Rancang Bangun *Identity and Access Management* IoT Berbasis KSI dan *Permissioned Blockchain*

Guntur Dharma Putra[1], Sujoko Sumaryono[1], Widyawan[1]

Abstract— Blockchain offers several technological breakthroughs, ranging from monetary solutions to healthcare systems. Some approaches have proposed blockchain implementation in IoT for providing better performance and scalability. However, massive scale implementation of IoT devices suffers from several issues in identity and access managements of interconnected devices. The present study proposes the combination of permissioned blockchain and Keyless Signature Infrastructure (KSI) as a means of governing the identity and access management of IoT devices. KSI is known for its ability to offer digital signature services without the need of public or private key but hash trees updated in a regular basis. With the decentralization fashion of blockchain, KSI can be implemented more efficiently. The results may give an identity and access management with high scalability.

***Intisari— Blockchain* menawarkan berbagai dobrakan di bidang teknologi, mulai dari bidang keuangan hingga kesehatan. Beberapa usulan juga menerapkan *blockchain* pada teknologi IoT untuk meningkatkan unjuk kerja dan *scalability*. Namun, tipikal penerapan teknologi IoT dalam skala masif masih memiliki beberapa kendala, terlebih dalam hal manajemen akses dan identitas peranti yang terkoneksi. Makalah ini mengusulkan kombinasi dari *permissioned blockchain* dan teknologi *Keyless Signature Infrastructure* (KSI) sebagai metode untuk mengatur hak akses dan identitas peranti IoT. KSI dikenal mampu untuk memberikan layanan tanda tangan digital tanpa tergantung pada kunci privat maupun publik dengan menggunakan teknik pohon *hash*. Dengan karakteristik dari *blockchain* yang terdistribusi, teknologi KSI dapat dipadukan secara lebih efisien. Hasil yang diperoleh memberikan manajemen akses dan identitas dengan *scalability* yang tinggi.**

***Kata Kunci*— manajemen identitas dan akses, *permissioned blockchain, Internet of Things, Keyless Signature Infrastructure,* keamanan data dan jaringan.**

I. PENDAHULUAN

Sejak pertamakali diperkenalkan oleh Satoshi Nakamoto sebagai teknologi dasar dari mata uang digital Bitcoin [1], *blockchain* menjadi semakin populer dan diterapkan di berbagai bidang selain bidang moneter, seperti *proof of location* [2], sistem penyimpanan terdistribusi [3], pendukung teknologi kota cerdas [4], dan teknologi kesehatan [5]. Pada dasarnya, *blockchain* adalah semacam buku catatan besar (*ledger*), tetap (*immutable*), dan terdistribusi yang terdiri atas rangkaian blok data yang saling terkoneksi tanpa titik kerusakan tunggal (*single point of failure*). Walaupun *blockchain* terkenal dengan tingkat komputasi yang tinggi dan berat, beberapa solusi sudah diusulkan untuk mengimplementasikan *blockchain* pada peranti *Internet of Things* (IoT) [6]–[8].

Implementasi *blockchain* pada peranti IoT tidak dapat dilakukan secara langsung karena karakteristik *blockchain* yang memiliki tingkat komputasi yang tinggi dan berat. Solusi yang ada mengoptimasi *blockchain* agar sesuai dengan karakteristik peranti IoT dengan mengeliminasi beberapa *overhead* tanpa pengorbanan yang signifikan pada sisi keamanan dan privasi [7]. Beberapa teknik implementasi *blockchain* di IoT menghilangkan sisi *Proof of Work* (PoW), pemisahan antara lapisan data dan transaksi, dan kombinasi antara *blockchain* publik dan privat. Pada teknik implementasi ini, komunikasi pada *nodes* selalu terenkripsi dengan mekanisme kunci publik dan menggunakan teknik verifikasi tanpa konsensus. Sebuah *node* dapat mengganti kunci publiknya secara berkala untuk menjaga anonimitas dan privasi [6].

Namun demikian, dalam kondisi dengan ribuan atau jutaan peranti IoT terhubung secara bersamaan, beberapa kendala akan muncul terkait kendali akses dan identitas dari masing-masing peranti. Arsitektur terdistribusi yang diusung oleh *blockchain* masih membutuhkan penelitian lebih lanjut untuk menjaga *scalability* dari jutaan interkoneksi peranti IoT untuk menjaga tingkat ketersediaan (*availability*) pada tingkat tertentu [9]. Manajemen akses dan identitas harus menjaga keamanan dan tata kelola kepemilikan dan hak akses peranti IoT serta tetap menjaga privasi.

Solusi manajemen akses dan identitas yang ada bekerja untuk menjamin privasi pengguna dengan mengatur data pribadi melalui mekanisme *user consent*. Namun, pada praktiknya IoT sering diterapkan dalam skala masif dengan ribuan hingga jutaan peranti yang saling terhubung, sehingga mekanisme *user consent* tidak mungkin untuk dilakukan disebabkan oleh faktor skalabilitas. Proses manajemen akses dan identitas juga mengalami kendala di sisi antarmuka, sehingga susah untuk dikendalikan langsung oleh manusia [10].

Makalah ini mengusulkan rancang bangun dari sebuah manajemen identitas dan akses peranti IoT berbasis *blockchain* dengan memadukannya dengan teknologi *Keyless Signatures' Infrastructure* (KSI). Teknologi KSI dapat memanfaatkan aspek desentralisasi dan terdistribusi dari *blockchain* untuk mempublikasikan *root hash* pada *blockchain* secara berkala. Selain itu, perpaduan dari dua teknologi ini mampu memberikan layanan identitas dan kendali akses dengan *scalability* dan *uptime* yang tinggi dikarenakan tidak adanya kebergantungan pada suatu titik (*node*).

Makalah ini dibagi menjadi beberapa bagian sebagai berikut. Pada bagian II, dijabarkan review singkat tentang teknologi BC, KSI, dan *Identity and Access Management* (IAM). Pada bagian III, metode yang diusulkan dibahas secara komprehensif. Pada bagian IV, dijelaskan mengenai pembahasan proposal teknologi yang diusulkan. Selanjutnya, kesimpulan makalah ini diberikan pada bagian akhir.

[1]*Dosen, Departemen Teknik Elektro dan Teknologi Informasi, Fakultas Teknik, Universitas Gadjah Mada, Jalan Grafika No. 2, Yogyakarta 55281 (tlp: 0274-552 305; fax: 0274-552 305;e-mail: {gdputra, sujoko, widyawan}@ugm.ac.id).*

TABEL I
PERBANDINGAN PLATFORM *BLOCKCHAIN*

Nama	Aplikasi	Konsensus	Bahasa	Repositori Kode Publik
Hyperledger	*Smart contracts*	Practical Byzantine Fault Tolerance (PBFT)	Golang	https://github.com/hyperledger/fabric
Bitcoin	*Cryptocurrency*	Bitcoin Proof of Work	C++	https://github.com/bitcoin/bitcoin
Ethereum	*Smart contracts*, *Cryptocurrency*	Ethas	Go	https://github.com/ethereum/go-ethereum
Rootstock	*Cryptocurrency*	RSK Proof of Work	Java	https://github.com/rsksmart/rskj
Ripple	*Cryptocurrency*	Ripple Consensus Ledger (PoS)	C++	https://github.com/ripple/rippled
Corda	*Smart contracts*	Raft	Kotlin, Java	https://github.com/corda/corda
Stellar	*Smart contracts*	Stellar Consensus Protocol (SCP)	C, C++	https://github.com/stellar/stellar-core

II. BLOCKCHAIN, KSI, DAN IAM

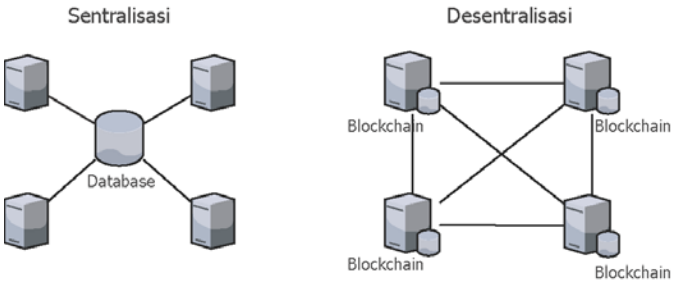
Makalah ini mengusulkan sebuah IAM dengan teknologi *blockchain* dan KSI. Berikut ulasan singkat dari studi literatur yang telah dilakukan.

A. Blockchain

Blockchain dapat dikatakan sebagai basis data terdistribusi yang tidak memerlukan otoritas pusat sehingga menghilangkan perlunya verifikasi dari pihak ketiga [1]. *Blockchain* terdiri atas sekumpulan blok yang terhubung satu dengan lainnya dengan metode *hash*, sehingga membentuk sebuah rantai dari kumpulan blok. Blok genesis adalah blok pertama dari sebuah *blockchain* yang selalu dituliskan secara manual (*hardcoded*) pada perangkat lunak BC. Blok genesis dapat dikatakan sebagai sebuah blok khusus yang tidak mengacu pada blok sebelumnya. Pada sebuah blok pada BC, hanya ada satu jalur menuju blok genesis. Namun, terdapat beberapa jalur dari blok genesis ke blok yang terakhir karena sebuah *blockchain* dapat memiliki cabang (*forking*).

Teknologi *blockchain* memiliki beberapa karakteristik sebagai berikut [11].

1. Kendali yang terdesentralisasi. Sebuah desentralisasi yang tidak ada sebuah otoritas yang mengatur secara mutlak, seperti tampak pada Gbr. 1.
2. Data yang transparan dan mudah untuk diaudit. Setiap *node* yang terhubung ke dalam jaringan *blockchain* memiliki salinan lengkap dari *blockchain* (publik), sejak blok genesis hingga blok terkini.



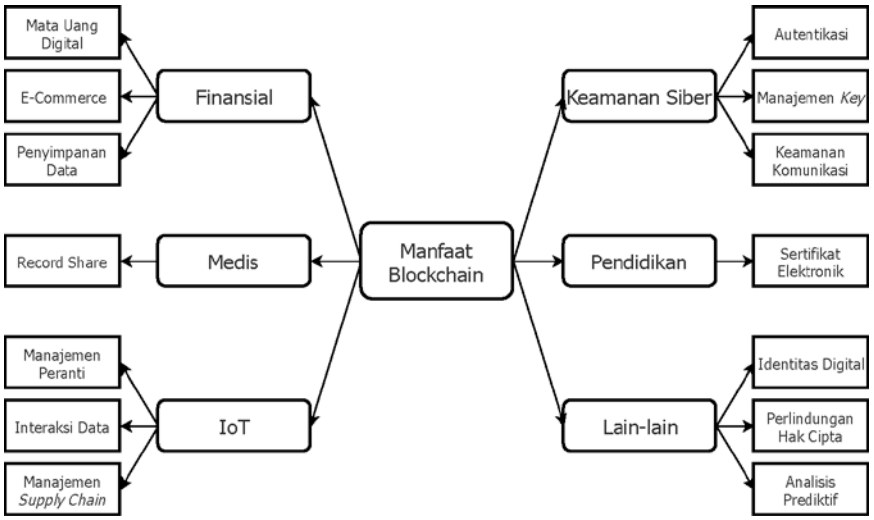
Gbr. 1 Konsep desentralisasi pada *blockchain*.

3. Informasi yang terdistribusi. Setiap *node* menyimpan salinan dari *blockchain* untuk menghindari adanya otoritas terpusat yang menyimpan informasi tersebut sendiri.
4. Konsensus yang terdesentralisasi. Transaksi-transaksi yang direkam ke dalam *blockchain* divalidasi oleh setiap *node* yang terhubung ke dalam jaringan BC. Hal ini mematahkan paradigma konsensus terpusat.
5. Aman. *Blockchain* kebal terhadap kerusakan yang disengaja dan tidak dapat dimanipulasi secara sengaja oleh pihak tidak bertanggung jawab.

Tiap blok menyimpan kumpulan transaksi yang merupakan catatan dari pertukaran nilai (*cryptocurrency*) antar dua entitas yang dikirimkan secara *broadcast* kepada semua *node* dalam jaringan BC. Semua transaksi bersifat transparan dan dapat dilihat oleh siapapun. Dalam *blockchain* dikenal istilah menambang (*mining*), yaitu proses penciptaan blok (*block generation*) baik secara individu maupun kolektif. Proses menambang dirancang agar memakan sumber daya secara intens dan sulit untuk dilakukan.

Masing-masing blok harus memiliki sebuah PoW sebagai bukti dari validitas sebuah blok [12]. PoW diperiksa oleh penambang-penambang (*miners*) yang lain saat menerima sebuah blok baru. Tujuan utama dari proses menambang adalah agar sistem *blockchain* dapat mencapai konsensus yang aman dan kebal terhadap tindakan-tindakan jahat. Sistem *blockchain* akan beradaptasi pada kemampuan menambang secara kumulatif untuk menjaga waktu yang diperlukan untuk menyelesaikan PoW pada suatu level tertentu (10 menit pada *blockchain* Bitcoin).

Konsensus adalah problematika mendasar pada suatu sistem terdistribusi yang memerlukan dua atau lebih agen untuk mencapai kesepakatan pada sebuah nilai tertentu untuk menjalankan sebuah komputasi. Pada pelaksanaannya, beberapa agen bisa jadi tidak andal dan proses untuk mencapai konsensus harus mempertimbangkan hal ini. *blockchain* menerapkan beberapa algoritme konsensus, seperti PoW, *Proof of Stake* (PoS), *proof of storage*, *proof of capacity*, dan lain-lain.



Gbr. 2 Peluang pemanfaatan *blockchain* di berbagai bidang [13].

Beberapa perangkat lunak yang populer berjalan di atas *platform* BC, seperti yang dijabarkan pada Tabel I. Perangkat lunak tersebut antara lain adalah sebagai berikut.

1. Bitcoin, yaitu konseptualisasi dan implementasi pertama dari *blockchain* sebagai *cryptocurrency* (mata uang digital berbasis kriptografi) yang bernilai ekonomis. Bitcoin berjalan dengan menggunakan kriptografi kunci publik, jaringan *peer to peer*, dan PoW. Bitcoin menggunakan PoW yang sengaja diprogram agar penciptaan blok baru hanya terjadi tiap 10 menit.
2. Ethereum, yang dirancang oleh seorang pengembang Bitcoin, V. Buterin, sebagai sebuah *platform* terdesentralisasi yang berjalan di atas teknologi BC. Ethereum memiliki mata uangnya sendiri yang dinamai *ether* dan mata uang internal untuk pembayaran biaya transaksi dan komputasi bernama *gas*. Walaupun saat ini Ethereum menggunakan PoW sebagai mekanisme konsensusnya, Ethereum akan mengubah mekanisme konsensus menjadi PoS. Ethereum memiliki waktu penciptaan blok yang paling cepat di antara aplikasi *blockchain* yang lain, yaitu 12 detik.
3. Rootstock, yakni platform *open source* baru yang mirip dengan Ethereum dalam hal pembuatan *smart contracts*, walaupun dalam praktiknya Rootstock berjalan di atas ekosistem Bitcoin. Rootstock berjalan sebagai Bitcoin *sidechain* dan bersifat *backwards compatible* dengan *Ethereum virtual machine* (EVM).
4. Hyperledger, yaitu sebuah proyek yang digawangi oleh Linux Foundation sebagai proyek kolaborasi antar berbagai industri. Pada awalnya, sistem dirancang dengan standar *enterprise* dengan kompatibilitas pada berbagai protokol konsensus. Hyperledger menggunakan algoritme *practical Byzantine fault tolerant* (PBFT) yang terkenal dengan kemampuannya untuk menangani ribuan *request* per detik dengan latensi yang kurang dari satu milisekon.

Selain keempat aplikasi tersebut, *blockchain* dapat dan telah diimplementasikan di berbagai bidang [13], seperti tertera pada Gbr. 2. Sebagai contoh, *blockchain* dapat digunakan sebagai dasar pengembangan perangkat lunak *e-commerce* dan penyimpanan data finansial. Selain itu, *blockchain* dapat digunakan dalam bidang kesehatan untuk menyimpan catatan kesehatan seseorang secara terdistribusi dan tetap menjaga privasi pribadi.

B. Identity and Access Management (IAM)

Kebutuhan akan manajemen autentikasi, akses, dan identitas semakin tidak terelakkan dengan perkembangan teknologi web sebagai platform yang terdiri atas aplikasi yang bermacam-macam. Arsitektur perangkat lunak modern memiliki kemampuan tata kelola keamanan dan akses tidak hanya untuk aplikasi yang berdiri sendiri atau terisolasi, tetapi juga aplikasi besar yang memiliki hubungan dengan berbagai aplikasi dan layanan (*services*) lain.

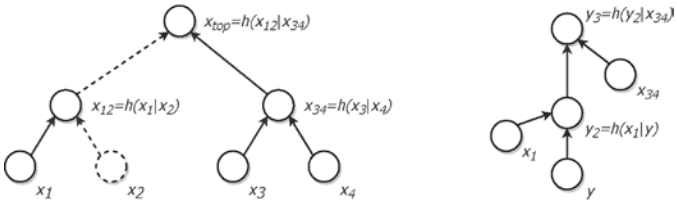
Salah satu pendekatan dalam IAM adalah dengan menggunakan konsep komputasi *cloud* yang juga dikenal dengan istilah *Identity as a Service* (IDaaS) [14]. Metode ini bertujuan untuk menyederhanakan manajemen identitas dan akses agar lebih efisien dengan memanfaatkan *enterprise service layer*. Dengan kata lain, pengguna dapat memanfaatkan sistem manajemen identitas yang disediakan melalui teknologi komputasi *cloud*. Beberapa manfaat akan didapatkan seperti berkurangnya infrastruktur *on-site*, integrasi manajemen dengan *cloud*, dan kemudahan dalam penggunaan. Namun, penggunaan IDaaS berarti memasrahkan kendali kritikal sebuah sistem yang menyangkut identitas dan autentikasi kepada pihak ketiga, sehingga komitmen dalam perlindungan dan pemrosesan data tidak dapat dipastikan.

C. Keyless Signatures' Infrastructure

Keyless Signatures' Infrastruktur (KSI) diusulkan pertama kali sebagai sebuah metode untuk melakukan proses *timestamping* data dalam skala besar [15]. *Timestamp* yang dihasilkan dapat diverifikasi oleh siapa pun dengan infrastruktur publik pendukung yang menjamin tidak adanya modifikasi dari dokumen atau *timestamp* itu sendiri. Dengan kata lain, *timestamp* pada KSI dapat dinilai sebagai tanda tangan digital. Kata *keyless* di sini berarti tanda tangan digital

tersebut dapat diverifikasi tanpa bergantung pada kerahasiaan sebuah kunci privat. Integritas dari tanda tangan dilindungi oleh fungsi *hash* yang bersifat satu arah dan tidak terlibatnya kunci privat apapun [16]. KSI juga memiliki *scalability* yang tinggi, mengikuti waktu dan jumlah transaksi.

Pada praktiknya, pengguna KSI mengirimkan *hash* dari dokumen untuk kemudian mendapatkan *signature token* yang merupakan sebuah jalur (*path*) ke *root* dari pohon Merkle. *Signature token* merupakan bukti bahwa data tersebut sudah memiliki *timestamp* digital yang valid. KSI melakukan agregasi terhadap semua permintaan yang datang ke dalam sebuah pohon *hash* besar dan menyimpan *hash value* paling atas (*root*) yang dihasilkan tiap detik. Kumpulan dari *top hash values* disimpan secara terstruktur untuk disusun ke dalam kalender *hash*.



Gbr. 3 Perhitungan sebuah pohon *hash* (kiri) dan verifikasi y sebagai posisi dari x_2 [15].

Pada Gbr. 3 disajikan cara untuk memverifikasi sebuah *signature token* y terhadap posisi x_2 yang dimulai dengan menggabungkan y dan x_1 (nilai x_1 diketahui karena merupakan bagian dari *signature token*) dengan fungsi *hash* $y_2 = h(x_1|y)$. Nilai dari y_2 kemudian digunakan sebagai masukan dari proses penggabungan selanjutnya. Jika $x_{top} = y_2$, maka dapat dianggap bahwa y memang bagian dari pohon *hash* yang sudah dibangun sebelumnya. Besarnya *signature token* bergantung pada tingkat agregasi. Dengan bertambahnya permintaan dari pengguna, jumlah atau tingkat agregasi bertambah secara logaritmik. Konsekuensinya, jumlah *hash* yang harus disimpan untuk berhasil membangun ulang pohon *hash* hingga ke *top hash* (*root*) juga bertambah.

Seperti yang tertera pada Gbr. 4, proses yang berjalan pada mekanisme KSI dikelompokkan menjadi tiga proses, yaitu *hashing*, agregasi, dan publikasi. Transaksi atau *statements* direpresentasikan dan disimpan dalam bentuk *hash* untuk kemudian dikirim melalui *gateway* KSI dan selanjutnya mendapatkan *signature token* sebagai responsnya. Sebuah pohon *hash* global per satuan waktu disusun oleh agregator yang merupakan gabungan dari semua permintaan (*request*) dari pengguna. *Top hash value* (*root*) dari pohon *hash* global per satuan waktu tersebut digabungkan satu dengan lainnya dan dipublikasikan pada sebuah media yang dapat dilihat secara publik (dalam hal ini *blockchain*). Arsitektur secara umum dari KSI ditampilkan pada Gbr. 5.

III. RANCANG BANGUN IAM

Perancangan sistem manajemen identitas dan akses yang tepat akan melindungi peranti IoT dari penggunaan yang tidak bertanggung jawab seperti kejadian *Distributed Denial-of-Service* (DDos) yang terjadi di Amerika Serikat di akhir tahun 2016 [17]. Menurut laporan yang diterima, peralatan-peralatan IoT sederhana disalahgunakan untuk melancarkan serangan DDoS yang sangat masif dengan membanjiri layanan DNS bernama Dyn. Serangan dilaporkan datang dari puluhan juta alamat IP pada satu waktu yang sama sehingga menyebabkan waktu *downtime* sampai dua jam.

TABEL II
TANTANGAN IMPLEMENTASI *BLOCKCHAIN* PADA PERANTI IOT

Blockchain	**IoT**
Kebutuhan sumber daya besar	Sumber daya sangat terbatas
Proses menambang memakan waktu yang lama	Membutuhkan latensi yang singkat
Scalability yang rendah	Implementasi skala besar
Boros dalam *bandwidth*	Terbatas dalam *bandwidth*

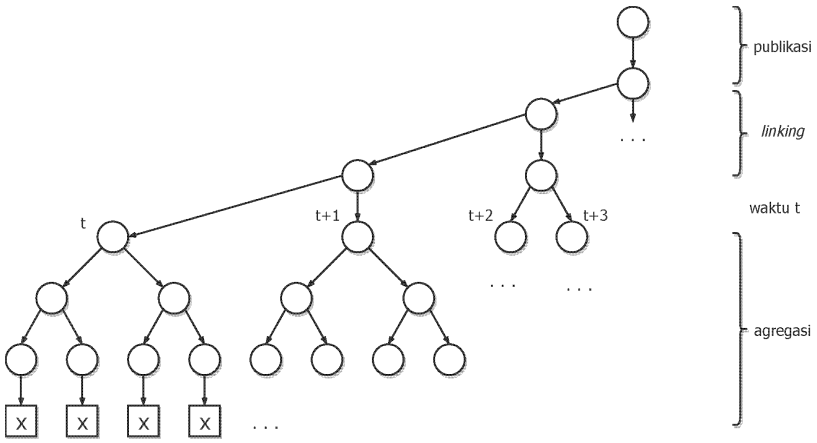
Secara garis besar, solusi *blockchain* dan KSI tidak diterapkan secara langsung pada peranti IoT itu sendiri dikarenakan keterbatasan yang dimiliki oleh sumber daya peranti tersebut, seperti dijabarkan pada Tabel II. Oleh karena itu, sistem IAM yang diusulkan melibatkan infrastruktur lain yang memiliki sumber daya dan kemampuan komputasi lebih tinggi sebagai pelengkap jalannya sistem IAM. Agar interoperabilitas antara peranti IoT yang memiliki sumber daya terbatas dan peranti pendukung dengan sumber daya besar dapat berjalan, komunikasi peranti IoT menggunakan protokol *Constrained Application Protocol* (CoAP) [18]. Protokol tersebut andal dalam menangani komunikasi pada peranti dengan keterbatasan sumber daya dan mudah untuk ditranslasikan ke dalam *Internet Protocol* (IP).

Rancang bangun sistem IAM dijabarkan dari arsitektur garis besar beserta komponen-komponen dari sistem tersebut dan kemudian penjelasan alur kerja sistem disertai dengan contoh.

A. *Komponen-Komponen Sistem*

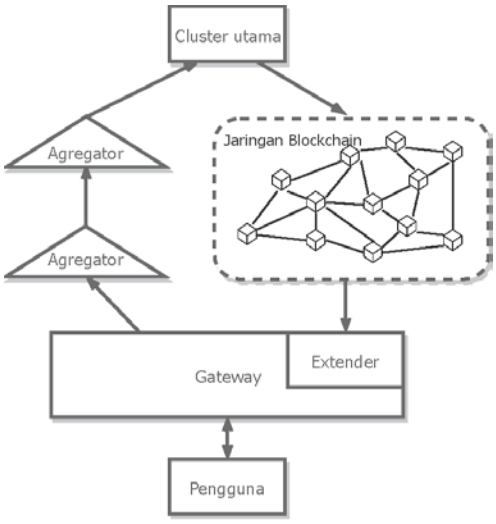
Arsitektur dari sistem IAM berbasis KSI dan *permissioned blockchain* dijabarkan pada Gbr. 6. Secara garis besar, komponen-komponen dari sistem IAM dibagi menjadi empat kelompok, yaitu jaringan peranti IoT, *management hub*, *KSI provider*, dan jaringan *blockchain*.

1) Jaringan Peranti IoT: Jaringan peranti IoT yang dimaksud adalah interkoneksi peranti IoT konvensional. Tidak ada prasyarat khusus dari peranti tersebut. Namun, diasumsikan protokol pada *service layer* yang digunakan dalam berkomunikasi adalah CoAP, sebagaimana dijabarkan pada dokumen RFC7252 [18]. Protokol lapisan bawah mengikuti protokol yang secara khusus didukung oleh peranti, mengingat peranti IoT memiliki model komunikasi yang beragam, mulai dari koneksi kabel hingga nirkabel. Dengan demikian, peranti IoT yang saling terhubung dapat melakukan aktivitasnya seperti biasa tanpa ada intervensi khusus. Untuk memanfaatkan layanan IAM, peranti IoT berkomunikasi dengan *management hub*.



Gbr. 4 Proses *timestamping* berbasis pohon hash [15].

2) Management Hub: Management hub bertindak sebagai jembatan antara peranti dengan sumber daya terbatas (IoT) dan peranti pendukung layanan IAM. Proses penjembatanan yang dilakukan adalah proses translasi dari protokol CoAP ke protokol HTTP, yang umum dilakukan pada komunikasi internet. Masing-masing jaringan IoT dapat memiliki *management hub*-nya sendiri dan untuk menjaga tingkat ketersediaan yang tinggi, *management hub* diimplementasikan secara *redundant*. Selain melayani permintaan dari peranti-peranti IoT, *management hub* juga berkomunikasi dengan *KSI provider* dengan cara meneruskan permintaan akan verifikasi identitas (autentikasi) dan kebijakan akses (*policy*) dan mengembalikan hasil permintaan kembali kepada peranti yang bersangkutan.



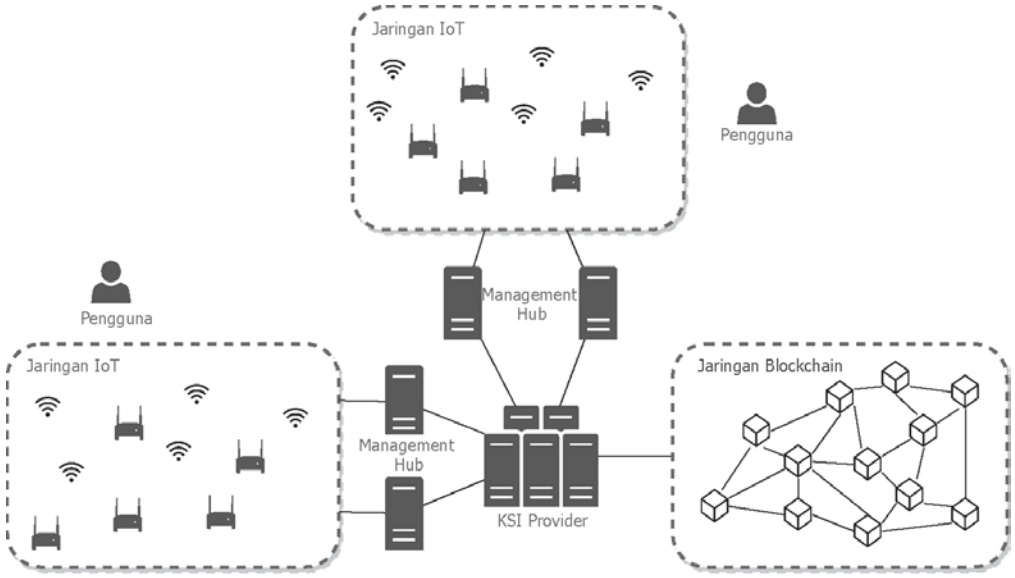
Gbr. 5 Arsitektur *high-level* dari *Keyless Signatures' Infrastructure*.

3) KSI Provider: Komponen ini adalah salah satu komponen utama dari sistem IAM yang diusulkan. KSI menyediakan sebuah layanan *timestamping* (*digital signature*) kepada pengguna, dalam hal ini peranti IoT yang dijembatani oleh *management hub*. Arsitektur *KSI provider* pada sistem IAM yang diusulkan secara garis besar mengikuti arsitektur awalnya, seperti dijabarkan pada [15], tetapi dengan sedikit modifikasi. Makalah ini mengusulkan penggunaan BC sebagai media untuk menyimpan pohon *hash* dan mempublikasikan nilai dari *top hash* (*root value*). Pada tahap awal implementasi, jumlah permintaan *signing* yang masih sedikit memungkinkan untuk implementasi *agregator* dengan skala kecil. Pada *gateway*, *extender* atau yang juga bisa disebut *verifier*, bertindak sebagai asisten dalam verifikasi *signature token*, dengan cara memberikan *missing hash values* yang diperlukan klien untuk membangun pohon *hash* secara utuh.

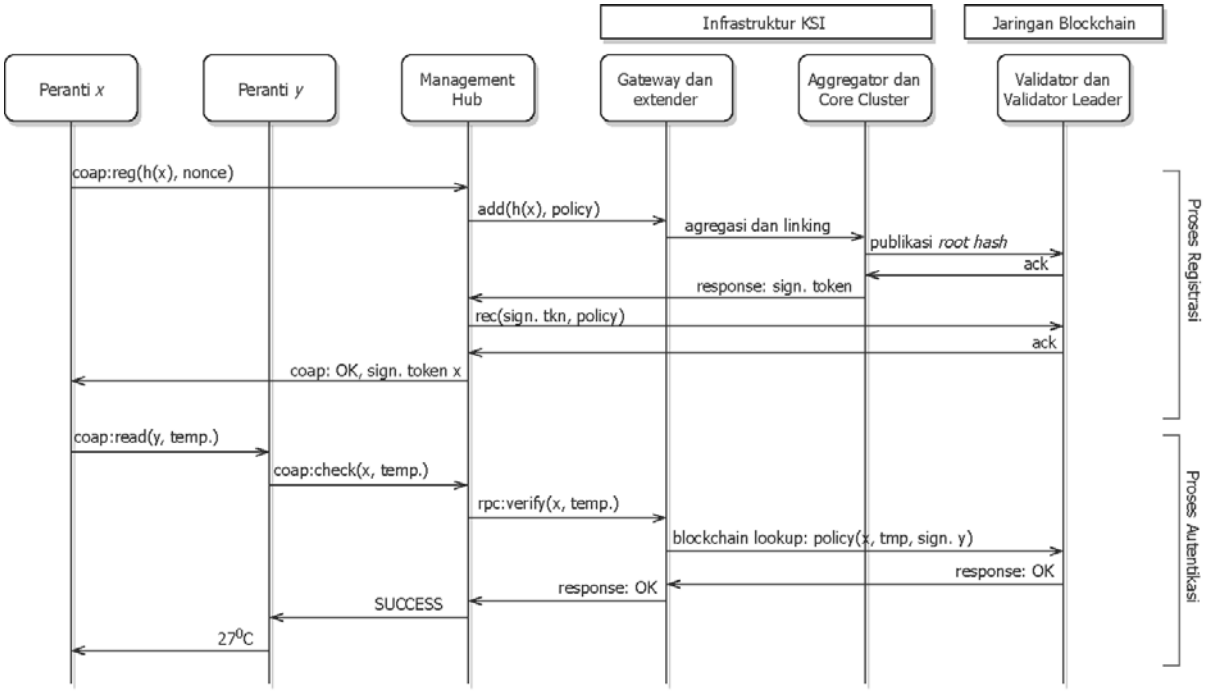
TABEL III
PERBANDINGAN DENGAN *BLOCKCHAIN* BITCOIN DAN ETHEREUM

Fitur	***Blockchain* Bitcoin**	***Blockchain* Ethereum**	***Permissioned Blockchain***
Konsensus	PoW	PoS	PBFT
Percabangan	Tidak ada	Tidak ada	dimungkinkan
Double spending	Tidak diizinkan	Tidak diizinkan	Tidak diizinkan
Enkripsi	Asimetrik	Asimetrik	Simetrik
Visibilitas *blokchain*	Publik	Publik	Privat
Diseminasi transaksi	*Broadcast*	*Broadcast*	*Broadcast*
Verifikasi terdistribusi	Semua	Semua	Tidak ada

4) Jaringan Blockchain: Salah satu komponen penting lain dalam sistem IAM yang diusulkan adalah jaringan *blockchain*. Pada sistem ini, jenis *blockchain* yang digunakan adalah *permissioned blockchain* atau yang sering juga disebut dengan *private blockchain*. Sedikit modifikasi dilakukan untuk mengakomodasi kebutuhan sistem. Perbandingan antara *permissioned blockchain* pada sistem IAM ini dengan *blockchain* pada aplikasi lain tertera pada Tabel III. *Blockchain* digunakan untuk menyimpan transaksi-transaksi yang berupa rekaman entitas yang terhubung, kebijakan akses, *top hash value* secara berkala (per detik), dan transaksi pengaksesan peranti (*log*). Untuk menjaga kecepatan penulisan atau pembuatan blok baru, jaringan *blockchain* menggunakan konsensus PBFT. *Blockchain* hanya dapat diakses oleh *KSI provider* untuk menjaga keamanan. Karena data yang disimpan ke dalam *blockchain* hanya berupa *hash value*, tidak ada data pengguna yang bocor ke dalam *blockchain*.



Gbr. 6 Arsitektur sistem *identity and access management* peranti IoT berbasis KSI dan *blockchain*.



Gbr. 7 *Sequence diagram* proses registrasi identitas baru dan verifikasi/autentikasi hak akses.

B. Alur Kerja Sistem

Pada Gbr. 7, diperlihatkan contoh *sequence diagram* yang menggambarkan cara sistem bekerja. Pada *sequence diagram* tersebut, faktor latensi tidak diperhitungkan untuk memberikan penekanan pada proses-proses dan aktor-aktor yang terlibat pada proses manajemen identitas dan akses.

Gbr. 7 memberikan contoh dua proses utama yang dilayani oleh sistem IAM yang diusulkan, yaitu registrasi identitas baru dan autentikasi atau verifikasi hak akses dari sebuah peranti. Protokol yang digunakan pada komunikasi IoT dan *management hub* menggunakan CoAP, sedangkan pada tingkat KSI dan *blockchain* menggunakan protokol yang beragam. Dicontohkan terdapat dua buah peranti IoT dan alur komunikasi antara *management hub*, infrastruktur KSI, dan jaringan *blockchain*.

Pada proses registrasi, peranti *x* mengirimkan permintaan registrasi yang disertai dengan *hash* dari identitasnya kepada *management hub* untuk kemudian diteruskan kepada infrastruktur KSI yang akan menggabungkannya dengan permintaan-permintaan lain ke dalam sebuah pohon *hash* besar. Nilai *top hash* secara berkala dipublikasikan pada *blockchain*, dan setelah dipublikasikan peranti *x* akan mendapatkan *signature token* yang bersangkutan. *Management hub* memiliki *policy* hak akses standar untuk

peranti yang baru saja melakukan registrasi. *Policy* tersebut kemudian disimpan ke dalam *blockchain* untuk nantinya dibaca jika diperlukan.

Untuk memastikan peranti yang bersangkutan (*x*) memiliki hak akses atau tidak, peranti *y* melakukan verifikasi pada sistem IAM sesaat peranti *y* menerima permintaan akses data, dalam hal ini permintaan pembacaan sensor suhu. Proses permintaan dilakukan melalui mekanisme protokol CoAP untuk kemudian ditranslasikan ke dalam sebuah RPC ke *KSI gateway*. Proses *lookup* untuk mengecek *record* yang sudah disimpan sebelumnya mengenai hak akses dilakukan oleh *KSI gateway* ke *blockchain*. Jika terdapat *policy* yang mengizinkan atas hak akses tersebut, maka *gateway* akan memberikan konfirmasi kepada *management hub* yang kemudian diteruskan kepada peranti *y*. Setelah mengetahui bahwa peranti *x* memiliki hak akses akan informasi yang diminta, peranti *y* memberikan jawaban atau respons atas permintaan pembacaan suhu yang diminta. Jika ternyata peranti atau pengguna yang melakukan permintaan tidak memiliki hak akses, maka peranti *y* menolak permintaan dari pengguna tersebut.

IV. PEMBAHASAN

Usulan dari sistem *identity and access management* dirancang untuk memiliki *scalability* yang tinggi terhadap tingkat implementasi jaringan IoT yang bisa mencapai ribuan bahkan jutaan *node* dalam sebuah jaringan. Namun demikian, terdapat beberapa hal yang dapat digarisbawahi sebagai limitasi dari sistem. IAM yang diusulkan memiliki kekebalan terdapat problem *single point of failure* di level *management hub* yang dipasang secara *redundant* dan *blockchain* yang terdesentralisasi tetapi *KSI provider* adalah satu titik yang memerlukan *backup* jika terjadi kegagalan sistem. Selain itu, pada praktiknya proses *request* dan respons dapat berjalan dengan latensi yang tinggi apabila terjadi gangguan pada kanal komunikasi. Perlu dipertimbangkan sebuah metode *caching* untuk memperkecil latensi komunikasi. Pada usulan ini, *blockchain* yang digunakan adalah *permissioned blockchain*, yaitu *blockchain* yang bersifat privat. Walaupun *blockchain* ini lebih aman dari serangan pihak luar karena tidak dapat dibaca dari luar sistem, nilai transparansi dari *blockchain* itu sendiri dinilai kurang. Idealnya sebuah jaringan *blockchain* memungkinkan publik untuk membaca dan berpartisipasi di dalamnya.

V. KESIMPULAN

Makalah ini mengusulkan implementasi KSI dan *permissioned blockchain* sebagai pendukung sistem IAM peranti IoT dalam implementasinya yang berskala masif. KSI dan *permissioned blockchain* dipilih karena karakteristiknya yang mendukung *scalability*. Sistem IAM juga dirancang untuk menyediakan layanan dengan ketersediaan yang tinggi.

Pengembangan selanjutnya dapat mempertimbangkan *data sharding* pada *blockchain* untuk membuat komunikasi dengan latensi yang lebih kecil. Selain itu, penerapan sistem *caching* juga dapat dilakukan untuk memperkecil latensi. Sebagai usaha untuk meningkatkan transparansi data, ke depannya sistem dapat dikembangkan dengan menggunakan *blockchain* publik, seperti halnya Bitcoin dan Ethereum.

REFERENSI

[1] S. Nakamoto, (2008) "Bitcoin: a peer-to-peer electronic cash system," [Online], http//www.bitcoin.org/bitcoin.pdf, tanggal akses: 13 Agt. 2018.

[2] G. Brambilla, "Peer-to-Peer Location-Based Services based on Blockchain and Web Technologies," Disertasi, Università degli Studi di Parma, Parma, Italia, Des. 2017.

[3] S. Wilkinson dan J. Lowry, "MetaDisk: Blockchain-Based Decentralized File Storage Application," Storj Labs Inc., Technical Report, hal. 1–11, 2014.

[4] S. Ibba, A. Pinna, M. Seu, dan F.E. Pani, "CitySense," *Proc. XP2017 Sci. Work. - XP '17*, 2017, hal. 1–5.

[5] X. Yue, H. Wang, D. Jin, M. Li, dan W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J. Med. Syst.*, Vol. 40, No. 10, hal. 1–8, Oct. 2016.

[6] A. Dorri, S.S. Kanhere, R. Jurdak, dan P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work*, 2017, hal. 618–623.

[7] A. Dorri, S.S. Kanhere, dan R. Jurdak, "Towards an Optimized BlockChain for IoT," *Proc. Second Int. Conf. Internet-of-Things Des. Implement. - IoTDI '17*, 2017, hal. 173–178.

[8] H. Shafagh, L. Burkhalter, A. Hithnawi, dan S. Duquennoy, "Towards Blockchain-based Auditable Storage and Sharing of IoT Data," *Proc. of the 2017 on Cloud Computing Security Workshop*, 2017, hal. 45–50.

[9] M. A. Khan dan K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Futur. Gener. Comput. Syst.*, Vol. 82, hal. 395–411, 2018.

[10] J. Bernal Bernabe, J.L. Hernandez-Ramos, and A.F. Skarmeta Gomez, "Holistic Privacy-Preserving Identity Management System for the Internet of Things," *Mob. Inf. Syst.*, Vol. 2017, hal. 1–20, 2017.

[11] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things J.*, Vol. 5, No. 2, hal. 1184–1195, 2018.

[12] M. Jakobsoson dan A. Juels, "Process of Work and Bread Pudding Protocols (Extended Abstract)," *Proc. IFIP TC6/TC11 Jt. Work. Conf. Secur. Inf. Net- Work. Commun. Multimed. Secur.*, 1999, hal. 258–272.

[13] F. Dai, Y. Shi, N. Meng, L. Wei, dan Z. Ye, "From Bitcoin to Cybersecurity: A Comparative Study of Blockchain Application and Security Issues," *2017 4th Int. Conf. Syst. Informatics, ICSAI 2017*, 2018, hal. 975–979.

[14] J.H. Lee, "BIDaaS: Blockchain Based ID As a Service," *IEEE Access*, Vol. 6, hal. 2274–2278, 2017.

[15] A. Buldas, A. Kroonmaa, dan R. Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees," *Secure IT Systems*, 2013, pp. 313–320.

[16] N. Emmadi dan H. Narumanchi, "Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure," *Proc. of the 18th International Conference on Distributed Computing and Networking - ICDCN '17*, 2017, hal. 1–6.

[17] A. Khalimonenko, J. Strohschneider, dan O. Kupreev, (2017) "DDoS Attacks in Q4 2016," [Online] https://securelist.com/ddos-attacks-in-q4-2016/77412/, tanggal akses: 13 Agt. 2018.

[18] Z. Shelby, K. Hartke, dan C. Bormann, "The Constrained Application Protocol (CoAP)," Internet Engineering Task Force, Jun. 2014.