DISPROVE : SISTEM VERIFIKASI PEMILIHAN DAN PEMILIH DENGAN MENGGUNAKAN TEKNOLOGI *BLOCKCHAIN*

OLEH :

MUHAMMAD FAUZAN LUBIS

NIM. 191524026

D4 - TEKNIK INFORMATIKA

POLITEKNIK NEGERI BANDUNG

BANDUNG

2021

LEMBAR PENGESAHAN

1. Judul Karya Tulis : *DisProve* : Sistem Verifikasi Pemilihan dan Pemilih dengan Menggunakan Teknologi *Blockchain*
2. Penulis
    a. Nama Lengkap : Muhammad Fauzan Lubis
    b. NIM : 191524026
    c. Program Studi : D4 Teknik Informatika
    d. Jurusan : Teknik Komputer dan Informatika
    e. Perguruan Tinggi : Politeknik Negeri Bandung

Bandung Barat, 5 Juni 2020

Pembantu Direktur
Bidang Kemahasiswaan,

Harita Nurwahyu Chamidy, LRSC., MT
NIP. 196601111994031002

Dosen Pembimbing,

Urip T. Setijohatmo
NIP. 196009281994031001

DAFTAR ISI

DAFTAR GAMBAR

PENDAHULUAN

1. Latar Belakang

Basis dari segala macam demokrasi di tingkatan apapun adalah dilakukannya pemilihan untuk pemimpin, keputusan, dan lainnya. Dan hal yang paling penting dari pemilihan itu sendiri adalah kepercayaan dari orang-orang yang melakukan pemilihannya itu sendiri. Kepercayaan bahwa dalam pemilihan itu tidak ada pihak manapun yang mengganggu jalanya pemilihan untuk kepentingan pihak itu sendiri. Hal ini dapat terjadi dengan banyak bentuk, dari mulai politik uang, hingga konflik kepentingan dengan panitia pemilihan. Isu-isu seperti inilah, yang seringkali mengurangi kepercayaan dari pemilih kepada sistem pemilihan yang mereka ikuti.

Permasalahan kepercayaan ini bisa berakibat lebih lanjut dalam dilakukannya keputusan yang dipilih, atau ketidakpercayaan kepada pemimpin yang terpilih dari pemilihan itu. Sayangnya lagi sistem yang ada sekarang didasari oleh kepercayaan dari pemilih kepada sistem pemilihan. Sistem ini, walaupun memang sudah cukup transparan dengan memberikan data yang diterimanya. Jika sudah sulit untuk pemilih untuk mempercayai suatu sistem maka apapun yang dikatakan oleh sistem itu bisa saja dianggap sebagai suatu kebohongan. Namun, bagaimana jika dibuat sistem yang dapat melakukan verifikasi dari sistem yang sudah ada, namun sistem kali ini tidak memerlukan kepercayaan apapun dari pemilih.

Disitulah ide utama dari *DisProve*, sistem pencatatan dari pilihan seorang pemilih tanpa adanya suatu otoritas yang harus dipercayai. Jadi dengan adanya sistem ini yang akan berdampingan dengan sistem yang sudah ada, seperti pemilihan berbasis kertas, hasil dari pemilihan itu dapat dibandingkan dengan apa yang ada di sistem *DisProve*, dan melihat apakah hasilnya berbeda. Dengan begitu kedua belah pihak, yang merupakan bagian dari sistemnya itu sendiri, dapat lebih mempercayai hasilnya. Dan jika memang ada kecurangan atau adanya kemungkinan

kesalahan dalam perhitungan, pihak yang merasa dirugikan dapat memperlihatkan kesalahan dari pihak panitia pemilihan itu hingga ke level suatu suara dari individu tertentu.

Dengan adanya sistem ini, bukan hanya dapat memberikan akuntabilitas yang lebih lagi, dan juga perhitungan langsung yang lebih cepat ke sistem yang sudah ada. Tetapi diharapkan dapat memberikan alat kepada pemilih untuk memastikan jujurnya suatu pemilihan, belum lagi di sistem seperti pemilihan menggunakan kertas, setelah kertas suara sudah di masukan ke dalam tempat kertas suara. Seorang pemilih tidak dapat mengetahui apakah kertas suaranya tidak berubah, dengan ini mereka bisa melihatnya. Walaupun begitu, orang lain tidak dapat menghubungkan suara pemilih itu ke pemilik suaranya.

Penulis juga terinspirasi membuat ini untuk mendukung SDGs ke-16. Dimana salah satu dari target SDG ke-16 adalah melakukan pengembangan transparansi dalam semua institusi. Lalu, institusi yang paling penting dari suatu demokrasi adalah institusi yang mengatur, membuat, dan menjalankan suatu pemilihan demokratis. Juga sesuai dengan apa yang penulis sudah katakan sebelumnya, hal ini dapat dilakukan di semua tingkatan, di suatu komunitas, hingga pada tingkatan suatu negara itu sendiri. Yang penting di sini adalah di tingkatan apapun itu adalah adanya pemilihan, dan keinginan untuk pemilihan itu untuk lebih transparan, dan lebih mudah untuk dipercaya.

2. Rumusan Masalah
    a. Mencari cara untuk melakukan pencatatan hasil pilihan dengan prinsip langsung, umum, bebas, rahasia, jujur, dan adil.
    b. Mencari cara melakukan verifikasi pemilih dengan sistem yang terdistribusi.

TELAAH PUSTAKA

1. *Blockchain*

Nofer, M. *dkk.* (2017) mengatakan bahwa *blockchain* biasanya berbentuk suatu kumpulan paket data (blok) yang dimana setiap blok terdiri dari berbagai macam transaksi. Blok itu dapat diperpanjang dengan menambahkan blok lainnya yang terhubung dengan blok sebelumnya. Dengan begitu dengan adanya hubungan dari paket data transaksi yang terhubung dari transaksi awal hingga terakhir, dapat merepresentasikan seluruh sejarah transaksi yang dilakukan oleh semua orang.

Kurang lebih cara kerjanya sama seperti bank yang melakukan pencatatan dari semua transaksi yang terjadi di bank tersebut. Berbedanya dalam *blockchain* transaksi dicatat, dan diverifikasi oleh banyak orang menggunakan data transaksi yang ada, akan mencapai suatu konsensus dari validitas transaksi tersebut. Mekanisme konsensus itu sendiri adalah "proses dimana mayoritas (atau di suatu kasus semuanya) dari suatu jaringan validator setuju dari kondisi suatu kas" (Swanson, 2015).

Dari *pengembangan* teknologi *blockchain* itu, terbentuklah *smart contract* atau kontrak pintar. Kontrak pintar itu sendiri adalah suatu kontrak yang dapat mengeksekusi kontraknya sendiri, sesuai dengan aturan dan ketentuan yang ada dalam bentuk kode komputer (Zou *dkk.*, 2019). Kontrak pintar itu berada di dalam suatu jaringan yang terdistribusi, yang memungkinkan untuk transaksi dilakukan oleh pihak yang tidak dapat dipercaya maupun identitasnya tidak diketahui (Tapscott dan Tapscott, 2016).

Teknologi kontrak pintar itu sendiri sekarang ini sudah memiliki banyak aplikasi di dunia asli. Bukan hanya di dalam bidang finansial seperti dalam asuransi, perdagangan ekuitas, dan lainnya. maupun dalam bidang non-finansial seperti dalam sistem anti pemalsuan dokumen, dan penyimpanan data yang tidak tersentralisasi di suatu *server* (Nofer *dkk.*, 2017).

2. *Decentralized Oracle*

Permasalahan dengan sistem kontrak pintar pada implementasinya pada sistem *blockchain* saat ini, seperti pada *Ethereum*, adalah walaupun dapat dilakukan konsensus dari hasil suatu kontrak pintar. Namun, data yang digunakan dalam komputasinya harus berada di dalam *blockchain*-nya itu sendiri (Greenspan, 2016). Hal ini diakibatkan oleh sistem *blockchain* yang deterministik, dimana semua hasil transaksi jika di jalankan kembali semua transaksi dari paket data pertama (*genesis block*) hingga yang terbaru, hasilnya maka hasilnya akan sama dengan kondisi yang ada sekarang.

Oleh karena itu untuk melakukan transaksi, atau melakukan eksekusi kontrak dari data yang tidak ada di *blockchain*, seperti data banjir untuk kontrak pintar asuransi banjir. Data ini tidak akan ada di dalam *blockchain*-nya sendiri, namun akan ada di misalkan website BMKG. Jadi dalam menggunakan kontrak pintar ini, dibutuhkan suatu sistem yang dapat menambahkan datanya ke dalam kontrak pintar-nya, agar dapat diverifikasi bahwa dalam menjalankan kontrak pintar itu, sudah sesuai dengan ketentuannya. Sistem ini dinamakan *oracles*, suatu sistem yang membawa data dari luar *blockchain* (*off-chain*) ke dalam *blockchain* (Greenspan, 2016; Breidenbach *dkk.*, 2021).

Namun, sistem *oracle* yang hanya berbentuk satu entitas yang dipercaya saja, bisa berbahaya. Entitas itu kurang lebih akan memiliki kekuasaan untuk merubah jalannya suatu kontrak pintar. Suatu titik permasalahan keamanan dan kepercayaan (Mendling *dkk.*, 2018). Oleh karena itu perlu dilakukan mitigasi, seperti menggunakan lebih dari satu *oracle* independen yang menjadi suatu *decentralized oracle* (Xu *dkk.*, 2018). Sehingga data yang masuk merupakan suatu konsensus dari berbagai *oracle* independen itu, mempertahankan konsep terdistribusi, dan saling tidak mempercayai dari *blockchain*.

ANALISA POTENSI DAN KEBUTUHAN

1. *Status Quo*

Pada pemilihan umum terakhir di Indonesia pada tahun 2019, dimana terjadi rekor jumlah pemilih, dimana jumlahnya naik 69% di pemilihan presiden, dan 75% di pemilihan legislatif. Walaupun begitu, tetap saja salah satu pihak di pemilihan itu yang tidak mau mengakui kekalahannya, bahkan sampai menyuruh pendukungnya untuk mengamati jika ada gangguan yang dapat merugikannya (2019). Hal ini bisa jadi memperlihatkan bahwa walaupun kondisi dalam pemilihan sudah baik, suatu pihak yang kalah akan tetap skeptikal terhadap sistem. Hal ini bukan saja hal yang terjadi di Indonesia, namun terjadi di pemilihan umum negara lain juga. Contohnya di Amerika Serikat, dimana pada tahun 2019 dimana partai Demokrat kalah, kepercayaan nya rendah pada 66%, namun pada tahun selanjutnya, saat rivalnya, Republikan kalah, kepercayaannya naik hingga ke 82% (*Voter Confidence*, 2021).

Hal ini juga dapat membuktikan bahwa sisi manapun dari suatu pemilihan sebenarnya dapat untuk mempercayai sistem itu sendiri. Namun, karena dianggap bahwa suatu otoritas sistem itu di bawah suatu sisi di suatu pemilihan. Jika otoritas itu disebarkan ke semua sisi di pemilihan, atau bahkan kepada orang yang netral di pemilihan itu. Penulis harapkan kepercayaan dapat lebih didapatkan karena mereka sendiri merupakan bagian dari pemilihan itu.

Permasalahan lainnya yang selalu muncul di pemilihan tingkatan apapun itu, adalah pemilih ganda. Data yang ada pasti akan dinamis, dengan jumlah pemilih yang akan bertambah dan berkurang setiap harinya (Hayati, 2018). Data ini yang lebih dinamis bisa saja dilakukan verifikasi lebih lanjut oleh pihak-pihak yang mengikuti pemilihan ini, sebagai suatu sumber data yang independen dari otoritas pemilihan utama. Data yang sudah diverifikasi secara independen dari setiap pihak yang ada di

pemilihan itu bisa digabungkan, dan hasilnya adalah konsensus dari semua pihak yang terpengaruhi oleh pemilihan tersebut.

Logika dari penulis di sini adalah pihak manapun yang mengikuti pemilihan itu pasti memiliki niatannya tersendiri. Dan pihak manapun itu di dalam pemilihan, pasti tidak ingin kalah. Jadi jika satu pihak menambahkan beberapa pemilih yang sebenarnya tidak ada, pihak lain pasti tidak menambahkannya, sehingga hasil konsensusnya pasti pemilih itu tidak ada. Sama halnya kepada pihak lainnya yang ada di situ. Di sini penulis bukannya tidak mempercayai otoritas utama, namun apa yang penulis rasakan jika pihak yang memilih itu di ajak untuk berpartisipasi langsung ke pemilihannya itu sendiri, mereka bisa mempercayainya lebih lagi, karena mereka itu juga yang menjalankannya.

2. Kebutuhan Dari Kondisi Sekarang
    a. Sistem Verifikasi Pemilihan

        Sistem verifikasi dari pemilih ini haruslah tidak memiliki suatu otoritas tertentu. Di dalam sistem ini kepercayaan tidak didapatkan namun memang tidak diperlukan. Perlu dibentuk sistem dimana tidak ada otoritas yang harus di percaya oleh pemilih itu sendiri. Walaupun begitu, sistem ini tidak boleh melupakan prinsip-prinsip dalam pemilihan, seperti langsung, umum, bebas, rahasia, jujur, dan adil.

    b. Sistem Verifikasi Pemilih

        Sama seperti sistem verifikasi pemilihan, sistem ini dilakukan secara terdistribusi ke semua pihak. Data pemilih yang ada divalidasi oleh semua pihak terkait, dan oleh otoritas utama dari pemilihan itu juga. Lalu, saat tenggat waktu sudah ditentukan, maka data pemilih, untuk setiap pemilih, akan dilakukan penggabungan data yang sudah divalidasi oleh semua pihak terkait dengan sistem konsensus dari data.

IDENTIFIKASI SOLUSI

1. Identifikasi Target Pembangunan

   Secara garis besar, target utama dari sistem ini adalah memberikan suatu sistem yang dapat digunakan untuk melakukan verifikasi dari pemilih dan pilihannya. Verifikasi pemilih yang dimaksudkan di sini adalah semua pihak yang ada di dalam suatu pemilihan dapat melakukan verifikasi independen, dan menyetujui daftar pemilih akhirnya. Sementara sistem verifikasi pilihan adalah sistem yang menyimpan dan memverifikasi data pilihan secara terdistribusi ke semua pihak yang terkait.

   Sistem ini dianggap memenuhi target jika sistem verifikasi pemilih dan pilihannya sudah diimplementasikan ke sistemnya. Dengan sistem verifikasi dapat melakukan verifikasi suatu pemilih berdasarkan suatu informasi yang dapat memverifikasi (seperti isi kartu e-KTP). Dengan registrasi tidak perlu dilakukan jika pemilih sudah terdaftar di daftar pemilih, namun jika konsensus dari validitasnya tidak valid, harus ditandai di dalam pilihannya.

   Sementara untuk sistem verifikasi pemilih dianggap memenuhi target jika sistem pemilihan dapat menyimpan hasil pilihan pemilih secara tersebar, dengan pilihannya masih dapat diakses oleh dirinya, namun tidak oleh orang lain. Hal ini berarti sistem harus dapat memberikan suatu identifikasi yang hanya diketahui oleh orang lain.

   Sementara itu produk hasilnya sendiri adalah suatu bukti dari konsep *DisProve* yang dapat memperlihatkan bagaimana kerja dari sistem yang ditargetkan. Prototipe ini harus bisa memperlihatkan bahwa sistem dapat dicapai, dan hal apakah yang dapat diperbaiki atau dikembangkan lebih lanjut untuk sistem penuhnya. Dengan hasil prototipenya dapat dibuat dengan waktu yang tidak begitu lama, sekitar dua minggu.

2. Analisis Solusi dari Target

Untuk mencapai target dari sistem yang akan dibuat maka ada beberapa hal yang harus dipertimbangkan terlebih dahulu, terutama dalam sistemnya yang tidak terdistribusi dan saling tidak mempercayai. Dengan adanya limitasi ini berarti tidak dimungkinkan untuk menggunakan sistem tradisional yang dimana data pilihannya di simpan ke satu titik tertentu, biasanya berupa server otoritas utama.

Sehingga disini penulis memilih sistem yang berbasis *blockchain*. Dimana sistem tidak membutuhkan kepercayaan antara satu sama lain, dan sistemnya yang terdistribusi berarti tidak memiliki suatu otoritas yang memegang semua data (Binance Academy, 2019). Sistem ini sudah pas sekali dengan kebutuhan yang sudah dijelaskan sebelumnya.

Untuk melakukan implementasi dari bukti konsep sistem *DisProve* ini akan dilakukan menggunakan implementasi dari *blockchain* yang sudah ada. Hal ini dilakukan karena kompleksitas dari melakukan implementasi *blockchain* dari awal. Apalagi *blockchain* yang sudah memiliki sistem kontrak pintar, yang dibilang sebagai *blockchain* generasi kedua (Sullivan, 2019). Sehingga akan digunakan *platform blockchain* yang sudah ada.

Beberapa *platform blockchain* yang dipertimbangkan adalah,

1. Ethereum

   Salah satu *platform blockchain* yang paling lama, dan merupakan salah satu yang pertama kali melakukan implementasi sistem kontrak pintar. Memiliki komunitas yang aktif, juga lingkungan pengembangan yang cukup lengkap dan mudah digunakan. Walaupun begitu, kecepatan transaksinya yang paling lambat di daftar pertimbangan ini.

2. Quorum

   Merupakan modifikasi dari Ethereum, dengan fitur tambahan yang berhubungan dengan privasi, dan fitur lainnya yang berhubungan dengan penggunaan *blockchain* di perusahaan. Memiliki pilihan algoritma verifikasi yang cukup lengkap. Juga

memiliki kecepatan transaksi yang jauh lebih cepat dibandingkan dengan Ethereum, dengan kemampuan hingga ribuan transaksi per detik (Baliga *dkk.*, 2018). *Platform* ini juga bisa menggunakan kontrak pintar di Ethereum yang berbasis EVM Solidity.

3. Hyperledger Fabric

   Suatu implementasi dari *blockchain* yang dibuat dengan arsitektur yang modular. Terdapat beberapa pilihan algoritma verifikasi yang dapat digunakan. Namun menggunakan sistem menjalankan kontrak pintar yang berbeda dengan lainnya, walaupun bahasa pemrograman yang sama bisa digunakan dengan translasi. Juga memiliki performa yang lebih baik dibandingkan dengan Ethereum (Thakkar, Nathan dan Viswanathan, 2018).

Dengan fungsi utama yang akan digunakan di dalam sistem ini adalah kontrak pintar, maka pilihannya akan diambil bergantung kepada performa, dan kemudahan dalam pengembangan. Walaupun memang Quorum dan Hyperledger Fabric memiliki performa yang jauh lebih baik dibandingkan dengan Ethereum, kemudahan dalam pengembangannya masih jauh di Ethereum. Walaupun begitu, dengan mengembangkan di Ethereum, kontrak pintar juga dapat di *deploy* di Quorum. Sehingga apa yang penulis gunakan di sini adalah Ethereum, dengan hasilnya nanti dapat di gunakan di Quorum.

Sementara untuk membangun *oracle* penulis memilih untuk menggunakan Node.js. Pemilihan ini berdasarkan kemudahan dari pengembangan aplikasi yang dibutuhkan, yaitu sumber data yang mendengarkan perintah dari kontrak pintar, dan juga familiaritas dari penulis. Bisa saja dilakukan dengan alternatif lain, seperti menggunakan Java, dan Go. Namun, dengan adanya *library* web3.js untuk Node.js untuk melakukan interaksi dengan *blockchain* Ethereum, hal ini sangatlah memudahkan pengembangan *oracle* dibandingkan dengan alternatif lain.

DESKRIPSI PRODUK SOLUSI

1. Deskripsi Produk

   DisProve merupakan suatu sistem yang dapat digunakan bersandingan dengan sistem pemilihan yang sudah ada, untuk melakukan pencatatan pilihan pemilih dan validasi pemilih dalam suatu pemilihan. Pencatatan dan validasi yang dilakukan dalam sistem *DisProve* ini dilakukan tanpa dibutuhkannya suatu otoritas pusat, melainkan dilakukan secara terdistribusi ke banyak pihak dan tempat. Hasil pencatatan yang terdistribusi tersebut kemudian dapat digunakan sebagai suatu sumber data validasi dari hasil pemilihan di sistem yang sudah ada.

2. Cara Kerja Produk

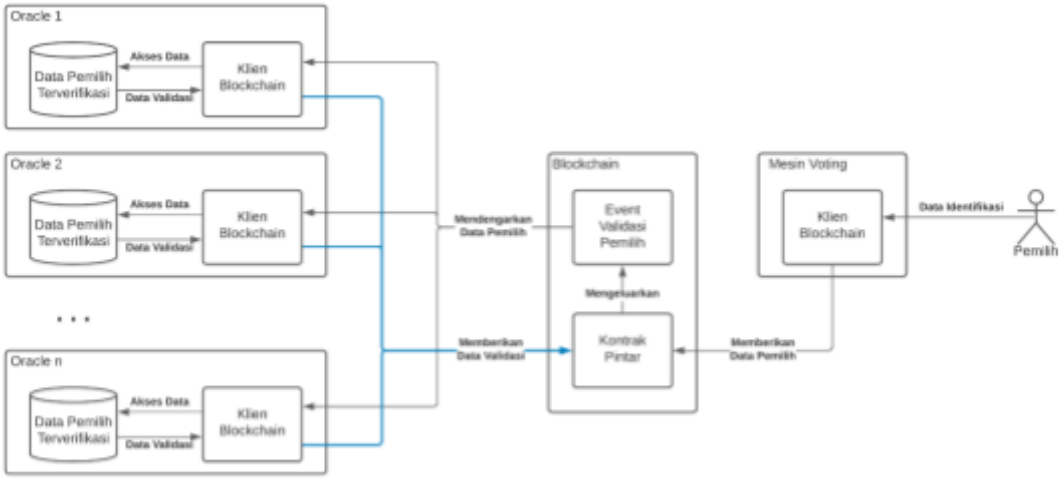
   Di dalam sistem *DisProve* sendiri terdiri dari 2 sistem yang memiliki fungsi yang berbeda, yang pertama adalah sistem validasi pemilih berbasis konsensus, lalu sistem pencatatan pilihan dari pemilih yang sudah tervalidasi. Penjelasan untuk tiap sistem akan dijelaskan di bawah ini,

   a. Sistem Validasi Pemilih Berbasis Konsensus

      Sistem validasi dari pemilih ini dilakukan dengan konsensus dari setiap pihak di dalam suatu pemilihan yang melakukan validasi dari daftar pemilih. Jadi, pertama haruslah sudah dibentuk suatu daftar dari pemilih yang akan mengikuti pemilihan ini. Lalu, setiap pihak yang terkait (misalkan KPU, dan pihak pasangan calon) akan melakukan validasi dari daftar pemilih secara independen.

      Setelah daftar pemilih sudah di validasi oleh setiap pihak, maka data itu akan dilakukan penggabungan untuk menghasilkan daftar pemilih akhir. Penggabungan ini dilakukan dengan setiap pemilih di daftar awal itu akan dilihat dan jika di mayoritas daftar yang sudah divalidasi ada, maka pemilih itu akan dimasukan ke dalam daftar pemilih akhir. Proses ini dilakukan sebelum pemilih

melakukan pemilihannya di sistem yang sudah ada. Jadi operator akan meminta validasi ke sistem terhadap suatu pemilih, dengan mengirimkan suatu informasi tertentu (seperti data KTP).

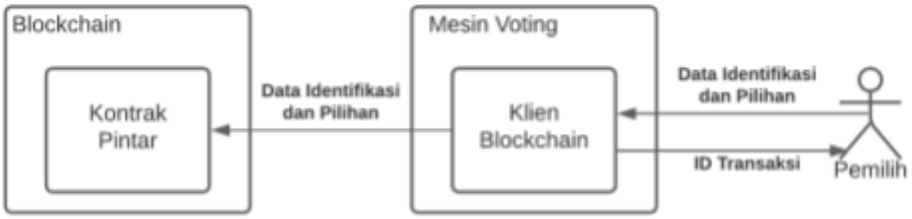


Gambar 1. Sistem Verifikasi Pemilih

Pemilih yang terverifikasi maupun tidak diperbolehkan untuk melanjutkan ke pemilihan. Namun, data apakah pemilih secara konsensus terverifikasi atau tidak akan ditambahkan ke data pemilihannya. Sistem pencatatannya akan dijelaskan selanjutnya/

b. Sistem Pencatatan Pilihan dari Pemilih

Pencatatan dari pemilih dilakukan dengan seorang pemilih memberikan informasi identifikasinya, dan pilihannya. Pilihannya ini akan di rekam di dalam daftar transaksi *blockchain* dan juga dihitung langsung di dalam kontrak pintarnya.



Gambar 2. Sistem Pencatatan Pilihan

Sementara untuk verifikasi apakah pilihan sudah dicatat dengan benar, digunakan id transaksi. Id transaksi ini dapat di lacak

di daftar transaksi *blockchain* dan dapat dilihat apakah benar apa yang dipilih memang dikirimkan ke kontrak pintarnya.

Di luar kedua sistem itu, akan terdapat fungsi tambahan di dalam kontrak pintarnya, yaitu fungsi untuk memulai dan mengakhiri pemilihan. Hal ini dapat dilakukan oleh siapapun, namun dengan ketentuan tertentu. Ketentuan itu adalah waktu mulai dan akhir dari suatu pemilihan. Jika kondisi tidak terpenuhi maka fungsi itu tidak akan dijalankan.

3. Rancangan Rencana Kerja

Tahapan utama yang dilakukan dalam membuat produk sesuai dengan targetnya adalah,

1. Pendefinisian Kebutuhan dan Target Sistem

   Tahapan ini ditunjukan dalam melakukan definisi kebutuhan, dan juga memberikan target dan batasan dari sistem. Tahapan ini dilakukan selama 2 hari.

2. Pencarian dan Pembentukan Rancangan Solusi

   Tahapan ini dilakukan untuk mencari contoh yang sudah ada, alat yang dapat membantu, dan lainnya untuk membentuk suatu solusi dari kebutuhan sistem. Tahapan ini dilakukan selama 5 hari.

3. Implementasi Solusi

   Pada tahapan ini dilakukan implementasi solusi yang sudah direncanakan pada tahapan sebelumnya. Diperkirakan akan memakan waktu 5 hari.

4. Verifikasi Implementasi Solusi

   Tahapan ini dilakukan dengan maksud verifikasi prototipe yang telah dibuat terhadap kebutuhan yang sudah didefinisikan. Diperkirakan akan memakan waktu 2 hari.

Sementara untuk pihak yang melakukannya hanyalah penulis. Hal ini dikarenakan produk akhir hanyalah suatu prototipe dari suatu konsep.

PRODUK HASIL DAN PEMBAHASAN

1. Produk Hasil

   Setelah dilakukan implementasi, sistem yang dihasilkan adalah suatu prototipe yang memperlihatkan konsep dari *DisProve* ini sendiri. Prototipe ini dibangung di atas *platform* Ethereum, dimana jaringannya dibentuk secara privat, dan bukan menggunakan jaringan utamanya. Hal ini dilakukan karena memang tidak diperlukan untuk berada di jaringan utamanya, apalagi dengan biayanya yang cukup tinggi. Sementara itu, dari sistem kontrak pintarnya dibuat dari Solidity yang merupakan bahasa pemrograman yang digunakan dalam Ethereum.

   Secara sistemnya sendiri, semua rancangan diikuti, berarti hasil implementasi terdiri dari kontrak pintar, klien *oracle*, dan juga klien pemilih. Semua klien yang ada tidak dibentuk tampilan grafis karena kekurangannya waktu, dan juga dianggap tidak diperlukan dalam tahapan ini. Melainkan, hal tersebut merupakan pengembangan lebih lanjut dari prototipe pertama ini.

2. Kelebihan dan Limitasi Produk Hasil

   Dalam memperlihatkan konsep dari *DisProve* ini sudahlah sangat baik. Dalam klien pemilih, pemilih dapat melihat siapa saja yang merupakan calonnya, pemilih melakukan verifikasi menggunakan data pemilihnya, dan juga hasil dari pilihannya dapat dilacak setelah melakukan pemilihannya. Namun, memang dalam melakukan pendaftaran pemilih ini masih harus ada komunikasi dan pertukaran informasi pemilih di luar jaringan *blockchain*. Hal ini membuatnya tetap harus memiliki suatu panitia yang harus melakukan pendaftarannya, atau sistem lainnya. Walaupun memang informasi pemilih sudah berhasil disembunyikan dengan fungsi kriptografi *hash*.

   Sementara itu dalam sistem *oracle*, mayoritas kebutuhan sudah diimplementasikan. Seperti sistem yang mendengarkan permintaan data

verifikasi dari kontrak pintar, juga validasi yang sudah berbasisi data yang sudah ada, dan dalam kontrak pintar sudah memiliki limitasi hanya *oracle* yang dapat melakukan validasi. Namun, sistem basis data masih sangat tradisional, hanya berbentuk suatu berkas digital, membuatnya cukup lambat terutama dalam jumlah pemilih yang besar (di atas 10000 orang).

Secara keseluruhan, sistem yang sudah ada sudah sesuai dengan prinsip utama dari *DisProve*, dengan sistemnya yang berbasis di Ethereum, maka bukan hanya terdistribusi, namun saling tidak mempercayai juga. Operasi apapun dilakukan hanya jika konsensus jaringan sudah didapatkan. Hanya bagian seperti validasi pemilih yang terbukti sulit, terutama dalam komunikasi di *blockchain* yang selalu publik, sehingga masih dibutuhkan komunikasi di luar *blockchain*. Juga permasalahan lainnya berada di dalam performa, walaupun penulis tidak bisa memperbandingkan dengan hasil yang ada di luar karena mesin yang ada tidak mencapai spesifikasi hasil yang ada, namun penulis melihat bahwa sistem ini dapat lebih cepat lagi dari kondisi yang ada sekarang.

3. Pengembangan Lanjutan

Melihat dari limitasi yang dimiliki *DisProve* saat ini, fokus dari pengembangan lanjutannya akan ke arah privasi pemilih, dan juga ke arah optimasi performa. Privasi yang ada sekarang ini di dalam *DisProve* masih bisa dibilang kurang, dengan data validasi dapat terlihat, walaupun data sebenarnya tersembunyi. Hal ini menurut penulis membutuhkan *platform blockchain* yang memiliki transaksi privat, seperti Quorum, sehingga data tidak bisa terlihat oleh orang lain.

Juga dalam performa, dengan melakukan skala yang diperbesar, maka sistem dipastikan akan cukup lambar. Hal ini terjadi karena basis dari Ethereum yang menggunakan algoritma yang lambat namun cukup aman, Tetapi jika *blockchain* yang dipakai privat, tidak diperlukan keamanan terlalu besar, sehingga *platform blockchain* quorum atau Hyperledger dapat digunakan untuk membuat performa *DisProve* lebih baik.

VISUALISASI GAGASAN

<table>
<tr>
<td rowspan="4">Situasi Saat Ini
Sistem pemilihan yang ada secara langsung, maupun digital masih membutuhkan kepercayaan terhadap suatu otoritas.
Otoritas tersebut bisa saja menjadi titik kegagalan dari sistem pemilihan.
Proses yang segalanya dilakukan oleh satu otoritas, menyulitkan akuntabilitas dan transparansi. Hal ini karena banyaknya bagian dari sistem yang berjalan.</td>
<td>Sasaran
Suatu sistem yang dapat digunakan bersandingan dengan yang sudah ada, tanpa adanya suatu otoritas yang mengaturnya. Caranya dengan menggunakan sistem terdistribusi.
Sistem ini akan dapat melakukan suatu validasi dari pemilih, dan pilihannya. Dengan semua pilihan dari semua pemilih dapat dilihat dan dibuktikan oleh pemilih yang memilihnya.</td>
</tr>
<tr>
<td>Hambatan
Teknologi yang digunakan masih baru dan masih cukup eksperimental. Penggunaannya di bidang voting terbatas di skala kecil. Juga dalam penggunaan di tingkatan tinggi (seperti nasional), dapat memakan waktu dan biaya cukup besar.
Dibutuhkan riset lebih lanjut, yang dapat memakan biaya cukup besar.</td>
</tr>
<tr>
<td>Bantuan
Perkembangan teknologi di bidang ini sangat cepat. Juga sudah mulai ada yang menggunakan sistem pemilihan dengan cara ini di tingkatan kota.</td>
</tr>
<tr>
<td>Tindakan
Melakukan riset lebih lanjut dalam penggunaan blockchain sebagai medium pemilihan. Juga dalam bidang pembuktian identitas dalam sistem terdistribusi.</td>
</tr>
</table>

LAMPIRAN

Hasil implementasi dari *DisProve* sesuai dengan hasilnya, dapat ditemui di https://github.com/fauh45/DisProve.

DAFTAR PUSTAKA

Baliga, A. *dkk.* (2018) "Performance Evaluation of the Quorum Blockchain Platform," *Computing Research Repository*. Tersedia pada: http://arxiv.org/abs/1809.03421.

Binance Academy (2019) *Trustless*. Binance Academy. Tersedia pada: https://academy.binance.com/en/glossary/trustless (Diakses: 13 Mei 2021).

Breidenbach, L. *dkk.* (2021) "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks." Tersedia pada: https://research.chain.link/whitepaper-v2.pdf (Diakses: 11 Mei 2021).

Greenspan, G. (2016) *Why Many Smart Contract Use Cases Are Simply Impossible*, *Coindesk*. Tersedia pada: https://www.coindesk.com/three-smart-contract-misconceptions (Diakses: 11 Mei 2021).

Hayati, N. N. (2018) "Daftar Pemilih Ganda, Masalah yang Itu-itu Melulu dalam Pemilu." Disunting oleh L. H. Wiwoho, 9 November. Tersedia pada: https://nasional.kompas.com/read/2018/09/12/13082951/daftar-pemilih-ganda-masalah-yang-itu-itu-melulu-dalam-pemilu?page=all (Diakses: 11 Mei 2021).

Mendling, J. *dkk.* (2018) "Blockchains for Business Process Management - Challenges and Opportunities," *ACM Transactions on Management Information Systems*, 9(1), hlm. 1–16.

Nofer, M. *dkk.* (2017) "Blockchain," *Business & Information Systems Engineering*, hlm. 183–187. doi: 10.1007/s12599-017-0467-3.

Sullivan, J. (2019) *Ethereum Fundamentals*. O'Reilly Media, Inc.

Swanson, T. (2015) "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems." Tersedia pada: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed

-ledgers.pdf.

Tapscott, D. dan Tapscott, A. (2016) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.

Thakkar, P., Nathan, S. dan Viswanathan, B. (2018) "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. doi: 10.1109/mascots.2018.00034.

Voter Confidence (2021) *MIT Election Lab*. Tersedia pada: https://electionlab.mit.edu/research/voter-confidence (Diakses: 11 Mei 2021).

Xu, X. *dkk.* (2018) "A Pattern Collection for Blockchain-based Applications," *Proceedings of the 23rd European Conference on Pattern Languages of Programs*. doi: 10.1145/3282308.3282312.

Zou, W. *dkk.* (2019) "Smart Contract Development: Challenges and Opportunities," *IEEE Transactions on Software Engineering*. doi: 10.1109/TSE.2019.2942301.

(2019) "Indonesia Sees Record Turnout in Historic Election, Braces for Fallout," 17 April. Tersedia pada: https://jakartaglobe.id/context/indonesia-sees-record-turnout-in-historic-election-braces-for-fallout (Diakses: 11 Mei 2021).