Identity Management System Menggunakan *Public Key Infrastructure* Berbasis *Blockchain*

Ihsan Muhammad Asnadi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13516028@std.stei.itb.ac.id

***Abstract*—Jumlah dokumen yang harus diurus bertambah banyak seiring meningkatnya populasi manusia. Kartu tanda penduduk, akta lahir, sertifikat kepemilikan tanah dan bangunan, dan ijazah adalah sebagian dari banyak jenis dokumen yang perlu diurus. Cara menyimpan dokumen secara tradisional—dicetak di atas kertas—rentan akan kehilangan dan pemalsuan. Makalah ini akan membahas *Identity Management System* secara umum dan dokumen digital secara spesifik dengan menggunakan *Public Key Infrastructure* berbasis *blockchain*.**

***Index Terms*—*Identity Management System*, *Public Key Infrastructure*, *blockchain*, identitas, dokumen**

I. Pendahuluan

Jumlah dokumen—dalam bentuk kertas—yang semakin banyak menimbulkan berbagai masalah. Tempat penyimpanan dokumen tidak bertambah walaupun jumlah dokumen terus bertambah. Dokumen rentan hilang karena tidak terurus. Dokumen juga rentan dipalsukan karena proses verifikasi dokumen cukup sulit. Oleh sebab itu, dokumen mulai diterbitkan secara digital. Kartu tanda penduduk sudah mulai beralih menjadi E-KTP. Ijazah juga akan mulai diterbitkan secara digital—walaupun pandemik adalah alasan utama. Proses peralihan dokumen dari bentuk kertas menjadi digital memunculkan masalah. Salah satu masalah tersebut adalah melakukan verifikasi keaslian dokumen. Untuk itu, diperlukan sebuah metode untuk mengidentifikasi jejak digital dari sebuah entitas. Sebetulnya, sudah diajukan solusi berupa *Public Key Infrastructure*. Akan tetapi, masih ada masalah karena *Public Key Infrastructure* masih tersentralisasi. Makalah ini mengajukan solusi penggunaan *Public Key Infrastructure* berbasis *blockchain* untuk menyelesaikan masalah pada *Centralized Public Key Infrastructure*.

II. Dasar Teori

A. Identity Management System

Menurut KBBI, identitas adalah ciri-ciri atau keadaan khusus seseorang; jati diri. Identitas terdiri dari data personal yang dapat merepresentasikan seseorang. *Identity Management System* adalah sebuah sistem yang menyediakan perkakas untuk memanajemeni identitas digital seperti keaslian, otorisasi, dan pemberian hak/kuasa. Identitas (atau sebagian dari identitas) digunakan untuk berbagai hal, misalnya ketika melamar pekerjaan, atau ketika membuka rekening di bank.

Identify applicable funding agency here. If none, delete this.

Pada beberapa transaksi, identitas diperlukan agar pelaku dapat diidentifikasi. Misal ketika memasuki daerah yang hanya boleh dimasuki orang tertentu. Tetapi ada juga transaksi yang dapat dilakukan secara anonim. Misal ketika membeli sesuatu di warung.

B. Public Key Infrastructure

Public Key Infrastructure adalah infrastruktur yang menyediakan layanan terintegrasi untuk membuat, menyimpan, memverifikasi, dan membuang sertifikat digital [2]. Infrastruktur [2] ini terdiri dari:

- *Certification Authority* yang bertugas untuk menerbitkan dan memverifikasi sertifikat digital.
- *Registration Authority* yang memverifikasi identitas pengguna yang meminta informasi dari *Certification Authority*.
- *Repository* untuk menyimpan sertifikat digital dan *Certificate Revocation List*.
- Aturan atau kebijakan.

C. Blockchain

Blockchain adalah sebuah *distributed database*, artinya, data yang terdapat pada *blockchain* disimpan di banyak komputer; itulah sebabnya *blockchain* disebut *distributed*. Tidak seperti *centralized database*, yaitu *database* yang ditangani oleh satu pihak tertentu untuk melakukan verifikasi data agar integritas data terjamin; *distributed database* menggunakan *consensus algorithm* untuk membuat semua *peer* menyetujui data yang akan disimpan.

D. Cara Kerja Blockchain

Terdapat syarat utama yang diperlukan untuk membangun sistem berbasis *blockchain*, yaitu *peer*. Sekurang-kurangnya diperlukan tiga *peer* agar *blockchain* dapat bekerja. Hal ini dikarenakan perlu ada konsensus saat memvalidasi data.

Pertama-tama, setiap *peer* memiliki jurnal kosong. Setiap ada data baru, semua *peer* menuliskan data baru pada jurnal masing-masing.

Setelah satu halaman jurnal penuh, yaitu ketika jumlah data telah mencapai nilai tertentu, maka halaman tersebut akan disegel dengan sebuah kunci tertentu. Segel ini adalah sebuah *cryptographic function* yang telah disetujui bersama oleh semua *peer* di dalam *network*.

Halaman yang sudah disegel disetujui sebagai transaksi yang valid, dan tidak akan dapat diubah lagi di masa mendatang. Setiap halaman yang telah disegel akan memiliki *pointer* yang menunjuk pada halaman selanjutnya, membentuk sebuah rantai dari *block* sehingga disebut *blockchain*.

Akibatnya, jika ada *peer* yang ingin melakukan perubahan pada sebuah *block*, *peer* tersebut harus melakukan penyegelan ulang yang dapat melampaui kecepatan semua *peer* yang ada di dalam *network* untuk membuat sebuah rantai *block* yang baru.

E. Consensus Algorithm

Consensus algorithm adalah sebuah algoritma yang digunakan oleh *peer* di dalam *network* untuk memvalidasi sebuah data. Beberapa *consensus algorithm* meliputi, tapi tidak terbatas pada:

- *Proof-of-Work*
  Proof-of-Work bekerja dengan mekanisme berikut: ketika terdapat data baru yang harus divalidasi, semua *peer* berlomba-lomba untuk memvalidasi data. Data akan divalidasi dengan membuat *complex hashing* yang melibatkan *computational power* yang tinggi. *Peer* yang berhasil menyelesaikan *hashing* pertama kali akan diberikan insentif.
- *Proof-of-Stake*
  Berbeda dengan *Proof-of-Work*, *Proof-of-Stake* tidak melibatkan perlombaan untuk melakukan *hashing*. *Validator* dipilih berdasarkan *stake* yang dimiliki oleh *peer*, artinya, semakin banyak *stake* yang dimiliki oleh *peer*, maka semakin besar kemungkinan untuk menjadi *validator*. Hal ini menghilangkan "perlombaan" seperti yang ada pada *Proof-of-Work* sehingga waktu yang diperlukan untuk melakukan validasi data menjadi lebih cepat.

F. Karakteristik Blockchain

- Dapat dipercaya
  Dengan asumsi bahwa *peer* yang jujur lebih banyak daripada *peer* yang berbuat curang, maka data yang terdapat pada *blockchain* diasumsikan valid.
- *Immutable*
  Berdasarkan penjelasan di atas, data yang terdapat pada *blockchain* bersifat *immutable*. Hal ini dikarenakan *peer* yang ingin berbuat curang harus mengubah semua data di dalam rantai terpanjang dalam *blockchain*. Dengan *consensus algorithm*, tidak mungkin *peer* yang ingin berbuat curang dapat menandingi kecepatan validasi mayoritas *peer* yang jujur.
  Terdapat pengecualian jika *peer* yang tidak jujur lebih banyak dari *peer* yang jujur (dikenal juga dengan *51% attack*), maka sistem *blockchain* akan gagal.
- Dapat menghindari *double spending*
  Untuk lebih mengenal *double spending*, diberikan ilustrasi berikut:
  Terdapat A, B, dan C yang masing-masing memiliki uang sejumlah X. Ketika A melakukan transfer uang sejumlah X kepada B, B mencatat transaksi tersebut, sebelum B selesai mencatat (dan C mengetahui kondisi A), A langsung melakukan transfer uang sejumlah X kepada C, yang juga langsung dicatat oleh C.
  Pada kasus tersebut, A berhasil melakukan transfer uang sejumlah X kepada B dan C (dengan total 2X), walaupun A hanya memiliki uang sejumlah X. Hal ini disebut *double spending*. Karena *blockchain* menggunakan *consensus algorithm*, maka tidak akan ada *double spending* karena semua *peer* dalam *network* akan menyetujui sebuah transaksi sebelum menyetujui transaksi berikutnya.

G. Smart Contract

Smart Contract adalah sebuah program yang dieksekusi dan diperlakukan sebagai pengguna. Apapun yang dapat dilakukan oleh pengguna, dapat dilakukan juga oleh *Smart Contract*.

Hal ini akan menjadi bermanfaat pada kasus berikut:

Bayangkan A meminjam uang kepada B. A berjanji akan mengembalikan uang tersebut satu bulan kemudian. Ada beberapa kemungkinan untuk menjamin transaksi tersebut terjadi:

- Saling percaya
  A akan membayar B bulan depan dan B percaya bahwa A akan menepati janjinya. Tidak ada basis yang dapat menjamin A akan membayar B. Jika A tidak membayar B, tidak ada yang dapat B lakukan untuk mendapatkan kembali uang miliknya.
- Menandatangani perjanjian yang ditegakkan dengan hukum
  A dan B menandatangani perjanjian yang menyatakan bahwa A harus membayar sejumlah uang pada B bulan depan. Tetapi kenyataannya, jika A tidak berhasil membayar sejumlah uang pada B bulan depan, perlu banyak usaha untuk membawa kasus ini ke pengadilan. Bahkan mungkin tidak sebanding dengan jumlah uang yang dipinjam.
- Menggunakan pihak ketiga
  A dan B mempercayai C untuk menjamin bahwa A akan membayar sejumlah uang bulan depan, misal dengan A memberikan jaminan kepada C untuk membayarkan sejumlah uang kepada B bulan depan. Tetapi, lagi-lagi hal ini melibatkan kepercayaan, yang tidak memiliki dasar kuat seperti yang telah dijelaskan di poin pertama. Jika C kabur dengan jaminan, A dan B akan mengalami kerugian.

Dengan *Smart Contract*, hal ini dengan mudah dapat diselesaikan, karena berbeda dengan poin "menggunakan pihak ketiga" di atas yang memiliki celah dalam kepercayaan, *Smart Contract* adalah program yang jika dibuat dengan benar, akan melakukan hal yang diperintahkannya dengan pasti.

H. Permission

- *Permissionless*
  Pada *permissionless blockchain*, semua orang dapat bergabung ke dalam *network*. Karena semua *peer* dapat menjadi *validator*, maka perlu diberikan insentif agar setiap *peer* dapat dipercaya.

- *Permissioned*
  Pada *permissioned blockchain*, hanya individu tertentu yang dapat bergabung ke dalam *network*. Setiap individu akan diberikan izin untuk membaca ataupun menulis *block*. Pada *permissioned blockchain*, konsensus dapat dicapai dengan cepat jika jumlah *validator* dibatasi dengan mengambil hanya sebagian *peer* di dalam *network*. Biasanya *permissioned blockchain* digunakan di dalam sebuah organisasi.

I. Visibility

- *Public*
  Pada *public blockchain*, data akan disimpan secara transparan. Artinya, semua *node* dapat melihat data yang ada. Biasanya digunakan pada *cryptocurrency*.
- *Private*
  Public blockchain tidak cocok untuk organisasi yang menyimpan data sensitif. Biasanya organisasi tersebut akan menggunakan *private blockchain*. *Private blockchain* hanya dapat dimasuki oleh *node* yang telah diundang.

III. Analisis

A. Permasalahan

Berdasarkan teori di atas, *Centralized Public Key Infrastructure* memiliki permasalahan sebagai berikut:

- *Single point of failure*. Sistem yang tersentralisasi akan lumpuh saat sistem tersebut diserang (*e.g. Denial-of-Service*)
- *Trust issue*. *Certification Authority* belum tentu dapat dipercayai sepenuhnya. Sebagai contoh, DigiNotar pernah menerbitkan sertifikat digital palsu yang digunakan untuk melakukan *man-in-the-middle attack* pada pengguna Google [4].

B. Desain Umum

Desain ini akan mencoba menyelesaikan permasalahan dalam *Centralized Public Key Infrastructure*. Pada *Centralized Public Key Infrastructure*, diperlukan *Certification Authority* untuk menerbitkan dan memverifikasi sertifikat digital. Penggunaan *blockchain* membuat entitas dapat menerbitkan sertifikat digital yang diverifikasi oleh mayoritas entitas lain di dalam sistem. Penggunaan *blockchain* yang terdesentralisasi juga menghilangkan kelemahan *single point of failure* pada *Centralized Public Key Infrastructure*. Sistem akan menggunakan *Smart Contract* untuk memanajemeni operasi pada identitas. Operasi yang dimaksud adalah membuat, menghapus, dan memverifikasi identitas.

C. Alur Sistem

Sistem yang dideskripsikan di atas akan berjalan dengan alur berikut:

- Entitas menerbitkan sertifikat digital pada sistem.
- Sistem melakukan verifikasi sertifikat digital.
- Sertifikat digital diterbitkan secara publik.
- Entitas lain yang ingin memverifikasi sertifikat digital dapat melihat kesahihan sertifikat melalui sistem.

IV. Kesimpulan

Melakukan pendekatan *Public Key Infrastructure* berbasis *blockchain* memberikan beberapa keunggulan dibandingkan *Centralized Public Key Infrastructure* seperti menghilangkan *single point of failure* dan *trust issue* terhadap *Certification Authority*.

V. Perbaikan Mendatang

Makalah ini dapat dilanjutkan dengan memperbaiki aspek-aspek berikut:

- Menentukan *consensus algorithm* yang akan dipakai.
- Menentukan *visibility* sistem *blockchain*.
- Menentukan *permission* sistem *blockchain*.
- Menentukan jenis *Smart Contract* yang perlu dikembangkan.

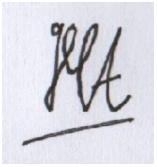
Referensi

[1] M. Rinaldi, "IF4020 Kriptografi – Tandatangan Digital".
[2] M. Rinaldi, "IF4020 Kriptografi – Sertifikat Digital dan Public Key Infrastructure (PKI)".
[3] N. Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009.
[4] A. Heather, "An update on attempted man-in-the-middle attacks", 2011.
[5] A. Mustafa, "SCPKI: A Smart Contract-based PKI and Identity System".

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Tangerang, 8 Mei 2020



Ihsan Muhammad Asnadi
13516028