Aplikasi Voting Online dengan Menggunakan Teknologi Blockchain

Ahmad Fajar Prasetiyo
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
me@ahmadfajar.com

Dr. Ir. Rinaldi Munir, M.T.
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
rinaldi@informatika.org

***Abstract*—Perkembangan teknologi banyak mengubah sistem yang telah ada. Salah satu contoh yang berubah adalah voting. Voting sekarang bisa menggunakan sistem teknologi informasi yang sekarang disebut *e-voting*. Beberapa orang telah membuat penelitian tentang *e-voting*. Dari beberapa penelitian telah menghasilkan beberapa standarisasi. Selain itu juga sudah terdapat beberapa produk dan sistem tentang *e-voting*. Salah satu contoh teknologi e-voting yang lain adalah Polys. Polys menggunakan teknologi yang sedang populer saat ini yaitu teknologi Blockchain.**

Keywords—Blockchain, Paillier, e-voting, Enkripsi Homomorfik Parsial.

I. Pendahuluan

Teknologi informasi berkembang dengan sangat cepat pada zaman sekarang. Salah satu penyebab perkembangan teknologi yang sangat cepat adalah internet. Dengan adanya internet arus pertukaran informasi bergerak dengan sangat cepat.

Pesatnya perkembangan teknologi menyebabkan banyak sistem yang berubah. Salah satu contoh yang berubah adalah voting. Dahulu orang voting menggunakan kertas dan dihitung secara manual, sekarang orang voting bisa menggunakan media elektronik. Voting dengan menggunakan media elektronik disebut dengan *e-voting*.

Beberapa negara telah menerapkan *e-voting*. Negara yang telah menerapkan sistem *e-voting* yaitu Estonia dan Norwegia. Dua negara ini menerapkan sistem *e-voting* tetapi menggunakan sistem yang berbeda. Hal ini disebabkan oleh perbedaan antara kedua negara tersebut.

Negara Norwegia menggunakan komputer yang terhubung ke jaringan internet[1]. Setiap orang yang akan melakukan voting harus mempunyai kode unik. Kode unik yang digunakan untuk voting dikirim oleh pemerintah melalui SMS atau menggunakan surat pos. Metode ini cocok untuk negara Norwegia karena menggunakan SMS dan surat pos untuk melakukan komunikasi jauh lebih aman jika dibandingkan dengan menggunakan internet[1].

Sistem *e-voting* yang diterapkan di Negara Estonia berbeda dengan sistem *e-voting* yang diterapkan di Negara Norwegia. Negara Estonia menggunakan ID-card untuk melakukan *e-voting*[2]. ID-card ini tidak hanya digunakan untuk e-voting saja tetapi juga digunakan untuk melakukan tanda tangan digital (*digital signature*). ID-card ini mampu melakukan operasi kriptografi dasar seperti menghasilkan bilangan random, melakukan verifikasi, melakukan operasi matematika dasar. Biaya untuk membuat ID-card cukup mahal sekitar 25 euro.

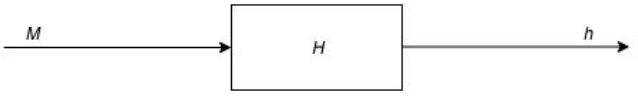
Banyak orang mencoba untuk melakukan riset tentang *e-voting* sehingga muncul teknologi *e-voting* yang baru. Salah satu contoh teknologi *e-voting* yang lain adalah Polys[3]. Polys menggunakan teknologi yang sedang populer saat ini yaitu teknologi Blockchain.

II. Dasar Teori

Pada bab ini akan dibahas teori-teori yang mendukung perancangan aplikasi voting online dengan menggunakan teknologi Blockchain.

A. Fungsi Hash

Fungsi *hash* (H) adalah sebuah fungsi matematika yang memiliki input string yang memiliki panjang bervariasi yang disebut *pre-image* (M) dan menghasilkan sebuah string yang memiliki panjang tetap yang disebut *hash value* (*h*)[4]. Fungsi *hash* banyak digunakan dalam berbagai protokol kriptografi.



Gambar 1 Fungsi *hash*

Fungsi *hash* merupakan fungsi satu arah. Fungsi satu arah adalah fungsi yang mudah untuk menghitung *hash value* dari *pre-image* tetapi sulit bahkan tidak mungkin untuk menghasilkan *pre-image* dari *hash value*.

Fungsi *hash* yang baik adalah fungsi *hash* yang memiliki karakteristik *collision free*. *Collision free* dalam fungsi *hash* adalah sulit untuk menemukan dua *pre-image* yang berbeda tetapi menghasilkan *hash* value yang sama.

B. Algoritma Enkripsi Paillier

Algoritma enkripsi pailier sering digunakan dalam e-voting [5]. Algoritma enkripsi pailier mendukung pertambahan dalam data yang terenkripsi (*chipertext*).

Berikut adalah cara membangkitkan kunci untuk skema enkripsi Pailier[6]:

1. Pilih dua buah bilangan prima yang besar yang memenuhi:
$$fpb\,(pq,\ (p-1)(q-1)) = 1$$
2. Hitung
$$n = pq \quad (1)$$
dan
$$\lambda = kpk(p-1,\ q-1) \quad (2)$$
3. Pilih sebuah bilangan *g* yang memenuhi
$$g \in Z^*_{n^2}$$
4. Definisikan fungsi *L*
$$L(u) = \frac{u-1}{n} \quad (3)$$
5. Hitung
$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n \quad (4)$$

Sehingga didapatkan pasangan kunci publik (n, g) dan pasangan kunci privat (λ, μ)

Berikut adalah cara melakukan enkripsi dengan menggunakan skema enkripsi pailier[6]:

1. Misal pesan adalah *m*
$$m \in Z_n$$
2. Pilih bilangan acak *r* yang memenuhi
$$r \in Z^*_n$$
3. Hitung *chipertext* (*c*)
$$c = g^m . r^n \bmod n^2 \quad (5)$$

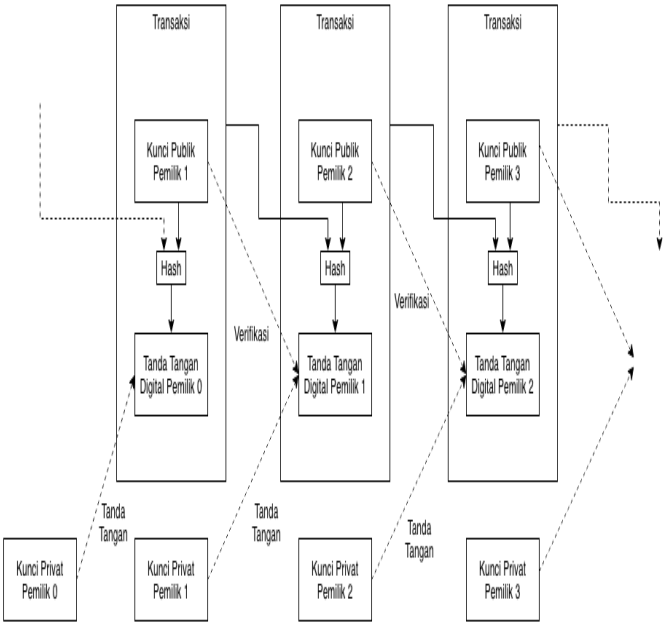
Berikut adalah cara melakukan dekripsi dengan menggunakan skema enkripsi pailier[6]:

1. Untuk melakukan dekripsi dengan *c* yang memenuhi
$$c \in Z^*_{n^2}$$
2. Untuk menghitung pesan asli *m*
$$m = L(c^{\lambda} \bmod n^2) . \mu \bmod n^2 \quad (6)$$

C. Blockchain

Blockchain pertama kali diperkenalkan oleh Satoshi Nakamoto pada paper yang berjudul "*Bitcoin: A Peer-to-Peer Electronic Cash System*" pada tahun 2008. Pada paper itu dijelaskan cara membuat sistem keuangan yang dapat melakukan transfer tanpa menggunakan pihak ketiga (*third trusted party*), jadi seperti kita mempunyai uang secara fisik.

Transaksi adalah sebuah aktivitas pemindahan saldo dari satu orang ke orang yang lain. Transaksi merupakan elemen dari Blockchain, transaksi memungkinkan orang bisa mengirim uang. Proses transaksi digambarkan pada Gambar 2. Misal pemilik 2 mau mengirim uang ke pemilik 3. Pertama yang dilakukan adalah melihat transaksi sebelumnya yaitu transaksi antara pemilik 1 ke pemilik 2. Kepemilikan uang pemilik 2 bisa diketahui dari kunci publik pemilik 2 yang telah dilakukan hash bersama dengan transaksi pemilik 1. Transaksi pemilik 1 ke pemilik 2 akan valid jika ada digital signature dari pemilik 1. Semua orang bisa mengetahui bahwa itu adalah tanda tangan digital dari pemilik 1 dengan cara melakukan dekripsi pada transaksi dengan menggunakan kunci publik pemilik 1. Jika semua orang bisa melakukan verifikasi transaksi antara pemilik 1 ke pemilik 2, maka semua orang juga bisa menentukan saldo dari pemilik 2. Ketika saldo dari pemilik 2 diketahui, maka semua orang bisa menentukan bisa atau tidak pemilik 2 mentransfer uang ke pemilik 3.



Gambar 2 Transaksi dari Blockchain
(Sumber: *Bitcoin: A Peer-to-Peer Electronic Cash System*(2008) oleh Satoshi Nakamoto)

D. Raft Consensus

Konsensus merupakan salah satu cara untuk menangani masalah *fault-tolerant* pada sistem terdistribusi. Banyak konsensus yang berdasarkan sistem dari Konsensus Paxos (Ongaro, 2014). Tetapi Paxos sangat sulit untuk dimengerti.

Paxos sangat sulit untuk dimengerti bahkan sangat sulit untuk diimplementasikan, oleh karena itu banyak orang yang membuat algoritma konsensus baru yang lebih dimengerti. Salah satu algoritma yang terkenal adalah algoritma *raft*. Dilakukan penelitian dari 43 mahasiswa dari dua universitas mempelajari algoritma Paxos dan *raft*. Hasil dari penelitian tersebut 33 mahasiswa berhasil menjawab lebih baik tentang algoritma *raft* dari pada Paxos.

Raft lebih mudah diimplementasikan dan dimengerti dari pada Paxos tetapi juga memiliki fitur yang cukup untuk sistem terdistribusi. Fitur - fitur utama *raft* yaitu *strong leader, leader election,* dan *membership change*. *Raft* memiliki fitur *strong leader* karena log hanya akan berjalan dari *leader* ke server yang lain. *Leader election* dalam *raft* menggunakan waktu acak yang berbeda setiap node sehingga tidak terjadi *split vote*. Fitur *membership change* memungkinkan *raft* untuk menambah node ke dalam konsensus.

E. Requirement pada E-voting

Ada beberapa aspek yang harus dipenuhi agar *e-voting* dapat berjalan dengan baik. Menurut Schneier (1996) ada tujuh aspek dasar yang harus dipenuhi dalam *e-voting*, yaitu:

1. Hanya orang yang terdaftar yang bisa memilih
2. Tidak ada yang bisa memilih lebih dari satu kali
3. Tidak ada yang dapat tahu pilihan orang lain
4. Tidak ada yang bisa menduplikasi hasil pemilihan orang
5. Tidak ada yang bisa mengubah pilihan orang lain tanpa diketahui
6. Setiap pemilih harus yakin kalau pilihannya masuk dalam perhitungan
7. Setiap orang bisa mengetahui hasil pemilihan

Dari tujuh aspek diatas aspek yang nomor empat adalah aspek yang sangat sulit untuk dipenuhi. Kalau dalam kriptografi aspek nomor empat terjadi jika terdapat *replay attack*.

III. Rancangan Solusi

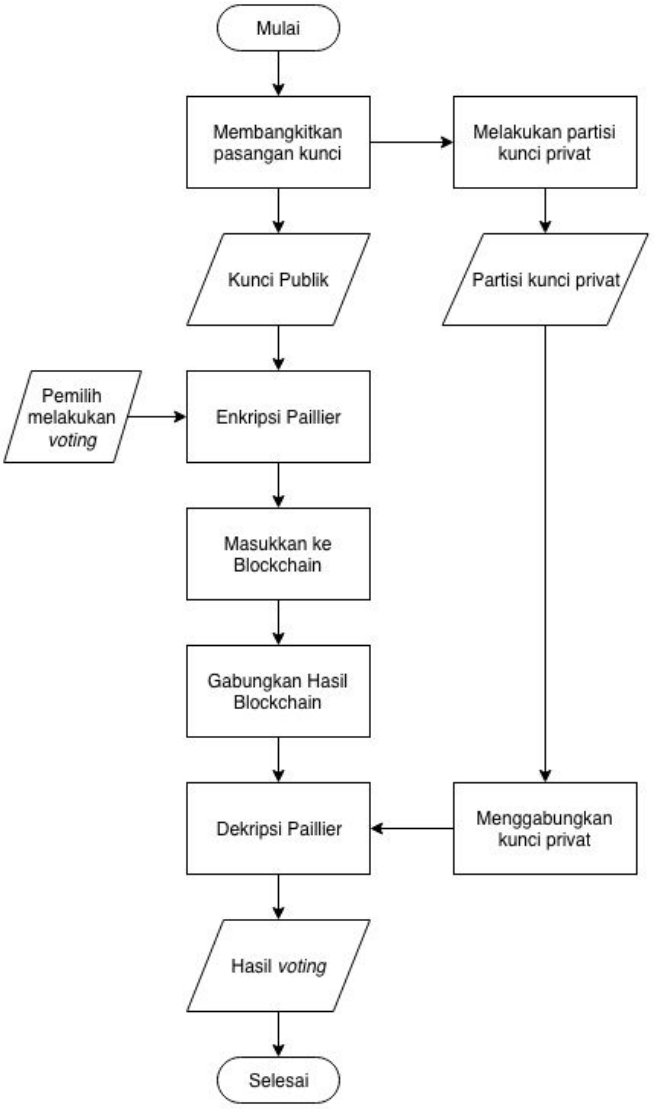
Pada bab ini akan dibahas secara detail rancangan dari aplikasi voting online dengan menggunakan teknologi Blockchain.

A. Alur e-voting

Pada bab ini akan dijelaskan alur dari *e-voting*. Gambar 3 menjelaskan alur dari *e-voting* yang dirancang. Pertama yang dilakukan adalah dengan membangkitkan pasangan kunci publik dan kunci privat. Setelah itu kunci privat dilakukan partisi dan disebar ke seluruh *stakeholder*. Hal ini dilakukan agar tidak ada yang bisa melakukan dekripsi sendiri. Setelah itu kita umumkan kunci publik untuk digunakan melakukan enkripsi saat melakukan *voting*.

Pada saat peserta *voting* melakukan *voting* dilakukan enkripsi homomorfik dengan menggunakan algoritma pailier menggunakan kunci publik yang telah dibangkitkan di awal. Setelah *voting* masuk kedalam Blockchain.

Blockchain dibagi menjadi beberapa daerah. Blockchain bertugas untuk mengumpulkan suara setiap daerah. Setelah *voting* selesai semua hasil Blockchain dikumpulkan menjadi satu.



Gambar 3 Alur dari *e-voting*

Hasil dari Blockchain tidak dapat diganti karena masih dalam bentuk *chipertext*. Hasil dari Blockchain bisa digabungkan atau dilakukan penambahan karena menggunakan enkripsi homomorfik parsial dengan menggunakan algoritma pailier.

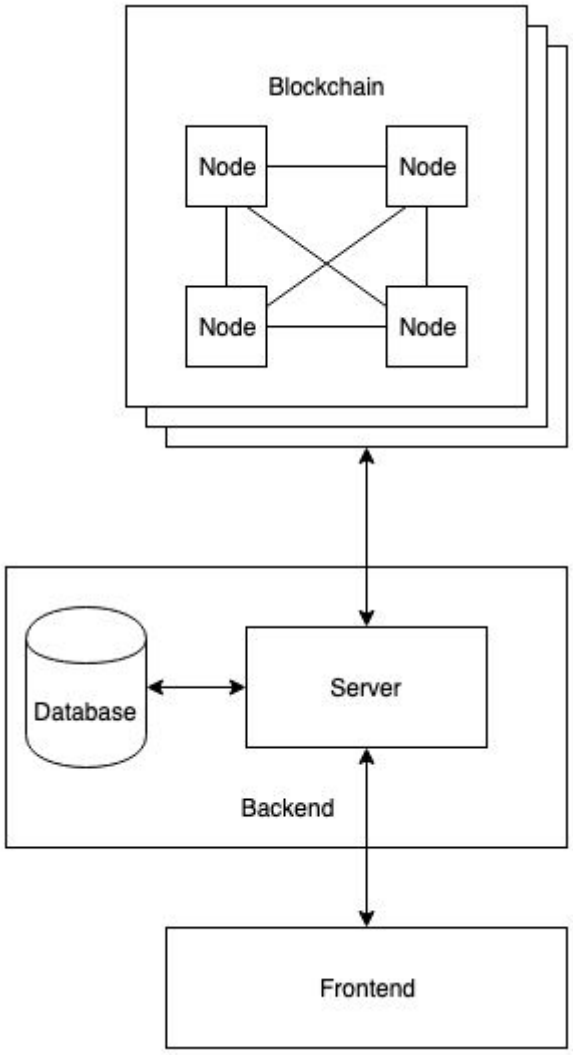
Setelah semua hasil dari Blockchain terkumpul dilakukan dekripsi untuk mengetahui hasil dari *voting*. Dekripsi dilakukan dengan menggabungkan semua kunci privat yang telah disebar ke *stakeholder*.

B. Arsitektur Blockchain dalam E-voting

Sistem arsitektur *e-voting* yang dirancang terdiri dari beberapa Blockchain. Setiap pemilih akan teregistrasi ke dalam satu Blockchain. Jadi pemilih hanya akan bisa melakukan pemilihan pada Blockchain tempat dia teregistrasi.

Blockchain ini bisa diakses lewat internet sehingga orang tidak perlu pergi ke TPS untuk melakukan pemungutan suara. Untuk melakukan pemungutan suara pemilih hanya perlu memasukkan kunci privat yang diberikan.

Sistem arsitektur ini terdiri tiga bagian utama yaitu Blockchain, *backend* dan *frontend*. *Backend* disini berperan sebagai jembatan antara Blockchain dan *frontend*.



Gambar 4 Arsitektur Blockchain dalam *e-voting*

Backend terdiri atas dua komponen yaitu database dan server. Database disini digunakan untuk menyimpan kunci publik semua yang terdaftar dalam Blockchain. Kegunaan dari menyimpan kunci publik ini untuk mengetahui kunci publik ini terdaftar pada Blockchain yang mana. Jadi *backend* disini fungsi utamanya adalah melakukan pemetaan kunci publik yang terdaftar dalam Blockchain.

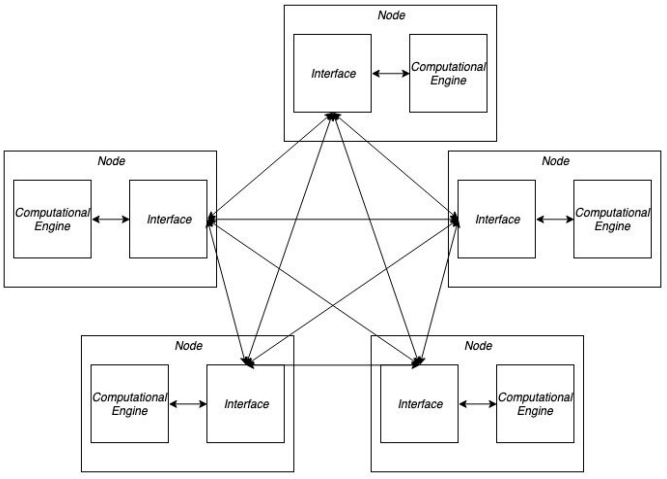
Bagian utama selanjutnya adalah *frontend*. Tugas utama dari *frontend* adalah memudahkan pemilih untuk berinteraksi dengan sistem *e-voting*. *Frontend* ini digunakan untuk memasukkan kunci publik pemilih dan memasukkan pilihan pemilih. Setelah itu data akan dikirim ke *backend* yang akan dikirim lagi ke Blockchain.

Bagian yang paling utama adalah Blockchain. Dalam sistem arsitektur *e-voting* ini terdiri dari beberapa Blockchain. Hal ini dilakukan agar panjang dari Blockchain tidak terlalu panjang agar kemampuan kecepatan dalam melakukan proses pemilihan suara tidak terlalu lama. Dalam satu Blockchain terdiri atas beberapa *node*. *Node* memiliki tugas utama untuk melakukan penyimpanan hasil pemilihan. Data yang disimpan dalam setiap *node* dalam satu Blockchain seharusnya sama karena ada beberapa kondisi saat *node* tidak memiliki data yang sama. Ketika pemilih melakukan pemilihan *node* akan memvalidasi pada pemilih. Jika pemilih *valid* maka setiap *node* akan menyimpan pilihan dari pemilih.

C. Arsitektur Blockchain

Pada subbab ini akan dibahas arsitektur dari Blockchain yang akan diimplementasikan. Secara umum arsitektur Blockchain bisa dilihat pada gambar 5. Satu Blockchain terdiri dari beberapa *node*. Setiap *node* akan terdiri dari dua komponen utama yang memiliki tugas masing-masing.

Komponen yang pertama dalam *node* adalah *interface*. *Interface* ini memiliki tujuan utama untuk berkomunikasi dengan *node* yang lain. *Interface* berkomunikasi dengan menggunakan RPC (*Remote Procedure Call*). RPC yang digunakan menggunakan jaringan internet melalui HTTPS.



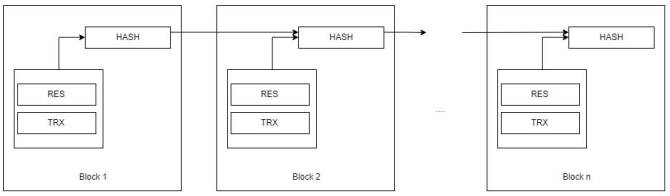
Gambar 5 Arsitektur Blockchain

Komponen selanjutnya adalah *computational engine*. *Computational engine* memiliki tujuan utama untuk melakukan verifikasi pada Blockchain dan membuat blok baru dalam Blockchain. *Computational engine* hanya berhubungan dengan *interface* saja.

Tujuan dipisahkan antara *interface* dan *computational engine* karena beberapa teknologi bagus di salah satu tempat. Teknologi yang digunakan dalam Blockchain akan dibahas pada sub bab selanjutnya.

D. Desain Blok dalam Blockchain

Pada subbab ini akan dijelaskan desain Blok dari Blockchain. Blok dari Blockchain memiliki tiga komponen utama yang bisa dilihat pada Gambar 6. Komponen utama tersebut yaitu HASH, RES dan TRX. Setiap komponen pada Blockchain memiliki peran masing-masing.



Gambar 6 Desain Blok dari Blockchain

Komponen pertama pada Blockchain yaitu RES. RES menyimpan data dari semua saldo yang dimiliki oleh akun Blockchain. Komponen ini berguna untuk mengetahui apakah akun Blockchain tersebut bisa melakukan transaksi.

Komponen yang kedua adalah TRX. TRX berisi transaksi dari akun Blockchain ke akun Blockchain lainnya. Dalam TRX juga terdapat tanda tangan digital dari pemilik akun Blockchain pengirim sehingga semua orang bisa memastikan bahwa transaksi ini benar dilakukan oleh akun tersebut.

Komponen yang terakhir adalah HASH. Dalam HASH terdapat nilai dari *hash* dari suatu Blok. Nilai *hash* dari suatu Blok dihitung dari nilai TRX dan nilai RES pada Blok ini dan nilai HASH pada Blok sebelumnya, kecuali pada Blok yang pertama tidak ada nilai HASH pada Blok sebelumnya.

IV. Pengujian

Dilakukan pengujian untuk sistem yang dirancang. Pengujian dilakukan secara *blackbox*. Kriteria yang diujikan adalah kriteria yang harus ada dalam *e-voting* yang telah dijabarkan pada bab III.

Hasil dari pengujian dapat memenuhi semua kriteria yang ada, tetapi terdapat beberapa asumsi yang harus dipenuhi. Asumsi yang pertama adalah semua komponen yang ada dapat berkomunikasi satu sama lain. Asumsi yang kedua adalah setiap *node* dalam Blockchain harus berlaku jujur. Asumsi yang ketiga adalah Blok dalam Blockchain dapat diakses secara publik.

V. Kesimpulan

Disini dapat disimpulkan bahwa sistem yang dirancang telah memenuhi tujuh kriteria keamanan yang dijabarkan pada bab III. Masih perlu penelitian lanjutan agar beberapa asumsi dapat dihilangkan.

Beberapa asumsi merupakan kelemahan. Asumsi yang merupakan kelemahan adalah setiap *node* harus berlaku jujur. Sehingga perlu dilakukan penelitian lanjutan untuk melakukan *verifikasi* bahwa *node* berlaku jujur.

References

[1] Gjøsteen, Kristian dan Anders Smedstuen Lund. 2015. *The Norwegian Internet Voting Protocol: A new Instantiation*. Department of Mathematical Sciences, NTNU.

[2] Heiberg, Sven, Arnis Parsovs dan Jan Willemson. 2015. *Log Analysis of Estonian Internet Voting 2013–2015*.

[3] https://docs.polys.me/technology-whitepaper/creating-a-vote diakses tanggal 6 Desember 2018.

[4] Schneier, Bruce. 1996. *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code*. C. John Wiley & Sons, Inc.

[5] https://blog.cryptographyengineering.com/2012/01/02/very-casual-introduction-to-fully/ diakses 27 Desember 2018.

[6] http://cryptowiki.net/index.php?title=Pailier_cryptosystem diakses 27 Desember 2018.

[7] Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

[8] Ongaro, Diego dan John Ousterhout. 2014. *In Search of an Understandable Consensus Algorithm (Extended Version)*. Stanford University.