



## Rancangan Simulasi Penerapan *Blockchain* dalam Pemilihan Presiden Indonesia

### Blockchain Implementation Simulation for Presidential Voting in Indonesia

Nopendri<sup>\*1</sup>, Rio Aurachman<sup>1</sup>, Muhammad Rafid Amrullah<sup>2</sup>

<sup>1</sup>Program Studi Teknik Industri, Fakultas Rekayasa Industri, Telkom University

<sup>2</sup>Program Studi Teknik Informatika, Fakultas Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung

#### ARTICLE INFO

##### Article history:

Diterima 03-10-2019

Diperbaiki 19-02-2020

Disetujui 21-06-2020

Kata Kunci:

*Blockchain*, Politik, *voting*

#### ABSTRAK

*Blockchain* memiliki beberapa fitur yang menjamin keamanan dan konsistensi dalam transaksi dan penyimpanan data. *Blockchain* telah diterapkan dalam berbagai bidang. Penerapan *blockchain* terutama marak dalam bidang keuangan dalam bentuk *cryptocurrency*. Dalam bidang politik, telah digagas pula opsi penerapan *blockchain*, yaitu dalam proses *e-voting*. Gagasan tersebut berkembang melalui berbagai riset di luar Indonesia maupun di Indonesia. Riset kali ini berusaha mengusulkan simulasi awal dari penerapan *blockchain* dalam pemilihan presiden di Indonesia.

#### ABSTRACT

Blockchain has several features that guarantee security and consistency in transaction and data storage. Blockchain has been applied in various fields. The application of blockchain is popular in the financial sector in the form of cryptocurrency. In the political field, the option of implementing blockchain has also been initiated, especially for e-voting process. The idea developed through various researches. This research tried to propose an initial simulation of blockchain implementation in the presidential election in Indonesia.

##### Keywords:

Blockchain, Politics, Voting

### 1. Pendahuluan

Blockchain umum digunakan di bidang jasa keuangan karena inefisiensi yang terjadi pada jasa keuangan dan sulitnya melakukan penelusuran data pada sistem yang ada sekarang [1]. Selain di jasa keuangan blockchain juga diterapkan pada bidang kesehatan sehingga pasien bisa mengetahui *history* penanganan kesehatannya lintas *provider* [2]. Blockchain juga diterapkan pada bidang Intelligent Transformation System, yang mana meningkatkan efisiensi dalam penggunaan sumber daya yang ada [3]. Internet of Thing pada supply chain juga berpotensi mendapatkan manfaat dari diterapkannya blockchain dalam aspek keamanan [4]. Selain *supply chain*, penerapan *internet of thing* dan *smart device* dengan *blockchain* nya juga dapat diterapkan dalam pembangunan *smart cities* [5]. Dalam bidang ekonomi, *blockchain* berpotensi untuk meningkatkan performansi ekonomi suatu wilayah seperti meningkatkan persaingan, mengurangi resiko privasi, dan mencegah terpusatnya kekuatan ekonomi pada pemilik platform [6].

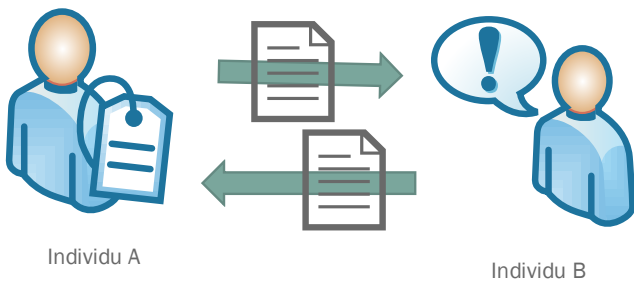
Secara khusus *blockchain* juga diterapkan dalam proses pemilihan dan demokrasi. Sebagai contoh terdapat kajian yang

membahas beberapa masalah dalam proses pemilihan politik kini, dan bagaimana blockchain dapat menjadi solusi [7]. Riset lain menganalisis aspek keamanan blockchain dalam *voting system* dan bagaimana performansinya dalam sistem skala besar [8]. Sementara itu riset lainnya merancang sebuah sistem bernama BEV (Blockchain Enabled Voting) dan mengkaji potensi manfaat dan potensi masalahnya [9]. Penerapan lainnya yang telah dikaji, menggunakan sistem *smart contract ethereum*, dengan nama Open Vote Network [10].

Beberapa riset telah berusaha menyampaikan penerapan *blockchain* dalam pemilihan di luar negeri. Untuk penerapan di Indonesia, juga telah ada riset tentang penerapan *blockchain* dalam sistem pemilu di Indonesia [11][12]. Adapun paper ini berusaha berkontribusi dalam mengilustrasikan dan mensimulasikan proses blockchain dalam konteks pemilihan presiden 2019. Riset ini diharapkan dapat berkontribusi memberikan pemahaman dan ilustrasi bagi pengambil keputusan yang akan menerapkan sistem blockchain dalam pemilihan calon presiden.

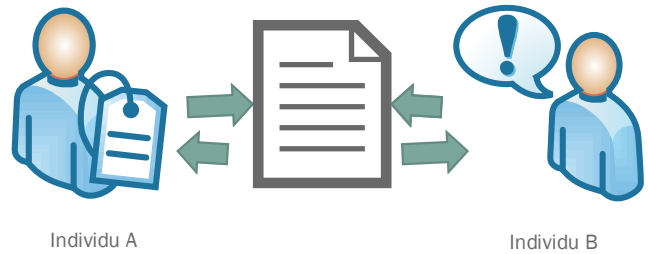
## 2. Studi Literatur

Dalam melakukan distribusi informasi, beberapa metode dapat dilakukan. Jika diilustrasikan dengan tata cara pengiriman informasi dokumen, cara paling sederhana yang bisa dilakukan adalah melakukan pengiriman dokumen lewat *email*. Ketika dilakukan pengiriman data lewat *email* antara dua individu, proses perubahan dokumen harus dilakukan secara bergantian. Ketika individu A melakukan edit terhadap dokumen, individu B tidak bisa melakukan perubahan. Begitu pun sebaliknya ketika individu B melakukan edit kepada dokumen, maka individu A tidak bisa melakukan edit terhadap dokumen. Jika setiap pihak ingin terlibat dalam proses edit, maka proses edit harus dilakukan secara bergantian. Bila kedua inividu melakukan perubahan secara Bersama-sama, maka akan terjadi masalah dalam sinkronisasi konten dokumen. Bisa jadi individu A mengedit halaman 1 menjadi berwarna hijau misalnya, di saat yang bersamaan individu B melakukan edit halaman 1 menjadi berwarna merah, tentu akan terjadi dua versi dokumen. Dokumen yang akan dikelola tersebut tetap hanya satu versi yang diisi secara bergantian. Individu A mengedit dahulu dokumen, kemudian setelah selesai, mengirimkan dokumen tersebut kepda individu B. Individu B boleh melanjutkan edit. Setelah selesai, dapat dikembalikan ke A untuk lalu giliran A melakukan proses edit. Hal tersebut dilakukan secara terus menerus hingga nanti didapatkan dokumen yang sesuai dengan harapan.



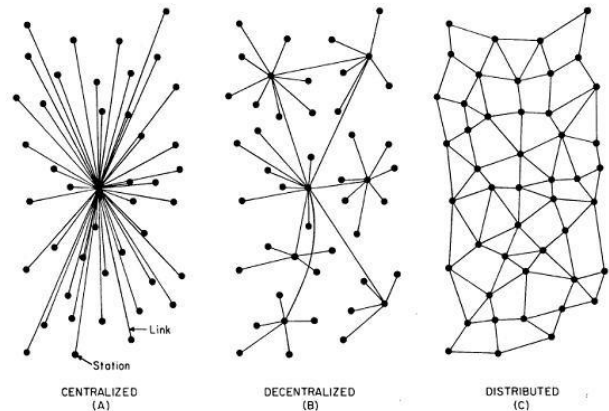
Gambar 1 Ilustrasi proses transaksi data menggunakan *email*

Cara kedua yang bisa dilakukan dalam melakukan edit dokumen adalah menggunakan sistem yang tersentralisasi. Teknologi yang umumnya digunakan adalah Google Docs. Dokumen yang biasanya tersimpan dalam Google Drive masing-masing individu, kini tersimpan di sebuah *server* yang bisa diakses melalui internet. Setiap individu dapat mengakses dokumen tersebut dan melakukan edit secara bersama-sama. Proses edit dokumen ini dapat diilustrasikan dengan proses menulis secara bersama-sama di papan tulis, hanya saja kali ini papan tulisnya terdapat di server awan dan diakses melalui internet. Sebagaimana papan tulis yang besar, individu A dan individu B dapat melakukan edit secara bersama-sama pada bagian yang berbeda. Individu A dan individu B tidak perlu saling berkirim dokumen dan menjaga sehingga hanya ada satu versi dokumen yang dipindah-pindahtanggankan. Menggunakan Google Docs, memang hanya ada satu versi dokumen yang terdapat di *server* awan. Dokumen tersebut dapat secara aman diedit bersama-sama. Dokumen tersebut menjadi semakin lama semakin terlengkapi dengan kontribusi individu A dan individu B yang melakukan edit secara simultan. Metode kedua ini lebih praktis dikarenakan menghilangkan proses berkirim data. Akan tetapi metode ini tetap menyimpan beberapa resiko dan bahaya.



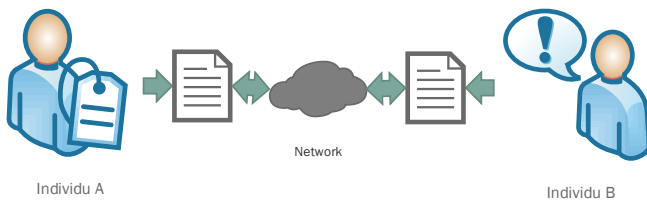
Gambar 2 Ilustrasi proses transaksi data menggunakan aplikasi berbasis *cloud* yang kolaboratif

Masalah yang timbul yaitu ada *single point of failure*. Jika terdapat masalah pada dokumen Google Docs dan *servernya*, maka keseluruhan sistem proses pengeditan dokumen juga menjadi bermasalah. Berbeda dengan proses transaksi data menggunakan *email*, jika terjadi kerusakan pada dokumen yang sedang dipegang oleh individu A, maka individu B masih memiliki versi dokumen sebelumnya sehingga informasi masih terjaga. Hal ini berbeda dengan sistem yang tersentralisasi seperti Google Docs. Ketika *server* Google Docs terganggu dan file terhapus, maka baik individu A dan individu B tidak memiliki dokumen untuk diperbaiki. Potensi masalah yang lain adalah setiap individu bisa jadi tidak punya akses terhadap Google Docs secara *online*.



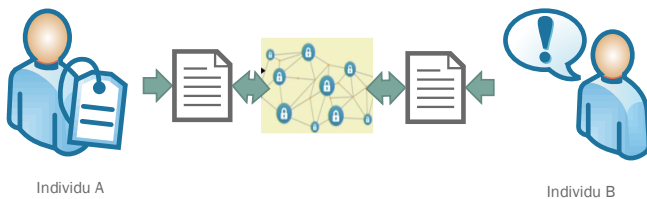
Gambar 3 Alternatif jaringan komunikasi dan penyimpanan informasi [13]

Dalam menyelesaikan potensi masalah *single point of failure* tersebut, terdapat teknologi yang dapat menjadi solusi. Alih-alih satu buah *file* yang disimpan dalam satu buah server tersentralisasi, informasi bisa tidak disimpan secara terpusat, dan tersimpan di masing-masing individu. Akan tetapi informasi yang disimpan di masing-masing individu tersebut selalu *terupdate* dan tersinkronisasi dengan perubahan-perubahan pada individu lainnya. Sistem ini disebut sebagai *distributed ledger*. Setiap individu mengendalikan satu buah versi dokumen, dan internet bertugas menjamin konsistensi antara semua data yang tersebar tersebut. Antara dokumen yang dipegang oleh individu A dan dokumen yang dipegang oleh individu B diperantarakan oleh sebuah sistem yang memastikan kedua dokumen tetap sinkron.



Gambar 4 Ilustrasi proses transaksi data menggunakan perantara *network*

Sistem perantara yang menjamin sinkronisasi tersebut dapat menggunakan database sederhana. Database tersebut lalu menguji kesesuaian data. Akan tetapi menggunakan database dan sistem sinkronisasi tersebut masih menimbulkan resiko *single point of failure*. Terdapat teknologi yang dapat melakukan pengecekan dan sinkronisasi data tersebut secara *massive* dan *crowdsourcing*. Sistem tersebut dilakukan secara *crowdsourcing* sehingga proses sinkronisasi tidak dilakukan oleh satu buah individu yang terpusat. Proses sinkronisasi dilakukan oleh *crowd* atau sekumpulan individu yang disebut sebagai *miner* atau *node*. Teknologi dan sistem tersebut disebut sebagai *blockchain*.



Gambar 5 Ilustrasi proses transaksi data menggunakan perantara *blockchain*

Selain data tersimpan pada setiap individu A dan individu B, data juga terdistribusi copy nya pada setiap *miner* yang berada dalam sistem *blockchain*. Maka dari itu sistem ini disebut sebagai *distributed ledger*. Dikarenakan tersimpan pada setiap *miner* yang berjumlah banyak tersebut, resiko terjadi kesalahan data, akan menjadi berkurang. Setiap *miner* memiliki *local copies*. *Local copies* tersebut diupdate menggunakan sistem global.

Setiap informasi yang muncul dan akan dicatat, disebut sebagai blok. Setiap blok tersebut membentuk suatu rangkaian sehingga disebut sebagai rantai blok atau *blockchain*. Ketika muncul satu buah blok data, maka blok tersebut akan *distributed* kepada semua *miner*. Para *miner* akan berlomba-lomba untuk melakukan verifikasi data dan melakukan *mining*. *Miner* yang berhasil lebih dahulu melakukan *mining*, akan mendapatkan insentif. Bila terjadi perbedaan verifikasi dan muatan data antara *miner*, maka akan dilakukan *consensus* dan diambil nilai terbanyak yang disepakati. Bila sudah dilakukan verifikasi dan *mining*, maka data tersebut akan tersimpan dalam *distributed ledger*. Blok berikutnya akan dibangun dengan melanjutkan blok sebelumnya. Koneksi antara blok tersebut diikat oleh nilai dari *hash*. Proses *hash* tersebut menggunakan SHA256. *Hash* pada blok selanjutnya akan merupakan hasil enkripsi dari *hash* di blok sebelumnya. Hal ini akan mencegah terjadinya penyelewengan data. Karena setiap perubahan dari data yang sudah tersimpan dalam *blockchain*, akan mempengaruhi blok yang ada setelahnya, dan tentu akan segera disadari oleh sistem.

### 3. Metode Penelitian

Dalam rangka mendapatkan rancangan awal dari sistem *blockchain* untuk Pemilu perlu dilakukan tahapan dan metode penelitian. Tahapan pertama adalah melihat seluruh proses transaksi informasi dan data dari proses pemilihan. Dari proses pemilihan tersebut lalu dipilih subproses mana yang akan ditunjang dengan teknologi *blockchain*. Pemilihan tersebut berdasarkan tipe aktivitas yang penuh dengan transaksi data lintas individu. Pemilihan juga bisa didasarkan pada aktivitas yang memiliki risiko paling tinggi. Risiko tertinggi tersebut perlu dimitigasi dengan sistem *blockchain*. Bentuk risiko salah satunya adalah terjadi penyelewengan dan manipulasi data. Manipulasi dapat terjadi pada perolehan suara bakal calon pimpinan yang dipilih maupun manipulasi terhadap data penunjang lainnya.

Tahap selanjutnya adalah memilih informasi mana saja dari aktivitas tersebut yang akan ditunjang dengan fungsi *blockchain*. Informasi tersebut perlu dipilih secara cermat untuk mencegah beratnya sistem dalam mengelola banyak data. Data perlu dibuat seefisien mungkin tanpa harus mengurangi efektifitas dari transaksi data. Informasi yang dipilih bisa berdasarkan tujuan utama dari sistem. Untuk sistem pemilihan presiden misalnya, memiliki tujuan untuk mendapatkan calon yang paling banyak dipilih oleh *voter*. Maka data jumlah memilih untuk masing-masing calon harus tersimpan dan terdata.

Tahap berikutnya adalah merancang bentuk tampilan dan antar muka dari simulasi penerapan *blockchain* tersebut. Tampilan tersebut dapat mengacu kepada aplikasi yang sudah ada. Dari aplikasi yang sudah ada tersebut dikembangkan untuk mendapatkan versi dan rancang baru. Rancangan baru tersebut dibuat sesuai dengan kebutuhan dari penerapan.

Setelah didapatkan rancangan tampilan dari aplikasi *blockchain*, tahap berikutnya adalah menentukan formulasi perhitungan yang akan digunakan. Formulasi yang dimaksud meliputi operasi matematika sederhana maupun metode enkripsi yang dibutuhkan.

Tahap terakhir adalah menguji coba simulasi yang sudah dirancang. Dalam uji coba tersebut, dilakukan pengecekan fungsi dan tampilan. Evaluasi dilakukan untuk analisis rencana perbaikan dan pengembangan lebih lanjut. Output dari perancangan ini dapat digunakan sebagai sebuah cikal bakal sistem yang lebih besar. Rancangan ini pun dapat berfungsi sebagai media komunikasi kepada *stakeholder* yang awam dalam bidang teknologi *blockchain*.

### 4. Hasil dan Pembahasan

Berdasarkan website KPU, tahapan pemilihan umum meliputi beberapa tahap sebagai berikut:

1. Perencanaan Program dan Anggaran
2. Penyusunan Peraturan KPU
3. Sosialisasi
4. Pendaftaran dan Verifikasi Peserta Pemilu
5. Penyelesaian Sengketa Penetapan Partai Politik Peserta Pemilu
6. Pembentukan Badan Penyelenggara
7. Pemutakhiran Data Pemilih dan Penyusunan Daftar Pemilih
8. Penyusunan Daftar Pemilih di Luar Negeri
9. Penataan dan Penetapan Daerah Pemilihan (Dapil)

10. Pencalonan Anggota DPR, DPD, DPRD Provinsi dan DPRD Kabupaten / Kota Serta Pencalonan Presiden dan Wakil Presiden
11. Penyelesaian Sengketa Penetapan Pencalonan Anggota DPR, DPD dan DPRD Serta Pencalonan Presiden dan Wakil Presiden
12. Logistik
13. Kampanye Calon Anggota DPR, DPD dan DPRD Serta Pasangan Calon Presiden dan Wakil Presiden
14. Laporan dan Audit Dana Kampanye
15. Masa Tenang
16. Pemungutan dan Perhitungan Suara
17. Rekapitulasi Perhitungan Suara
18. Penyelesaian Sengketa Hasil Pemilu DPR, DPD, DPRD, Provinsi dan DPRD Kabupaten / kota
19. Penyelesaian Sengketa Hasil Pemilu Presiden dan Wakil Presiden
20. Pene tapan Perolehan Kursi dan Calon Terpilih Tanpa Permohonan Perselisihan Hasil Pemilu
21. Penetapan Perolehan Kursi dan Calon terpilih Pasca Putusan Mahkamah Konstitusi
22. Peresmian Keanggotaan
23. Pengucapan Sumpah /Janji

Dari beberapa tahap tersebut, bagian yang terjadi transaksi data adalah proses

1. Pemutakhiran Data Pemilih dan Penyusunan Daftar Pemilih
2. Penyusunan Daftar Pemilih Di Luar Negeri
3. Rekapitulasi Perhitungan Suara

Tahapan-tahapan tersebut memiliki transaksi data yang besar dan bersifat kritis. Kritis di sini bermakna bahwa jika terdapat kesalahan data pada proses pengiriman, pencatatan, dan penetapan data maka implikasi dan resiko nya demikian besar. KPU sebagai organisasi mendapatkan kritikan dan membangkitkan ketidakpercayaan publik kepada penyelenggara negara. Dari ketiga proses tersebut, yang mendapatkan perhatian publik paling besar adalah proses rekapitulasi suara. Hal tersebut dapat dilihat pada jumlah berita dan percakapan publik di dunia maya tentang ketiga topik tersebut. Maka rancangan penerapan *blockchain* akan difokuskan pada proses rekapitulasi perhitungan suara, khususnya perhitungan suara calon presiden.

Data yang ditransaksikan adalah rekap hasil suara dari tiap TPS yang lalu dapat direkap pada tingkat kelurahan. Setelah direkap pada tingkat kelurahan, lalu direkap pada tingkat kecamatan, lalu, kota/ kabupaten, provinsi, dan terakhir rekap pada level nasional. Beberapa resiko kesalahan yang mungkin terjadi pada proses perhitungan adalah sebagai berikut.

1. Kesalahan penulisan pada form C1 (Formulir yang merekap hasil pemilu di TPS)
2. Kesalahan entri data pada sistem KPU

*Blockchain* dapat berperan dalam melakukan validasi dan verifikasi dari perhitungan dan pencatatan secara massal menggunakan *distributed ledger*. *Ledger* yang kini berada pada KPU, dapat didistribusikan dalam sistem *blockchain*. Pada dasarnya, *ledger* dari rekap pemilihan kini pun sudah terdistribusi pada beberapa sistem yang dibuat oleh relawan pemantau pemilu. Proses validasi pun dilakukan secara manual oleh para relawan pemantau. Dengan bantuan *blockchain*, pemantauan tersebut dibantu dengan sistem yang terpadu dan terstruktur proses validasinya.

Perancangan *mock up* berdasarkan konsep yang dibuat oleh Anders (<https://anders.com/blockchain>). Pada tahap pencatatan hasil dari tiap TPS, diwakili oleh satu *block*. Antara *block* yang satu dengan *block* yang lain mewakili hasil dari tiap TPS yang berbeda. Setiap *peer* nanti akan melakukan validasi terhadap hasil pencatatan dan melakukan *mining* bila ternyata hasil sudah valid. Bila ternyata antara *peer* tidak terjadi kesepakatan tentang hasil yang valid, maka proses validasi minoritas yang melakukan kesalahan, akan diabaikan.

Untuk menentukan data apa saja yang tertera pada transaksi setiap *block*nya, mengacu pada form C1. Form C1 tersebut dihasilkan oleh tiap TPS. Rancangan *blockchain* menggunakan konsep yang dipublikasikan oleh Anders melalui websitenya sebagaimana dapat dilihat pada Gambar

Block:	#	2
Nonce:	215458	
Coinbase:	\$ 100.00	-> Anders
Tx:	\$ 10.00	From: Anders -> Sophia
	\$ 20.00	From: Anders -> Lucas
	\$ 15.00	From: Anders -> Emily
	\$ 15.00	From: Anders -> Madison
Prev:	0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadd	
Hash:	0000baeab68c2a60f9a6fa56355438d97c672a15494fce8617064d931	

Gambar 6 Tampilan simulasi blockchain (Anders.com)

Untuk *block*, *nonce*, *previous hash*, dan *hash* masih menggunakan format yang sama. Perubahan dan penyesuaian terhadap proses pemilu adalah pada coinbase dan Tx. Coinbase dalam contoh adalah sejumlah uang yang diberikan dan akan ditransaksikan. Hal itu tidak berlaku dalam rancangan sistem *blockchain*.

**IV. DATA PEROLEHAN SUARA PASANGAN CALON PRESIDEN DAN WAKIL PRESIDEN**

NOMOR DAN NAMA PASANGAN CALON	SUARA SAH
01. Ir. H. JOKO WIDODO Prof. Dr.(H.C.) KH. MA'RUF AMIN Dua puluh lima	25
02. H. PRABOWO SUBIANTO H. SANDIAGA SALAHUDDIN UNO Seratus tujuh	107

**V. DATA SUARA SAH DAN TIDAK SAH**

URAIAN	JUMLAH
A. JUMLAH SELURUH SUARA SAH (IV.01 + IV.02) Seratus tiga puluh dua	132
B. JUMLAH SUARA TIDAK SAH empat	4
C. JUMLAH SELURUH SUARA SAH DAN SUARA TIDAK SAH (A + B) Seratus tiga puluh enam	136

DITETAPKAN DI: Sampang, Drien. TANGGAL: 17 BULAN: 04 TAHUN: 2019

**NAMA DAN TANDA TANGAN KELOMPOK PENYELENGGARA PEMUNGUTAN SUARA**

1. KETUA	2. ANGGOTA	3. ANGGOTA	4. ANGGOTA	5. ANGGOTA	6. ANGGOTA	7. ANGGOTA
[Signature]	[Signature]	[Signature]	[Signature]	[Signature]	[Signature]	[Signature]

**NAMA DAN TANDA TANGAN SAKSI PASANGAN CALON PRESIDEN DAN WAKIL PRESIDEN**

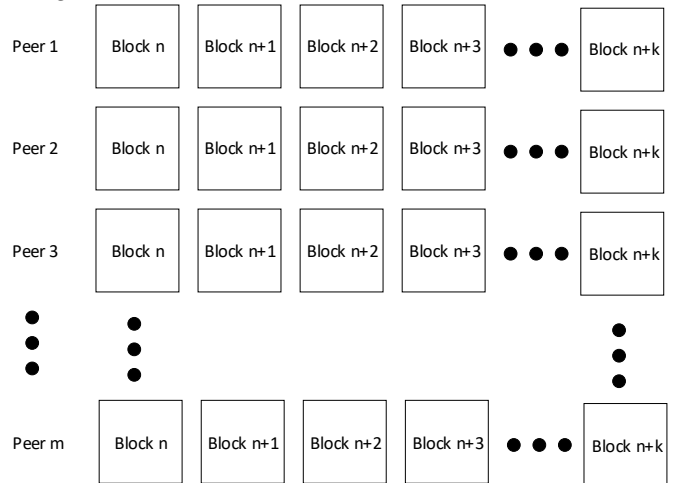
01. Ir. H. JOKO WIDODO - Prof. Dr.(H.C.) KH. MA'RUF AMIN	02. H. PRABOWO SUBIANTO - H. SANDIAGA SALAHUDDIN UNO
[Signature]	[Signature]

Gambar 7 Screenshot berita acara C1

Informasi terpenting dalam proses pencatatan pemilu dari setiap TPS adalah hasil suara. Form C1 memuat dua halaman informasi. Halaman pertama berisikan demografi dari pemilih seperti data pemilih, data pengguna hak pilih dan data penggunaan surat suara sah. Pada data penggunaan surat suara terdapat rincian informasi meliputi jumlah surat suara yang diterima, jumlah surat suara yang dikembalikan, jumlah surat suara yang tidak digunakan, dan jumlah surat suara yang digunakan. Sedangkan pada halaman kedua berisikan data jumlah pemilih setiap calon, jumlah suara sah, jumlah suara tidak sah, dan akumulasi jumlah suara sah dan suara tidak sah. Data terkait TPS ada di kedua halaman, meliputi, nomor TPS, kelurahan, kecamatan, kabupaten/kota, dan provinsi. Dari seluruh informasi tersebut beberapa informasi dipilih untuk masuk ke dalam sistem *blockchain*. Apabila seluruh informasi tersebut dilibatkan dalam *ledger blockchain* akan memberatkan sistem. Maka perlu dipilih informasi terpenting sehingga sistem dapat berjalan secara efisien. Informasi seperti gender dari pemilih, tidak menjadi prioritas untuk dilibatkan ke dalam sistem karena tidak berpengaruh langsung kepada hasil akhir pemilihan.

Beberapa informasi yang dipilih untuk dimasukkan adalah jumlah surat suara yang diterima, jumlah surat suara yang dikembalikan, jumlah surat suara yang tidak digunakan, dan jumlah surat suara yang digunakan, jumlah pemilih setiap calon, jumlah suara sah, jumlah suara tidak sah, dan akumulasi jumlah suara sah dan suara tidak sah, serta identitas dari TPS. Identitas TPS dapat

menggunakan suatu ID number yang spesifik dan unik. Antara kode identitas angka tersebut memiliki nilai yang saling mengunci. Sebagai contoh jumlah seluruh surat suara sah haruslah sama dengan jumlah surat suara yang dipilih untuk masing-masing calon. Kemudian jumlah seluruh surat suara yang digunakan adalah harus sama dengan jumlah dari surat suara sah dan suara tidak sah. Sedangkan jumlah surat suara yang diterima haruslah sama dengan penjumlahan dari surat suara yang digunakan dan surat suara yang tidak digunakan. Fitur tersebut dapat diberikan dalam sistem *blockchain* sehingga membantu *verifikator* dalam melakukan *mining*.



Gambar 8 Ilustrasi proses proses blockchain antara block dan peer

Pada Gambar 8 ditunjukkan suatu ilustrasi dari proses *blockchain*. Block n, block n+1, dan seterusnya membuat sebuah rantai. Block n+1 hanya bisa dilakukan *mining* setelah sudah dilakukan *mining block* sebelumnya. Maka hubungan antara block tersebut membentuk suatu rantai. Di sisi lain secara paralel antara *peer* satu dengan *peer* lainnya melakukan verifikasi data. Bila dari beberapa *peer* terjadi perbedaan data, maka akan diambil informasi dari mayoritas *peer*. Dengan cara tersebut, akan terjaga verifikasi informasi.

Block	1
Nonce	

1	Kode TPS	
2	Jumlah surat suara yang diterima termasuk cadangan 2,5 %	
3	Jumlah surat suara dikembalikan oleh pemilih karena rusak/keliru coblos	
4	Jumlah surat suara yang tidak digunakan	
5	Jumlah surat suara yang digunakan	
6	Jumlah Suara Sah Calon A	
7	Jumlah Suara Sah Calon B	
8	Jumlah Suara Sah Seluruh Calon	
9	Jumlah Suara Tidak Sah	
10	Jumlah Suara Sah dan Tidak Sah	

Prev Hash	
-----------	--

Gambar 9 Rancangan tampilan block untuk setiap TPS

Proses *blockchain* tersebut dapat disimulasikan dalam bentuk Excel sebagai mana terlihat pada Gambar 9. *Cell block* berisikan

nomor dari *block*. *Cell* nomor 1 hingga 10 berisikan informasi yang akan dituangkan dalam *distributed ledger*. *Cell prev* adalah *cell* yang berisikan *hash* dari *block* sebelumnya. Sedangkan *cell hash* berisikan nilai *hash* dari *block* ini. *Nonce* adalah nilai yang akan dicari menggunakan teknik komputasi oleh para *miner*. Para *miner* berlomba-lomba mencari nilai *nonce* yang tepat.

Antara *cell* yang satu dengan *cell* yang lain saling mengunci nilainya, sebagaimana sudah dijelaskan pada paragraph sebelumnya. *Cell 2* harus bernilai sama dengan akumulasi *cell 3,4,5*. *Cell 8* harus memiliki nilai yang sama dengan akumulasi *cell 6 dan 7*. Sedangkan nilai dari *cell 10* harus sama dengan akumulasi dari *cell 8 dan 9*. *Cell 8 dan 5* pun harus memiliki nilai yang sama. Fungsi tersebut dapat ditambahkan dalam sistem sehingga mencegah kesalahan input data.

Block		1	
Nonce			
1	Kode TPS		
2	Jumlah surat suara yang diterima termasuk cadangan 2,5 %	2	
3	Jumlah surat suara dikembalikan oleh pemilih karena rusak/keliru coblos	2	
4	Jumlah surat suara yang tidak digunakan	2	
5	Jumlah surat suara yang digunakan	7	Salah
6	Jumlah Suara Sah Calon A	1	
7	Jumlah Suara Sah Calon B	2	
8	Jumlah Suara Sah Seluruh Calon	3	Benar
9	Jumlah Suara Tidak Sah	6	
10	Jumlah Suara Sah dan Tidak Sah	7	Salah
Prev			
Hash			

Gambar 10 Rancangan tampilan block untuk setiap tps dengan fitur deteksi data salah

Sebagai ilustrasi. *Cell 5* akan memiliki notifikasi salah dikarenakan jumlah surat suara yang digunakan tidak sama dengan akumulasi *cell 2,3, dan 4*. Sedangkan *cell 8* bernilai benar karena sesuai dengan akumulasi dari *cell 6 dan 7*. *Cell 10* memiliki notifikasi “salah” dikarenakan tidak sesuai dengan akumulasi dari *cell 8 dan 9*. Tapi di sisi lain *cell 10* memiliki notifikasi kedua yang benar karena memiliki nilai yang sama dengan *cell 5*.

Block		1	
Nonce			
1	Kode TPS		
2	Jumlah surat suara yang diterima termasuk cadangan 2,5 %	2	
3	Jumlah surat suara dikembalikan oleh pemilih karena rusak/keliru coblos	2	
4	Jumlah surat suara yang tidak digunakan	2	
5	Jumlah surat suara yang digunakan	6	Benar
6	Jumlah Suara Sah Calon A	2	
7	Jumlah Suara Sah Calon B	3	
8	Jumlah Suara Sah Seluruh Calon	5	Benar
9	Jumlah Suara Tidak Sah	1	
10	Jumlah Suara Sah dan Tidak Sah	6	Benar
Prev			
Hash			

Block		1	
Nonce			
1	Kode TPS		
2	Jumlah surat suara yang diterima termasuk cadangan 2,5 %	2	
3	Jumlah surat suara dikembalikan oleh pemilih karena rusak/keliru coblos	2	
4	Jumlah surat suara yang tidak digunakan	2	
5	Jumlah surat suara yang digunakan	6	Benar
6	Jumlah Suara Sah Calon A	2	
7	Jumlah Suara Sah Calon B	3	
8	Jumlah Suara Sah Seluruh Calon	5	Benar
9	Jumlah Suara Tidak Sah	1	
10	Jumlah Suara Sah dan Tidak Sah	6	Benar
Prev			
Hash			

Gambar 11 Rancangan tampilan block untuk setiap tps dengan data yang sudah benar

*Block* tersebut masih salah dan belum bisa diteruskan untuk disambung *block* berikutnya. Entitas dalam sistem perlu melakukan revisi terlebih dahulu untuk lalu *block* ini dapat dianggap benar dan dilakukan mining. Gambar 11 ditunjukkan blok yang sudah benar dan verified diisikan datanya secara matematis. Selain dilakukan verifikasi secara hitungan matematis, perlu dilakukan juga verifikasi dengan membandingkan form C1 aslinya. Bila ternyata informasi yang dingkapkan sudah benar, *miner* dapat melakukan mining dan tercipta *block* baru untuk lalu dilanjutkan dengan rantai *block* berikutnya.



**Referensi**

- [1] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183-187.
- [2] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. *In 2016 2nd International Conference on Open and Big Data (OBD)* (pp. pp. 25-30). IEEE.
- [3] Yuan, Yong, & Wang, F.-Y. (2016). "Towards blockchain-based intelligent transportation systems." . *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE.
- [4] Kshetri, N. (2017). "Can blockchain strengthen the internet of things?". *IT professional* 19.4, 68-72.
- [5] Biswas, Kamanashis, & Muthukkumarasamy, V. (2016). "Securing smart cities using blockchain technology." . *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE.
- [6] Davidson, Sinclair, Filippi, P., & Potts, J. (2016). "Economics of blockchain.". *Available at SSRN 2744751*.
- [7] Osgood, R. (2016). "The future of democracy: Blockchain voting.". *COMPI16: Information Security*.
- [8] Wang, B., Sun, J., He, Y., Pang, D., & Lu, N. (2018). Large-scale election based on blockchain. *Procedia Computer Science*, 129, 234-237.
- [9] Kshetri, N., & Voas, J. (2018). "Blockchain-enabled e-voting.". *IEEE Software* 35.4, 95-99.
- [10] McCorry, Patrick, Shahandashti, S., & Feng Hao. (2017). "A smart contract for boardroom voting with maximum voter privacy.". *International Conference on Financial Cryptography and Data Security*. Cham: Springer.
- [11] Hanifatunnisa, Rifa, & Rahardjo, B. (2017). Blockchain based e-voting recording system design.". *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE.
- [12] Winarno, Agus, Harsari, J., & Ardianto, B. (2018). "Block-Chain Based E-Voting For Indonesia."
- [13] Paul, B. (1964). "On distributed communications." . Retrieved from [www.rand.org: https://www.rand.org/pubs/research\\_memoranda/RM3767.html](https://www.rand.org/pubs/research_memoranda/RM3767.html)