BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

2.1.1. Consolidating Indonesia's Fragile Election Through E-Voting: Lessons Learned from India and Phillipines. [3]

Penelitian ini membahas tentang penting dan mendesaknya kebutuhan akan voting elektronik (e-voting) di Indonesia sejak pemilu serentak pada tahun 2019 yang menyebabkan hilangnya nyawa sebanyak 527 panitia pemilu yang menurut laporan disebabkan oleh kelelahan yang ekstrim saat dan sesudah pemilu berlangsung. Pemilu tersebut membentuk sebuah konsensus dimana sistem pemilu manual sekarang yang menggunakan 5 pemilihan dengan kertas di pilih secara bersamaan harus segera diubah. Adapun kekhawatiran tentang perbedaan waktu yang panjang dari hari pemilihan sampai dengan hari pengumuman hasil pemilu yang memungkinkan adanya kecurangan saat penghitungan. Hal ini diperkuat karena banyaknya gugatan terkait pemilu ke Mahkamah Konstitusi yang menuduh kandidat lainnya saling melakukan kecurangan. Penelitian ini meneliti apakah e-voting dapat menjadi solusi dalam mengatasi isu dari voting konvensional seperti mempercepat proses penghitungan, mengurangi biaya serta meningkatkan kehadiran pemilih..

Berdasarkan penelitian ini, E-voting dapat meningkatkan akurasi dari voting karena pada voting konvensional ada faktor jika kertas rusak/tidak valid, e-voting juga mengurangi waktu yang dibutuhkan untuk melakukan voting dan lebih mudah untuk digunakan, lalu e-voting juga lebih transparan karena hasil vote dapat langsung diketahui setelah melakukan voting serta dapat memangkas biaya. E-voting dapat menjadi solusi jangka Panjang untuk menggantikan voting konvensional jika diterapkan dan di implementasikan dengan benar dan tepat. Namun untuk memaksimalkan e-voting ini dibutuhkan

sosialisasi dan peningkatan literasi tentang teknologi agar masyarakat dapat memahaminya dengan baik.

Poin yang dapat diambil dari penelitian ini adalah :

- Adanya kebutuhan beralih ke proses e-voting karena pemilu tradisional Indonesia pada tahun 2019 memakan sebanyak 527 korban jiwa yang diakibatkan kelelahan ekstrim
- Diperlukannya waktu untuk menghitung suara secara menual dapat menumbulkan kecurangan saat penghitungan
- Penelitian ini juga menjelaskan kelebihan e-voting dibandingkan voting tradisional

2.1.2. Conventional VS Blockchain-Based E-Vote System [4]

Pada penelitian ini dijelaskan tentang perbedaan dari berbagai aspek aspek yang ada dalam pemungutan suara konvensional (memakai kertas), *e-voting* konvensional dan *e-voting* berbasis *blockchain*. Setiap metode pemungutan suara mempunyai kelebihan dan kekurangan masing-masing. Pada penelitian ini juga dijelaskan proses-proses/tahapan pemungutan suara, cara kerja serta kritik dari ketiga metode tersebut. Untuk metode konvensional, metode ini sangat memakan banyak waktu untuk dilakukan dan dibutuhkan tenaga ekstra dan keamanan ekstra dalam pelaksanaanya agar berjalan lancer dan tidak menjamin privasi dari data pemilih. Untuk *e-voting* konvensional, pemilih di verifikasi oleh admin sistem dan memvoting dengan sidik jari atau memilih nama kandidat pada mesin voting dan hasil voting terhitung secara otomatis oleh sistem, kelemahan nya adalah karena basis data (*database*) yang digunakan tersentralisasi, sistem tersebut dapat diubah / di hack oleh pihak yang tidak bertanggung jawab. Lalu ada *E-voting* berbasis blockchain dimana basis data diubah menjadi ledger. Adapun 3 pilar yaitu tidak bisa diubah, transparan dan verifiabilitas dan berdasarkan 3 pilar tersebut, kelemahan dari sistem *e-voting* dapat di selesaikan dengan teknologi *blockchain* karena dibutuhkan konsensus 51% untuk dapat menghack sistem.

Poin yang dapat diambil dari penelitian ini adalah :

- Dijelaskan perbandingan antara metode voting konvensional, evoting dan evoting dengan *blockchain* dari beberapa aspek seperti *time consuming*, efisiensi, akurasi, dan lain lain.
- Penelitian ini menjelaskan karakteristik dari masing-masing metode voting dan mengapa *blockchain* dapat menyelesaikan masalah dari e-voting konvensional karena memiliki 3 pilar yaitu *immutability*, *transparency* dan *verifiability*.

2.1.3. Toward Secure E-Voting Using Ethereum Blockchain [5]

Smart contract merupakan suatu alat yang *powerful* untuk mendigitalisasikan servis servis yang ada di kehidupan sehari hari. *Smart contract* ini dapat diluncurkan (*deploy*) ke *blockchain* dan di eksekusi. *Blockchain* dengan *smart contract* muncul sebagai kandidat untuk mengembangkan e-voting yang lebih murah, aman, transparan dan lebih mudah digunakan. Ethereum merupakan jaringan yang paling cocok digunakan untuk mengembangkan e-voting karena konsitensinya, banyak dipakai dan menyediakan provisi untuk logika *smart contract*. Sebuah sistem e-voting harus aman, artinya sistem e-voting tidak memperbolehkan adanya voting yang duplikat dan harus transparan serta harus melindungi privasi dari pemilih.

Pada penelitian ini, dibuat sebuah sampel aplikasi e-voting sebagai *smart contract* dalam *blockchain* Ethereum dengan menggunakan dompet Ethereum dan Bahasa pemograman Solidity. Setelah eleksi diadakan , *blockchain* Ethereum akan menyimpan semua rekaman dari hasil voting yang telah dilakukan pemilih.

Dengan membuat *smart contract* sesuai dengan spesifikasi yang ada di penelitian, penelitian ini berhasil mengimplementasikan *blockchain* ke dalam e-voting. Penelitian ini juga membahas beberapa isu mendasar yang dimiliki oleh e-voting konvensional. Hasil yang didapat dari percobaan pada penelitian ini, konsep *blockchain* dan metodelogi keamanan seperti rantai *hash*

yang tidak bisa diubah, menjadi dapat beradaptasi ke eleksi dan poll. Pada titik ini, Ethereum dan *smart contract* yang menjadi salah satu terobosan yang revolusioner setelah *blockchain* itu sendiri membantu untuk memutarbalikan persepsi yang terbatas tentang *blockchain* sebagai *cryptocurrency* saja, tetapi *blockchain* dapat digunakan untuk menjadi solusi dari berbagai isu yang berkaitan dengan Internet di dunia modern.

Poin yang dapat diambil pada penelitian ini adalah :

- Penelitian ini menjelaskan pembuatan *smart contract* voting pada *blockchain* Ethereum karena Ethereum memiliki *use case* yang luas.
- Penelitian menggunakan skala kecil dan ditampilkan waktu yang dibutuhkan untuk melakukan *deployment* dan voting

2.1.4. Implementasi Blockchain dalam Aplikasi Pemilu [6]

Pemilu merupakan kegiatan demokrasi di Indonesia yang dilaksanakan setiap lima tahun sekali untuk memilih pemimpin – pemimpin, tetapi pemilu masih manual dalam segi perhitungan dan pelaksanaan sehingga hasilnya dapat bocor dan menimbulkan masalah keamanan terhadap data pemilu. Penelitian ini membahas tentang penggunaan teknologi *blockchain* untuk aplikasi pemilu yang dapat memberikan keamanan terhadap data hasil pemilu yang tersimpan di *blockchain*. Penelitian ini menggunakan Jaringan Ethereum yang dibuat local menggunakan ganache, sebuah alat untuk membuat *blockchain* ethereum secara lokal dan Bahasa pemograman Solidity untuk membuat *smart contract*.

Poin yang didapat dari penelitian ini adalah :

- Dibuat sebuah aplikasi voting berbasis *blockchain*

- Penelitian ini menunjukan jika *blockchain* dapat mengatasi permasalahan e-voting karena memiliki sifat yang *immutable*, *transparent* dan *decentralized*.

2.1.5. Performance and Cost Evaluation of Smart Contracts in Collaborative Health Care Environment [7]

Penelitian ini membahas tentang penerapan *blockchain* kedalam aplikasi Kesehatan dimana dibuat *smart contract* lalu kemudian dilakukan *deployment* ke 2 tipe *blockchain* yaitu Ropsten testnet dan *private blockchain*. Setelah itu, performa dari *smart contract* pada kedua *blockchain* tersebut di bahas pada penelitian ini serta membahas tentang biaya yang diperlukan dalam implementasi

Hal yang didapatkan pada penelitian ini adalah, penelitian ini menganalisa biaya yang diperlukan untuk menjalankan *smart contract* pada *public blockchain* serta waktu yang dibutuhkan untuk mengeksekusi fungsi pada *smart contract* tersebut. Hal yang dibandingkan meliputi waktu transaksi, biaya yang dibutuhkan dari segi *deployment* serta infrastruktur serta performa dan biaya dalam beberapa skenario pemakaian aplikasi tersebut.

Poin penting pada penelitian ini adalah

- Penelitian ini membuat aplikasi Kesehatan berbasis *blockchain* yang kemudian di *deploy* ke *public* dan *private blockchain*
- Penelitian ini membandingkan performa dari *smart contract* tersebut pada kedua *blockchain*tersebut dan membandingkan biaya yang diperlukan

2.2 Tinjauan Teori

2.2.1 Voting

Voting merupakan fondasi utama dari sistem demokrasi. Menurut KBBI, voting merupakan pemungutan suara karena tidak tercapai kata mufakat [8]. Metode voting dapat dibagi 2 yaitu tradisional dan e-voting. Metode voting

tradisional menggunakan kertas dan pemilih mencoblos kertas tersebut dan dimasukan ke dalam kotak. Di Indonesia, masih diterapkan voting tradisional memakai kertas dan voting ini berjenis *majority vote* dimana suara kandidat yang mencapai lebih dari 50% dapat dinyatakan sebagai pemenang.

2.2.2 E-Voting

Selain voting adapula E-Voting atau *electronic voting*. E-voting adalah proses pemilihan umum yang memungkinkan pemilih untuk mencatatkan pilihannya yang bersifat rahasia secara elektronik dan teramankan [9]. Pengertian lain e-voting adalah pemungutan suara yang dilakukan secara elektronik (digital) mulai dari psoses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara dan pengiriman hasil suara(6). Kelebihan utama E-voting dibanding voting tradisional adalah meningkatkan efisiensi, menghemat tenaga dan mempercepat proses pemilihan secara keseluruhan.

2.2.3 **E-KTP**

KTP (Kartu Tanda Penduduk) merupakan kartu yang berfungsi sebagai bukti diri yang diterbitkan oleh pemerintah dan merupakan identitas resmi seorang penduduk bahwa penduduk tersebut merupakan Warga Negara Indonesia ataupun Warga Negara Asing yang memiliki Izin Tinggal Tetap , KTP ini berlaku di seluruh Indonesia. Setiap individu yang berusia 17 tahun akan mendapatkan KTP. Pada tahun 2009, pemerintah meluncurkan E-KTP dimana data KTP disimpan secara elektronik / digital/ E-KTP memiliki masa berlaku seumur hidup sehingga masyarakat tidak perlu memperbarui KTP lagi dan individu hanya memiliki 1 KTP saja. E-KTP memiliki beberapa manfaat yaitu mengamankan korupsi, tidak dapat dipalsukan dan diduplikasi/digandakan serta karena menggunakan RFID chip, dapat digunakan sebagai *smart card* untuk beberapa aplikasi seperti e-voting [10].

2.2.4 ***Website***

Website atau situs web merupakan fasilitas internet yang menghubungkan dokumen dalam lingkup local maupun jarak jauh. Dokumen dalam *website*

disebut dengan *webpage* dan *link* dalam *website* dapat digunakan oleh pengguna untuk beralih dari satu halaman ke halaman lain (*hypertext*) baik antar halaman yang disimpan di server yang sama maupun dalam server yang ada di seluruh dunia. Halaman dapat diakses atau dibaca melalui *browser* seperti Google Chrome, Mozilla Firefox dan lain sebagainya [11] . Fondasi dari website adalah HTML, CSS dan juga Javascript dimana setiap *browser web* mempunyai sebuah *browser engine* yang berfungsi untuk mengubah hal tersebut menjadi sebuah *web page* yang berfungsi.

2.2.5 *Blockchain*

Blockchain merupakan sebuah *database* terdistribusi dari rekaman (*records*) atau buku besar (*ledger*) publik dari semua transaksi atau acara digital yang telah dieksekusi dan dibagikan ke partisipan – partisipan yang terlibat [12]. Setiap transaksi pada *Blockchain* di verifikasi dengan menggunakan konsensus (kesepakatan Bersama) dari mayoritas pihak yang berpartisipasi. Setiap informasi pada *blockchain* bersifat *immutable* yang artinya tidak bisa diubah/dihapus. Blockchain terdiri dari transaksi – transaksi yang telah diverifikasi yang telah dilakukan dalam sistem yang menggunakan *blockchain*. *Blockchain* digunakan dalam mata uang digital (*cryptocurrency*) seperti Bitcoin , Bnb, Ether dan banyak lainnya. Selain itu *blockchain* bersifat *decentralized* yang artinya proses verifikasi *record* dibagi kedalam banyak entitas-entitas yang ada pada *blockchain* tersebut sehingga untuk memanipulasi *record* yang masuk diperlukan 1 entitas menguasai mayoritas >50% dari suatu *blockchain* yang merupakan suatu hal yang hampir mustahil dilakukan sehingga *blockchain* cocok digunakan untuk menampung data-data yang mudah dimanipulasi jika disimpan pada *database* konvensional.

2.2.6 *Proof of Stake*

Setiap *blockchain* memiliki suatu mekanisme yaitu konsensus. Konsensus merupakan suatu cara untuk mencapai kesepakatan Bersama diantara jaringan *nodes* atau sistem [13]. Ada macam macam jenis konsensus diantaranya adalah *Proof of Stake* (PoS). *Proof of Stake* ini merupakan mekanisme yang memungkinkan untuk mencapai konsensus dengan membuktikan kepemilikan

dari *stake*. Jaringan PoS pertama merupakan Peercoin yang dikembangkan sebagai mekanisme konsensus PoX yang bertujuan untuk mengurangi syarat komputasi dari *Proof of Work* (PoW). PoS memilih *block leader* berdasarkan jumlah *stake* yang mereka pegang dimana semakin banyak kepemilikan, semakin besar kesempatan terpilih [14] .

2.2.7 Ethereum

Ethereum merupakan teknologi yang digunakan untuk membuat suatu aplikasi,organisasi, transaksi dan komunikasi tanpa di control oleh autoritas sentral. Ethereum bersifat *decentralized* yaitu tidak dikontrol satu entitas namun berdasarkan partisipan dalam network Ethereum tersebut. Ethereum menggunakan *nodes* (komputer dengan Salinan data *blockchain* Ethereum) yang dijalankan oleh relawan / partisipan untuk merepliksasi *server* individual dan sistem cloud. *Nodes* ini dijalankan oleh individu / bisnis di seluruh dunia dan menyediakan resilensi atau ketahanan ke jaringan infrastruktur Ethereum [15] .

Ethereum dibuat sebagai protocol alternatif untuk membuat aplikasi terdesentralisasi (dApp). Ethereum dibuat dengan sebagai *blockchain* dengan Bahasa pemograman sendiri yaitu Solidity yang memungkinkan pengembang untuk menulis aturan aturan pada dApp yang dibuat. Ethereum dapat digunakan untuk membuat dApps seperti *smart contract* dan *cryptocurrency*. Ethereum menggunakan *Proof of Stake* sebagai mekanisme konsensus sejak 2022 dimana sebelumnya Ethereum menggunakan *Proof of Work.* Ethereum mempunyai *cryptocurrency* sendiri yaitu Ether dimana Ether ini dapat digunakan sebagai mata uang di jaringan ethereum [15].

Ethereum dipakai pada penelitian ini karena mudah untuk mengimplementasikan *smart contract* kedalam *blockchain* Ethereum dan memiliki Bahasa pemograman khusus untuk membuat *smart contract* yaitu solidity dan memiliki IDE (*Integrated Development Environment*) bernama Remix yang memudahkan untuk membuat , testing dan *deploy smart contract* ke *blockchain*

2.2.8 *Smart Contract*

Salah satu aplikasi dari *blockchain* merupakan *smart contract* (kontrak pintar). *Smart Contract* merupakan sebuah program yang berisikan fungsi-fungsi yang disimpan dalam blockchain dan dijalankan saat suatu kondisi terpenuhi dan dapat menjalankan fungsi-fungsi yang ada didalamnya. *Smart contract* digunakan untuk mengautomasi eksekusi dari sebuah persetujuan sehingga partisipan-partisipan yang ada dapat memastikan hasil nya. Membuat *smart contract* yang bisa mengeksekusi dirinya sendiri dalam *blockchain* dilakukan dengan cara menulis kode dimana kita dapat mendefinisikan *rules* (aturan), objek, model data dan kontrak dapat mulai dieksekusi [16].

Setelah *smart contract* dikerahkan pada *blockchain*, kontrak tersebut tidak dapat dihapus dari *blockchain* dan semua orang dapat melihat hasil dari eksekusi *smart contract*. *Smart contract* dalam Ethereum dibuat menggunakan bahasa pemograman Solidity yang di kompilasi menjadi file .sol yang dapat di *deploy* ke *blockchain* untuk digunakan.

2.2.9 Solidity

Solidity merupakan Bahasa pemograman berorientasi objek, dan *high-level* untuk mengimplementasikan *smart contract* . Solidity didesain untuk menargetkan Ethereum Virtual Machine (EVM) dan dipengaruhi oleh bahasa pemograman seperti C++, Python dan Javascript. Solidity bersifat *statically typed* , mendukung *inheritance* , *library* dan *user-defined types*. Dengan menggunakan Solidity, programmer dapat membuat *smart contract* yang biasanya digunakan untuk melakukan voting, penggalangan dana, dan lelang buta [17].

2.2.10 MYSQL

MySQL merupakan *relational database management system* (RDBMS) yang paling banyak digunakan, bersifat sumber terbuka dan dikembangkan di Swedia pada tahun 1995 dan sekarang dimiliki oleh Oracle. MySQL digunakan Ketika memiliki data-data yang memiliki relasi terhadap satu sama lain seperti *one to many , one to one* dan *many to many* [18].

2.2.11 ExpressJS

Express merupakan sebuah *framework* untuk membangun aplikasi *server side* / backend NodeJS yang efisien dan *scalable* . NestJS menggunakan Bahasa pemograman Javascript dan menggunakan desain unoppiniated dimana *framework* ini tidak memaksakan cara *developer* membuat programnya dan merupakan salah satu *framework* NodeJS paling popular [19]. Alasan penulis menggunakan NestJS adalah:

- Familiar dengan *framework* ini sehingga memudahkan proses pengembangan
- Simpel, ringan dan cepat
- Memiliki dokumentasi lengkap

2.2.12 React

React merupakan *library* berbasis react yang ringan dan fleksibel dan dapat membuat aplikasi web yang cepat [20]. React merupakan *library* bukan *framework* yang artinya fitur tambahan React harus di install secara manual, hal ini membuat React fleksibel, simple dan ringan karena hanya menginstall fitur yang diperlukan saja:

- *Framework* ini memiliki dokumentasi yang lengkap sehingga dengan mudah mencari solusi jika ada permasalahan dalam membuat frontend
- Mudah mengintegrasikan ke *backend.*
- Simpel dan ringan

2.2.13 RFID

RFID (Radio Frequenct Identification) merupakan suatu terminology untuk teknologi yang menggunakan gelombang radio untuk secara otomatis mengidentifikasi orang ataupun objek dari jarak beberapa inci ke beberapa meter [21]. E-KTP menggunakan teknologi RFID sebagai chip *embedded* sehingga E-KTP bisa di scan menggunakan RFID *scanner* untuk mendapatkan RFID ID yang terkandung didalamnya, RFID ID bersifat unik.

2.2.14 *Proof of Authority*

Proof of Authority (PoA) atau *Proof of Stake Authority* merupakan turunan dari Proof of Stake. *Proof of Authority* dalam Ethereum ini digunakan sebagai solusi atas permasalahan Ropsten Testnet dimana testnet yang menggunakan *Proof of Work* tidak aman karena sangat rentan terhadap 51% attack karena power dari network yang kecil sehingga mudah diserang [22]. *Proof of Authority* bekerja mirip seperti *proof of stake,* namun untuk mengvalidasi blok, alih alih menggunakan ether untuk melakukan stake, PoA menggunakan identitas dalam staking jadi validator mempertaruhkan identitas mereka dimana hanya validator yang terpercaya saja dapat melakukan *signing* pada blok. Walaupun lebih tersentralisasi, PoA termasuk transparan dan aman karena Ketika blok dibat, identitas dari *signer* dapat dibandingkan dengan validator yang ada, jika cocok maka blok tersebut valid. *Proof of Authority* ini juga memiliki konstrain yaitu blok baru hanya akan terbuat jika jumlah node aktif N/2+1 dengan minimal 2 node aktif. Contoh ada 5 Node yang menjadi validator, blok baru hanya akan dibuat jika 3 node melakukan *signing* blok tersebut (5/2+1 = 3 dibulatkan ke bawah), jika hanya 2 node online maka blok baru tidak akan dibuat dan transaksi akan gagal masuk ke dalam *blockchain*

2.2.15 Geth

Geth / go-ethereum merupakan implementasi ethereum yang ditulis dengan Bahasa golang, Geth juga merupakan client eksekusi ethereum yang dimana Geth dapat melakukan transaksi, *deployment* serta eksekusi dari *smart contract* dan sudah menyediakan EVM (Ethereum Virtual Machine) didalamnya [23]. Geth dapat menggunakan 2 konsensus yaitu Ethash (*deprecated*) dan Clique dimana Ethash menggunaakn *proof of work* dan Clique menggunakan *Proof of Authority*.