proses sesuai dengan keperluan mereka.

4.1 Fasa Perancangan

Fasa ini melibatkan proses pengenalpastian masalah, objektif, persoalan kajian dan menentukan skop. Langkah seterusnya adalah sorotan susastera yang melibatkan pengumpulan, pencarian dan pembacaan jurnal dan kajian yang lepas bagi mencetus idea dan inspirasi. Contoh topik yang berkaitan dikaji terutama berkaitan dengan konsep reka bentuk an visualisasi sistem pengundian elektronik yang sedia ada. Penggunaan Internet untuk mencapai maklumat berkaitan dan pencarian

bahan di perpustakaan dilakukan. Maklumat dikumpul, distrukturkan dan disintesis dan dipersembah secara kritis dan kreatif dalam fasa analisis.

4.2 Fasa Analisis

Fasa ini melibatkan analisis dan tafsiran maklumat yang dikumpul dalam fasa perancangan. Analisis tentang kesesuaian topik dan menilai kepentingan untuk menjalankan kajian ini dilakukan. Selain daripada itu, analisis tentang perkakasan dan perisian juga dijalankan untuk memastikan perkakasan dan perisian yang sedia ada adalah sesuai untuk membangun projek ini.

4.3 Fasa Reka Bentuk

Fasa ini merupakan fasa yang penting dalam keseluruhan projek. Fasa ini melibatkan dua proses penting, iaitu mereka bentuk dan membuat visualisasi objek.



Rajah 1 Struktur Pecahan Kerja

4.4 Fasa Pengujian

Fasa ini bertujuan menguji model dan pergerakan animasi yang dihasilkan dalam fasa reka bentuk. Sekiranya gagal mencapai objektif projek, penyelarasan perlu dijalankan atau mengimbas Kembali fasa analisis bagi membuat penambahbaikan kajian yang mendalam.

Perkakasan dan perisian yang diguna untuk membangun projek harus dipilih dengan teliti. Perkakasan dan perisian yang baik berfungsi dengan lancar serta menyokong pembangunan projek pengundian menggunakan *Blockchain*. Pemilihan perkakasan dan perisian yang tidak tepat boleh menjejaskan hasil projek.

5 HASIL KAJIAN

Bahagian ini membincang hasil daripada proses pembangunan sistem pengundian menggunakan *Blockchain*. Penerangan yang mendalam tentang reka bentuk dan hasil daripada sistem pengundian menggunakan *Blockchain*.

Kontrak pintar Etehreum, teknologi yang diperlukan yang akan menjadi asas sistem pengundian. Kontrak pintar bertindak sebagai nod Etehreum yang wujud sebagai potongan kod, dikodkan ke dalam blockchain dan membolehkan pengguna lain di rangkaian Etehreum iaitu pelajar untuk berinteraksi dengan kod tersebut. Komunikasi ini berlaku pada pelayan *Remote Procedure Call* (RPC) yang dikendalikan oleh web3.js, klien RPC JSON Ethereum yang dibina dengan JavaScript. Oleh itu, jika pengguna ingin memberikan suara undi, komputer/rangkaian mereka akan memanggil fungsi yang ditulis ke dalam kontrak pintar dengan bercakap dengan node kontrak untuk melakukan tindakan yang diperlukan

Dalam proses pendaftaran, pemilih menyampaikan pesanan rahsia (*hash*). Sebagai tindak balas kepada mesej rahsia, laman web sisi pelanggan menghasilkan nombor rujukan unik yang unik untuk pemilih yang harus diperhatikan untuk rujukan masa depan semasa pengundian. Mesej rahsia dalaman dan nombor rujukan dihasilkan dan disimpan dalam pangkalan data. Penting agar pengundi tidak berkongsi mesej rahsia dan nombor rujukan. Jika tidak, suruhanjaya pilihan raya dapat mengetahui siapa dan berpotensi memanipulasi keseluruhan proses pengundian pada peringkat pengundian kemudian. Pengundi adalah dari kalangan pelajar yang berstatus aktif. Suruhanjaya Pilihan Raya akan menghasilkan alamat awam dalam rangkaian pelbagai rangkaian dan menyimpannya terhadap calon. Kemudian, semasa mengundi, alamat awam ini akan dapat dilihat oleh para pengundi untuk memilih calon.

Di seluruh dunia, pengundian berlaku dalam jangka waktu yang ditentukan, begitu juga di universiti. Prosedur yang sama diikuti di peringkat universiti. Walau bagaimanapun, tempoh pengundian dapat diperpanjang. Pemilih yang dikenal pasti sebagai pengguna yang sah oleh sistem akan dibawa ke halaman pengundian. Di sana, senarai calon akan ditunjukkan berdasarkan organisasi. Semasa proses ini, pihak ketiga yang dipercayai menghasilkan kunci awam untuk pemilih menggunakan rangkaian pelbagai rantai dan menyimpan maklumat ini terhadap *hash* mesej rahsia dan nombor rujukan pemilih.

Pengujian sistem perlu dijalankan selepas pembangunan sistem untuk memastikan sistem berfungsi dengan baik dan menepati spesifikasi yang ditetapkan.

6 KESIMPULAN

Sistem Pengundian Pelajar Menggunakan *Blockchain* ini telah berjaya disempurnakan di samping memenuhi tujuan projek seperti yang telah dinyatakan pada peringkat awal pembangunan sistem ini. Secara keseluruhannya, sistem ini telah memenuhi keperluan dan kehendak pengguna. Sistem ini berupaya menjalankan fungsi pengundian yang sepatutnya seperti membolehkan pendaftaran calon dan pengundi, mengira undi secara automatik dan sebagainya. Kesimpulannya, cadangan telah diberikan bagi meningkatkan prestasi dan kemantapan sistem pada masa hadapan dengan memberikan perkhidmatan yang terbaik.

Copyright@FTSM
UKM