ISSN 2303-0089
e-ISSN 2656-9949

DINAMIKA GOVERNANCE
JURNAL ILMU ADMINISTRASI NEGARA
DOI: http://ejournal.upnjatim.ac.id/index.php/jdg/article/view/3396

ADOPSI TEKNOLOGI BLOCKCHAIN DI SEKTOR PUBLIK: PELUANG PEMBENTUKAN SISTEM IDENTITAS DIGITAL NASIONAL DI ERA VUCA

Lilis Ratna Suminar[1], Alih Aji Nugroho[2]
Politeknik STIA LAN Jakarta[1,2]
lilisratnasuminar@gmail.com

ARTICLE INFORMATION

Article history:
Received date: 27 Maret 2023
Revised date: 21 April 2023
Accepted date: 23 Januari 2023

ABSTRACT

Digital identity is a community needs in the era of the Industrial Revolution 4.0 as it is now. The use of the E-KTP identity system in bureaucratic affairs has been considered less effective and efficient. Blockchain as a cutting-edge invention can be an alternative solution. This article aims to analyze the potential adoption of blockchain as a digital identity system. Researchers used descriptive research methods with a qualitative approach to analyze this potential. By looking at the condition of Indonesia's identity system and analyzing literature sources from international journals and articles, it can be said that it is time for Indonesia to need a new national digital identity system. The Ministry of Communication and Informatics is preparing a national digital identity system (E-KTP Digital) to manage the personal data of citizens in the digital world. This digital e-KTP has been integrated and verified with NIK. To support this security, the use of blockchain technology can be applied. The blockchain model that can be applied in the national digital identity system in Indonesia is the claim identity model proposed and described by Xiaohui Yang and Wenjie Li. The use of blockchain can increase the security and privacy of digital identities. The government needs to prepare a regulatory framework and its instruments.

Keywords: *E-KTP; Digital E-KTP; Digital identity system; Blockchain technology*

ABSTRAKSI

Identitas digital menjadi kebutuhan masyarakat di era Revolusi Industri 4.0 seperti sekarang. Penggunaan sistem identitas E-KTP dalam urusan birokrasi sudah dinilai kurang efektif dan efisien. *Blockchain* sebagai penemuan mutakhir bisa menjadi alternatif solusi. Artikel ini bertujuan menganalisis potensi adopsi *blockchain* sebagai sistem identitas digital. Peneliti menggunakan metode penelitian deskriptif dengan pendekatan kualitatif untuk menganalisis potensi tersebut. Dengan melihat kondisi sistem identitas Indonesia serta menganalisis sumber literatur dari jurnal dan artikel internasional, dapat dikatakan bahwa sudah saatnya Indonesia membutuhkan sistem identitas digital nasional baru. Kementerian Kominfo mempersiapkan sistem identitas digital (E-KTP Digital) nasional untuk mengelola data pribadi warga di dunia digital. E-KTP digital ini sudah terintegrasi dan terverifikasi dengan NIK. Untuk mendukung keamanan tersebut, penggunaan teknologi *blockchain* bisa diterapkan. Model *blockchain* yang bisa diterapkan di dalam sistem identitas digital nasional di Indonesia adalah model identitas klaim yang diusulkan dan dijelaskan oleh Xiaohui Yang dan Wenjie Li. Penggunaan *blockchain* dapat meningkatkan keamanan dan privasi dari identitas digital. Pemerintah perlu menyiapkan kerangka regulasi dan perangkatnya.

Kata Kunci: E-KTP; E-KTP digital; Sistem identitas digital; Teknologi *blockchain*

PENDAHULUAN

Dewasa ini adopsi teknologi informasi di sektor publik masih dilakukan. Menurut kajian *International Telecommunication Union* (ITU) dengan judul *"Digital Life Internet Report"* menyatakan bahwa teknologi digital sentral (misalnya telekomunikasi, penyiaran, dan komputasi) telah menjadi bagian dari kehidupan sehari-hari bagi orang-orang di seluruh dunia (Middleton, 2007). Artinya, kehidupan seseorang pada zaman sekarang sudah sangat melekat dengan dunia digital. Selain itu, era VUCA yang entitasnya semakin kuat juga telah membuat teknologi menjadi semakin canggih dengan perubahan yang cepat. Istilah VUCA sendiri merupakan singkatan dari empat (4) kata yang menggambarkan suatu keadaan yang saat ini kita hadapi yaitu, *Volatility, Uncertainty, Complexity,* dan *Ambiguity* (LAN RI, 2022).

Permasalahan kebijakan muncul akibat dari data identitas yang tidak valid (Yona et al., 2021). Pada kebijakan jaring pengaman penanggulangan COVID-19 contohnya, kebijakan tidak tepat sasaran karena data masyarakat tidak *update* (Aji Nugroho & Fitri Azmi, 2021). Adanya fenomena-fenomena tersebut menjadi alasan dibutuhkannya identitas digital. Istilah identitas digital ini muncul seiring dengan terjadinya evolusi internet yang memungkinkan bagi pengguna internet untuk membagikan identitas digital mereka dengan orang lain guna memperkuat keberadaan mereka. Philip Windley menjelaskan di dalam bukunya yang berjudul *"Digital Identity"* bahwa identitas digital berisi data yang secara unik mendeskripsikan seseorang atau benda, dan juga berisi informasi tentang hubungan subjek dengan entitas lain (Windley, 2023). Di samping itu, identitas digital ini juga berkaitan dengan mekanisme yang menjadi pusat dari sistem modern, jaringan, serta aplikasi dengan sistem keamanannya.

Identitas digital sering kali diartikan sebagai suatu identitas *online* atau jaringan yang diadopsi di dunia maya oleh individu, organisasi, atau perangkat elektronik. Pengguna identitas digital ini juga dapat memproyeksikan lebih dari satu identitas digital melalui beberapa komunitas. Dalam hal manajemen sistem identitas digital, yang menjadi fokus utamanya ialah keamanan dan privasi dari para pengguna (Techopedia, 2021).

Seperti identitas manusia di kehidupan nyata yang menyajikan informasi personal, dalam identitas digital ini juga disajikan beberapa informasi personal dari penggunanya seperti nama pengguna dan kata sandi, foto, sidik jari, jenis kelamin, alamat, tanggal lahir, nomor KTP, aktivitas pencarian *online* (seperti transaksi elektronik), riwayat kesehatan, riwayat atau perilaku pembelian, riwayat pendapatan, bukti kelayakan untuk mengakses layanan *online*, dan lain sebagainya (NZ Digital government, 2022). Potongan informasi ini dikenal sebagai atribut. Meskipun sama-sama menyajikan informasi personal, tetapi sistem identitas digital lebih lengkap dalam menyajikan data dan fungsinya lebih banyak. Hal ini dikarenakan dalam identitas digital ditautkan ke satu atau lebih identitas digital lainnya seperti alamat *email*, URL, atau nama domain (Rathee & Singh, 2022).

Layanan identitas digital bergantung pada hubungan antara pengguna *(user)* dengan penyedia layanan *(provider)*, sebagai bagian dari sistem identitas digital. Identitas digital tersebut pada umumnya digunakan sebagai sarana untuk mengidentifikasi diri mereka (pengguna) di dunia digital (NZ Digital government, 2022). Data yang diperlukan tentang seseorang akan disimpan dalam sistem komputer, atau saat ini disimpan di *blockchain*, yang nantinya dapat dikaitkan dengan identitas kedaulatan, sipil, atau kewarganegaraan mereka. Tujuan dari identitas digital itu sendiri untuk menciptakan tingkat kepercayaan yang sama atau sebanding seperti yang dihasilkan oleh kegiatan transaksi secara tatap muka.

Teknologi *blockchain* memiliki sebuah teknologi buku besar terdistribusi yang tidak mudah rusak, dan siapa pun dapat meng-*host* buku besar tersebut dan mencatat segala kegiatan transaksi secara permanen (Yang & Li, 2020). Oleh karena itu, teknologi *blockchain* ini memiliki potensi yang besar jika digunakan dalam proses pembentukan sistem identitas digital di Indonesia. Penerapan *blockchain* dalam pembentukan sistem identitas digital ini dapat menjadi salah satu perwujudan dari implementasi konsep *Smart City* di Indonesia.

Smart City atau kota cerdas didefinisikan sebagai sebuah konsep pengembangan dan pengelolaan kota dengan pemanfaatan Teknologi Informasi dan Komunikasi (TIK) untuk menghubungkan, memonitor, dan mengendalikan berbagai sumber daya yang ada didalam kota dengan lebih efektif dan efisien untuk

memaksimalkan pelayanan kepada warganya serta mendukung pembangunan yang berkelanjutan (Wahyudi et al., 2022). Buku besar terdistribusi dan mekanisme konsensus antar-*node* dimanfaatkan untuk membentuk sistem identitas digital yang terdistribusi dan tepercaya di lingkungan yang tidak terpercaya. Sehingga segala proses dapat dilakukan dengan mudah dan aman, mulai dari pendaftaran, autentikasi, otorisasi, hingga pembatalan yang memungkinkan pengguna mengelola identitas mereka tanpa bergantung pada pihak ketiga.

Dalam penelitian yang yang membahas tentang *Digital identity – From emergent legal concept to new reality* menunjukkan bahwa identitas digital telah membuka domain siber baru untuk nasional, perdagangan internasional, serta cara-cara baru dalam bertransaksi (Sullivan, 2018). Identitas digital ini diklaim tetap bersifat revolusioner dan menjadi sebuah inovasi terbaru yang cakupannya sangat luas hingga ke program internasional. Inovasi teknologi ini penggunaannya lebih luas dari teknologi *blockchain* perihal autentikasi dan verifikasi identitas untuk perdagangan modern yang diatur. Sehingga hal tersebut menimbulkan masalah baru yang menantang untuk supremasi hukum, tata kelola, serta untuk keamanan nasional maupun internasional. Sullivan (2018) juga menyatakan bahwa identitas digital sekarang menimbulkan implikasi yang belum pernah terjadi sebelumnya untuk perdagangan, keamanan, pertahanan, hukum internasional dan norma-norma hukum. Hal tersebut disebabkan oleh pembongkaran batas-batas geografis dan konsep tradisional imigrasi, tempat tinggal, dan kewarganegaraan yang berdasarkan pada kelahiran dan/atau kehadiran fisik.

Dalam penelitian yang berjudul *Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India* menunjukkan bahwa secara umum identitas digital memiliki kapasitas untuk kebahagiaan dan kesengsaraan (Mir et al., 2020). Sistem identitas digital yang terencana dengan baik, memiliki langkah-langkah yang diperlukan untuk dapat mengatasi masalah-masalah seperti keamanan, privasi, inklusi, dan pemberdayaan warga yang dapat mengembangkan nilai-nilai ekonomi yang luar biasa. Dalam penelitian tersebut, mereka melakukan studi terperinci untuk mengidentifikasi tujuan utama yang harus dimiliki oleh sebuah sistem identifikasi biometrik apa pun.

Program identifikasi biometrik India yang disebut dengan *Aadhaar* ini telah digunakan sebagai studi kasus dan telah dianalisis dari perspektif *Design Theory* (DT) dalam penelitian tersebut. Setelah memprioritaskan tujuan desain *Aadhaar* menggunakan Metode *Best-Worst* dan diverifikasi menggunakan *Total Interpretive Structural Modeling* (TISM) dan *Matrix of Cross Impact Multiplications Applied to Classification* (MICMAC), diamati bahwa tiga kelompok tujuan tersebut terbentuk. Ketiga cluster tersebut sangat penting untuk setiap program identifikasi biometrik tetapi dengan prioritas yang berbeda-beda. Karena penelitian tersebut terbatas hanya pada satu studi kasus yaitu tentang *Aadhaar*, maka mereka tidak bisa mengklaim prioritas tujuan sebagai prioritas mutlak.

Oleh karena itu, Mir et al., (2020) menyatakan bahwa arah penelitian yang akan dilakukan di masa yang akan datang adalah untuk memverifikasi tujuan yang diprioritaskan pada beberapa sistem identifikasi biometrik lainnya yang akan ada nantinya dan menggunakan hasil prioritas dalam merancang sistem identifikasi biometrik di dunia nyata. Selain itu, keamanan dan privasi juga telah muncul sebagai tujuan terpenting kedua dalam penelitian mereka. Namun, sering terjadi keluhan terkait keamanan dan privasi *Aadhaar* menunjukkan bahwa masih ada yang kurang. Hal tersebut dianggap sebagai kesenjangan yang bisa menjadi area lain yang menarik untuk dibahas lebih lanjut.

Tujuan dari artikel ini untuk mengetahui bagaimana potensi penggunaan teknologi *blockchain* bisa menjadi faktor pendukung dalam pembentukan sistem identitas digital nasional di Indonesia. Selain itu, artikel ini diharapkan memantik pendiskusian tentang penggunaan teknologi *blockchain* dan sistem identitas digital.

METODE PENELITIAN

Dalam penulisan artikel ini, peneliti menggunakan metode penelitian pendekatan deskriptif kualitatif dengan menganalisis referensi di internet yang membahas tentang sistem identitias digital, teknologi *blockchain*, sistem identitas nasional di Indonesia saat ini yang kemudian dianalisis dan dinarasikan.

Sumber data dalam penelitian ini ialah data sekunder yang berasal dari jurnal, buku, artikel, penelitian terdahulu, berita-berita di internet, dan dokumen resmi negara seperti Undang-Undang, Peraturan Presiden, dan Surat Edaran Menteri.

Sumber data sekunder yang telah dikumpulkan, dianalisis dan ditriangulasi dengan literatur yang ada. Penelitian dilakukan antara Maret sampai Mei 2022.

HASIL DAN PEMBAHASAN

Sistem Identitas Nasional di Indonesia saat ini

Gambar 1. E-KTP.
(Sumber: Adi & Hendra, 2016)

Sampai saat ini, di Indonesia masih belum memiliki sistem identitas yang canggih dan modern untuk warganya. Sistem identitas yang digunakan saat ini oleh warga Indonesia adalah E-KTP atau KTP Elektronik (Gambar 1), dijelaskan menurut UU No. 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan pada pasal 1 ayat (14) bahwa "KTP Elektronik adalah Kartu Tanda Penduduk yang dilengkapi cip yang merupakan identitas resmi penduduk sebagai bukti diri yang diterbitkan oleh Instansi Pelaksana". Selain itu juga, E-KTP ini diklaim memiliki sistem keamanan atau pengendalian baik dari aspek administrasi maupun teknologi informasinya yang berbasis pada database kependudukan nasional.

Informasi personal yang disajikan dalam E-KTP ini seperti NIK, nama, tempat dan tanggal lahir, alamat, agama, status perkawinan, pekerjaan, kewarganegaraan, masa berlaku E-KTP, pas foto, serta dilengkapi karakteristik biometrik dengan sidik jari yang digunakan untuk verifikasi dan validasi sistem. Sidik jari tersebut terkandung di dalam cip E-KTP. Cip yang terkandung di dalam E-KTP tersebut memiliki fungsi sebagai alat penyimpan data elektronik penduduk, kemudian data tersebut diklaim bisa dibaca secara elektronik dengan *card reader*, serta data yang tersimpan di dalam E-KTP telah dienskripsi dengan algoritma kriptografi tertentu.

E-KTP ini memiliki kelebihan dan kekurangan, kelebihan yang dimiliki di antaranya setiap kartu mengandung cip untuk menyimpan data, serta E-KTP ini berlaku secara nasional maupun internasional. Sedangkan yang menjadi kekurangannya yaitu jika cip yang terkandung mengalami kerusakan maka E-KTP menjadi tidak berlaku lagi. Kemudian jika terjadi kesalahan dalam memasukkan data maka akan memakan waktu lama untuk membuat ulang atau merevisi data pada E-KTP, hal ini dikarenakan di kelurahan masih belum memiliki alat canggih untuk merevisi E-KTP tersebut dengan cepat. Dan juga meskipun E-KTP ini memiliki cip di dalamnya, tetapi tetap saja masih sering terjadi pencurian, penduplikatkan, pemalsuan, penjualan, dan penyalahgunaan data E-KTP. Hal ini menunjukkan bahwa sistem keamanan pada E-KTP ini masih lemah karena masih bisa ditembus oleh penjahat.

Selain itu, sistem E-KTP ini bukan tipe kartu identitas yang multifungsi karena masih belum terintegrasi dengan layanan publik lainnya seperti SIM, asuransi, pajak, transportasi, transaksi di perbankan, dan lain sebagainya. Kemudian dilaporkan pada tahun 2017, pembuatan E-KTP yang merupakan sebuah mega proyek negara ini memakan biaya APBN yang sangat besar hampir mencapai Rp6 triliun (Fadhil & Atriana, 2017). Di sisi lain, selain sebagai identitas jati diri warga negara, seperti yang disinggung di atas bahwa E-KTP ini berlaku secara nasional sehingga akan memudahkan warga negara dalam menerima pelayanan baik dari lembaga pemerintah maupun swasta.

Namun pada kenyataannya, meskipun di dalam E-KTP sudah mengandung sebuah cip, tetapi dalam penggunaannya di kehidupan sehari-hari masih konvensional. Fungsi dari teknologi E-KTP ini masih belum secanggih namanya. Dalam urusan birokrasi, warga Indonesia sering kali masih harus melakukan fotokopi E-KTP tersebut. Hal ini dikarenakan, masih banyak instansi pemerintah atau swasta di Indonesia yang belum bisa memanfaatkan digitalisasi dari teknologi E-KTP ini dengan semestinya. Kemudian masih banyak juga dari mereka yang belum menyediakan alat seperti *card reader,* sehingga fungsi cip pada E-KTP pun menjadi sia-sia.

Padahal sudah ada peraturan yang jelas mengatur hal tersebut, yaitu dijelaskan di dalam PERPRES No. 67 Tahun 2011 tentang Perubahan Kedua Atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional pada pasal 10 C ayat (1) bahwa "Instansi Pemerintah, Pemerintah Daerah, Lembaga Perbankan, dan Swasta wajib menyiapkan kelengkapan teknis yang diperlukan berkaitan dengan penerapan KTP Elektronik" dan ayat (2) bahwa "Kelengkapan teknis yang diperlukan sebagaimana dimaksud pada ayat (1) terdiri dari dan tidak terbatas pada pembaca kartu pintar, pemindai sidik jari dan aplikasi pembaca KTP Elektronik".

Di samping itu juga, sudah terdapat peraturan yang melarang untuk memfotokopi E-KTP terlalu sering (Redaksi Majalah ICT, 2022). Hal ini dijelaskan di dalam SE Mendagri Nomor 471.13/1826/SJ tentang Pemanfaatan E-KTP Dengan Menggunakan *Card Reader* bahwa "E-KTP tidak diperbolehkan untuk difotokopi, distapler, dan perlakuan lainnya yang merusak fisik dari E-KTP, sebagai gantinya dicatat NIK dan Nama Lengkap".

Melihat hal tersebut dapat disimpulkan bahwa yang menjadi permasalahan di sini adalah masih banyak instansi atau lembaga swasta yang tidak mematuhi peraturan di atas. Dan juga pemerintah kurang memperhatikan permasalahan ini dengan memberikan sanksi yang tegas kepada para pelanggar. Padahal jika semua instansi pemerintah atau lembaga swasta mematuhi peraturan tersebut, maka prosesnya akan jauh lebih mudah karena semua data akan langsung terbaca di komputer jadi mereka tidak perlu lagi meminta fotokopi E-KTP kepada si penerima layanan.

Jadi pada intinya adalah secanggih apa pun teknologi di Indonesia akan tetap menjadi sia-sia, jika SDM yang ada khususnya para pelayan publik tidak mau berusaha untuk mempelajari dan menerapkan digitalisasi ini. Sehingga fungsi dari adanya teknologi tersebut tidak dimanfaatkan dengan baik, dan hal inilah yang menjadi salah satu faktor penghambat kemajuan birokrasi di Indonesia.

Permasalahan seperti yang dijelaskan di atas menjadi urgensi dibutuhkannya pembentukan sistem identitas digital nasional di Indonesia yang lebih canggih. Untuk mengatasi permasalahan di atas, Indonesia harus mulai membentuk sistem identitas digital nasional yang hanya menghasilkan satu kartu saja, tetapi kartu tersebut memiliki banyak fungsi. Penyederhanaan kartu ini dilakukan agar warga Indonesia bisa menerima pelayanan baik dari pemerintah maupun swasta tanpa perlu repot untuk membawa banyak kartu (Angga et al., 2019). Karena tiap otoritas atau lembaga mengeluarkan kartu mereka masing-masing, misalnya E-KTP, kartu ATM, kartu transportasi, kartu asuransi kesehatan, kartu asuransi ketenagakerjaan, dan masih banyak lagi.

Gambar 2. Kartu Identitas Digital di Negara Estonia. (Sumber: Stephanie & Nistanto, 2021)

Seperti kartu identitas digital yang dimiliki oleh Warga Negara Estonia (Gambar 2), mereka hanya memiliki satu kartu identitas digital yang fungsinya telah mencakup ke berbagai aspek. Hal ini dikarenakan, seluruh sistem telah tergabung ke dalam *e-service* yang keamanannya sangat terjamin. Di Estonia, warganya hanya butuh satu kartu saja tetapi sudah mencakup KTP, pajak, tanda tangan digital, *login bank,* asuransi, rekam medis, menebus resep obat dari dokter, *i-voting*, bahkan identitas untuk bepergian di UE (Stephanie & Nistanto, 2021).

Pembentukan Sistem Identitas Digital Nasional di Indonesia

Di samping permasalahan di atas, ada beberapa alasan lain yang membuat dibutuhkannya pembentukan sistem identitas digital nasional di Indonesia. Alasan berikut ini disampaikan oleh Mariam F. Barat selaku Direktur Tata Kelola Aplikasi Informasi, Kementerian Kominfo RI (Gobel, 2020) sebagai berikut:

1. dengan adanya sistem identitas digital nasional dapat membangun kepercayaan dalam ekonomi digital. Hal ini dikarenakan adanya penguatan data pribadi serta baik warga, swasta, maupun

pemerintah dapat melakukan transaksi dengan sistem keamanan yang terjaga;
2. sistem identitas digital nasional ini juga dapat mengurangi terjadinya penipuan. Berdasarkan pada studi LexisNexis (2019), penipuan yang terjadi di Indonesia telah menimbulkan kerugian hingga mencapai 1,66 persen dari pendapatan perusahaan. Yang di mana menurut 62 persen responden, penyebab utama dari penipuan tersebut adalah masalah pada verifikasi identitas;
3. sistem identitas digital nasional ini akan memberikan kemudahan dalam bisnis. Perizinan usaha akan semakin mudah untuk dilakukan karena transaksi dilakukan tanpa tatap muka dan tidak lagi dibutukan dokumen dalam bentuk fisik;
4. adanya sistem identitas digital nasional ini juga akan membuat terjadinya penghematan biaya. Hal ini dikarenakan nantinya akan ada efisiensi pengelolaan dokumen dan otomasi yang kemudian dapat mengurangi risiko terjadinya penipuan serta mendorong penghematan biaya;
5. seiring adanya sistem identitas digital nasional membuat perekonomian ikut tumbuh dengan baik. Hal tersebut dapat terjadi karena di sektor ekonomi akan ada banyak potensi dan peluang baru dari identitas digital tersebut. Hal ini juga didukung dengan perkiraan yang dilakukan oleh *McKinsey Global Institute* yang menyatakan bahwa dengan adanya identitas digital ini, kontribusi pertumbuhan GDP dapat mencapai 3 sampai 13 persen di tahun 2030; dan
6. sistem identitas digital nasional ini juga akan mendukung penyelenggaraan pelayanan publik yang inklusif. Nantinya baik pemerintah maupun swasta bisa memberikan pelayanan secara lebih luas dan lebih tersentuh ke warga, dan warga pun juga bisa mengakses layanan di mana saja.

Selain penjelasan di atas, adanya sistem identitas digital ini membuat proses pendaftaran yang dilakukan oleh warga dalam suatu platform menjadi lebih mudah dan praktis. Jadi setiap masuk ke ruang digital tidak perlu mengisi formulir data pribadi lagi, karena data yang sudah ada sebelumnya langsung tersimpan ke sistem. Kemudian, sistem identitas digital juga dinilai bisa mengurangi terjadinya potensi pemalsuan identitas. Karena ada beberapa langkah yang harus dipenuhi untuk bisa memverifikasi identitas digital seseorang seperti kode unik perangkat, kata sandi, karakteristik biometrik seperti sidik jari, sampai pola perilaku dari orang tersebut (Prihadi, 2017).

Baru-baru ini, terdapat kabar baik yang disampaikan oleh Semuel Abrijani Pangerapan selaku Direktur Jenderal Aplikasi Informatika (APTIKA) Kementerian Kominfo bahwa saat ini Kementerian Kominfo sedang mempersiapkan sistem identitas digital nasional untuk mengelola data pribadi warga di dunia digital (Jemadu & Prastya, 2022). Dengan begitu, nantinya data warga dalam menggunakan platform digital dapat teridentifikasi.

Alih-alih membuat sistem identitas digital nasional yang baru, rencana pemerintah tersebut lebih mengarah ke pembaruan E-KTP biasa menjadi E-KTP digital. E-KTP digital inilah yang akan menjadi sistem identitas digital nasional bagi warga Indonesia. Kemudian yang menjadi pertanyaannya adalah pembaruan seperti apa yang terjadi di dalam E-KTP digital, berikut ini penjelasannya:

1. nantinya E-KTP digital ini akan dikeluarkan dalam bentuk sebuah aplikasi identitas yang bernama Digital ID. Dengan melakukan *scan QR code*, identitas diri seseorang akan langsung tertampil di layar *gadget*. Informasi data diri yang ditampilkan juga sama seperti yang ada di E-KTP biasa;
2. selain berisikan identitas pribadi, data lain yang terintegrasi dan terverifikasi dengan NIK juga akan termuat di dalam E-KTP digital ini. Seperti KK, NPWP, SIM, STNK, Kartu Vaksin *Covid-19*, dan lainnya. Dengan dilakukan penyederhanaan kartu ini, warga Indonesia bisa menerima pelayanan baik dari pemerintah maupun swasta tanpa perlu repot untuk membawa berkas fisik atau banyak kartu yang berisiko hilang;
3. E-KTP digital juga dapat digunakan untuk keperluan administrasi yang membutuhkan KTP, KK, atau semacamnya. Sehingga warga tidak perlu repot untuk membawa fotokopi berkas tersebut, karena nantinya hanya perlu melakukan *scan QR code* dan data-data yang dibutuhkan akan langsung tertampil di komputer; dan
4. Bagi warga yang ingin membuat E-KTP digital, diharuskan untuk mengunduh aplikasi yang ada di *Google Play Store* untuk pengguna *android* dan *App Store* untuk pengguna *Apple*. Maka dari

itu, warga perlu mempunyai *gadget* yang terhubung ke dalam jaringan internet untuk mengunduh dan mengoperasikan aplikasi tersebut. Bagi warga yang tidak punya *gadget,* nantinya Kemendagri tetap akan menerbitkan E-KTP biasa dalam bentuk fisik.

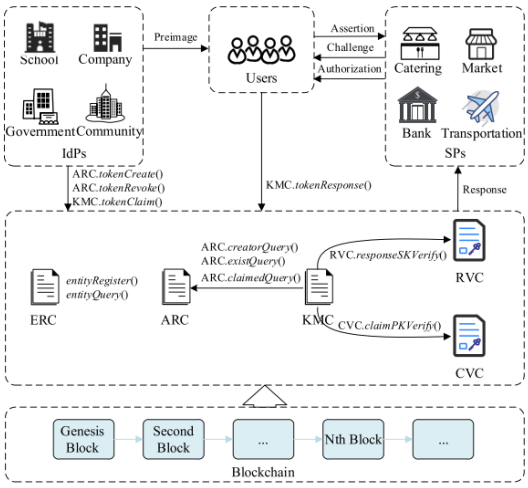
Setelah mengunduh aplikasi Digital ID, terdapat tiga tahap yang perlu dipenuhi untuk memiliki identitas digital (Hardiansyah et al., 2022) yaitu:

1. setelah membuka aplikasi, warga perlu memasukkan NIK, alamat *email*, dan nomor *handphone* yang aktif;
2. setelah itu, melakukan verifikasi wajah; dan
3. terakhir adalah melakukan verifikasi *email.*

Dalam pembentukan sistem identitas digital nasional tersebut diperlukan adanya sistem keamanan yang terjamin sehingga data warga Indonesia tidak akan bocor dan disalahgunakan, serta privasi pengguna tetap terjaga. Untuk mendukung keamanan tersebut, dibutuhkan penggunaan teknologi *blockchain*. Model *blockchain* yang bisa diterapkan di dalam sistem identitas digital nasional di Indonesia adalah model identitas klaim yang diusulkan dan dijelaskan oleh (Yang & Li, 2020) yaitu sistem manajemen identitas digital (BZDIMS) berbasis *blockchain* dan *Zero-knowledge proof* (ZKP) dengan bantuan *ZeroKnowledge Succinct Non-interactive ARguments of Knowledge* (zk-SNARK) dan *Ethereum*.

Penerapan sistem manajemen identitas digital yang bernama BZDIMS ini bertujuan untuk mencapai siklus hidup atribut privasi yang lengkap. Manajemen atribut yang efisien dan berjaringan halus dalam BZDIMS ini memberikan dasar yang baik untuk mekanisme keamanan lainnya. Sedangkan ZKP sendiri merupakan sebuah teknik kriptografi yang berarti bahwa pembukti *(the prover)* dapat meyakinkan pemeriksa *(the verifier)* bahwa suatu pernyataan tertentu adalah benar tanpa memberikan keterangan tambahan apapun kepada pemeriksa atau membocorkan keterangan apapun tentang saksi *(witness).* Kemudian penggunaan zk-SNARK di sini untuk memperoleh privasi di *blockchain* karena perhitungannya yang minim untuk verifikasi dan bukti yang ringkas.

Dengan zk-SNARK inilah nantinya pembukti dapat meyakinkan pemeriksa bahwa mereka telah melakukan perhitungan dengan benar pada sekumpulan input data tanpa mengungkapkan beberapa input tersebut. Dan informasi yang diperlukan untuk verifikasi jauh lebih kecil daripada perhitungan. Secara keseluruhan, zk-SNARK ini memungkinkan untuk memperoleh desain transfer kepemilikan atribut secara pribadi di *blockchain* publik dengan *overhead* komputasi yang minimal. Lalu, di sini *Ethereum* telah merancang *Ethereum Virtual Machine* (EVM) Turing-lengkap untuk mengimplementasikan fungsi kontrak pintar *(smart contracts)* dan memungkinkan pengembang *(developers)* untuk mengembangkan kontrak pintar dengan menggunakan *high-level language Solidity.*



Gambar 3. Model Sistem.
(Sumber: Yang & Li, 2020)

Di dalam model sistem yang diusulkan (Gambar 3), terdapat tiga entitas dalam skema tersebut yaitu:

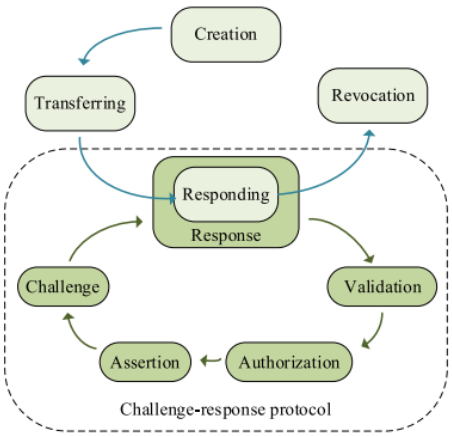
1. penyedia identitas *(Identity Provider/IdP)* bertanggung jawab untuk menerbitkan dan mencabut atribut privasi, serta mengeluarkan klaim *hash* yang dapat diverifikasi;
2. penyedia layanan *(Service providers/SP)* bertanggung jawab untuk menyediakan layanan *online* atau *offline* yang kebijakan aksesnya berisi persyaratan untuk atribut dan memvalidasi profil yang disediakan oleh pengguna; dan
3. pengguna *(User)* memiliki atribut identitas yang disimpan di *blockchain*, serta mengakses layanan dari IdP dengan membuktikan kepemilikan atas pengenal atau identitas dan atributnya.

Dan penjelasan siklus dari model sistem di atas seperti ini:

1. atribut privasi diabstraksikan sebagai token. Selain itu, lima kontrak pintar dikembangkan

untuk mencapai siklus hidup atribut privasi yang lengkap termasuk *Entity Register Contract* (ERC), *Attribute Repository Contract* (ARC), *Knowledge Management Contract* (KMC), *claimPK Verify Contract* (CVC) dan *responseSK Verify Contract* (RVC);

2. ERC menyediakan entitas *interface entityRegister()* untuk entitas guna mendaftarkan kunci publik dan *interface entityQuery()* untuk menanyakan informasi kunci publik entitas. Selain itu, ada empat fungsi yang dirancang untuk dipanggil oleh entitas guna mengelola atribut yaitu *ARC.tokenCreate(), ARC.tokenRevoke(), KMC.tokenClaim(), dan KMC.tokenResponse()*. Yang hubungan pemanggilan keempat fungsi antarkontrak tersebut seperti yang ditunjukkan (Gambar 3), yang mana KMC di sini akan memanggil fungsi-fungsi di ARC, RVC, dan CVC untuk mengelola atribut yang ada;
3. selain itu, karena ZoKrates tidak dapat secara langsung memperoleh kunci publik dari kunci pribadi *Ethereum* berdasarkan secp256k1, Xiaohui Yang dan Wenjie Li menggunakan sha256 di pustaka standar ZoKrates, bukan secp256k1. Mereka mendefinisikan pasangan kunci yang dihasilkan oleh sha256 sebagai pasangan kunci ZK, yang di mana kunci publik ZK tersebut akan disertakan dalam gambar awal klaim *hash*, dan kunci pribadi ZK perlu disimpan dengan benar; dan
4. Sebelum solusi berjalan, BZDIMS perlu menerapkan kontrak pintar dan menjalankan fase penyiapan zk-SNARK untuk membagikan kunci pembuktian ke semua. Entitas perlu mendaftarkan kunci publik ZK mereka dengan alamat *blockchain* di ERC.



Gambar 4. Empat prosedur BZDIMS dan protokol tantangan-tanggapan.
(Sumber: Yang & Li, 2020)

Seperti yang ditunjukkan (Gambar 4), protokol tantangan-tanggapan terdiri dari lima langkah, dan siklus hidup atribut privasi yang lengkap meliputi empat prosedur berikut:

1. penciptaan *(creation)* merupakan sebuah langkah awal di mana token atribut privasi yang berisi pasangan nama-nilai diterbitkan oleh IdP dan ERC yang kemudian akan mencatat alamat si pencipta *(creator's address)* sebagai pengesahan atribut;
2. mentransfer *(transferring)* dilakukan untuk mentransfer kepemilikan atribut privasi kepada pengguna di *blockchain* secara diam-diam, IdP perlu mengeluarkan klaim *hash* pada token ini dan membuktikan bahwa ia melakukan perhitungan tertentu yang disebut dengan *claimPK* bahwa klaim *hash* telah di-*hash* dari pengidentifikasi token dan kunci publik pengguna ZK oleh ZKP;
3. menanggapi *(responding)* dilakukan untuk mendemonstrasikan kepemilikan token atribut privasi, karenanya pengguna perlu membuktikan kepemilikan atas kunci pribadi ZK yang sesuai dengan kunci publik ZK yang terkandung dalam gambar awal klaim *hash*. Perhitungan khusus yang dilakukan oleh pengguna selama proses ini disebut dengan *responseSK*. Langkah ini juga merupakan bagian dari protokol tantangan-tanggapan; dan
4. pembatalan *(revocation)* ini merupakan proses pembatalan yang memungkinkan IdP untuk memblokir respons atribut dengan memodifikasi bidang keberadaan token.

Di sisi lain, melihat penjelasan tentang pembentukan sistem identitas digital nasional di Indonesia dengan menggunakan teknologi *blockchain*, peneliti dapat melihat adanya tantangan atau permasalahan yang dimiliki Indonesia untuk mengaplikasikan teknologi tersebut yaitu mulai dari yang paling dasar permasalahan SDM. Di Indonesia sendiri, jumlah SDM yang berkompeten atau ahli di bidang TIK termasuk penguasaan teknologi *blockchain* ini masih sangat terbatas. Hal ini dikarenakan masih kurangnya edukasi atau pengenalan tentang teknologi *blockchain* kepada masyarakat luas khususnya pelajar di Indonesia. Seharusnya pemerintah Indonesia sudah mulai menggencarkan

edukasi tentang konsep *blockchain* ini mulai dari bangku SMP atau SMA.

Karena melihat teknologi *blockchain* ini memiliki manfaat yang luar biasa dan jika diaplikasikan dengan benar akan mempermudah segala kegiatan birokrasi di Indonesia. Di sisi lain, dengan semakin canggihnya teknologi yang ada di dunia ini membuat Indonesia mau tidak mau harus mengikuti perkembangan yang ada. Jika warga Indonesia tidak bisa menguasai teknologi, maka akan dipastikan Indonesia tertinggal dengan negara-negara lainnya. Oleh karena itu perlu untuk melakukan edukasi seputar penguasaan teknologi, agar warga Indonesia bisa melek teknologi dan bisa bersaing dengan negara lain.

Kemudian yang menjadi tantangan selanjutnya adalah meskipun teknologi *blockchain* dapat menghemat biaya transaksi, tetapi untuk mengkustom sistem *blockchain* ini memerlukan biaya yang besar. Hal ini sejalan dengan permasalahan sebelumnya yaitu keterbatasan tenaga ahli di bidang teknologi *blockchain* dan teknologi pendukung dalam proses kustomisasi *blockchain.* Dan juga jikalau pun teknologi *blockchain* ini berhasil digunakan dalam sistem identitas digital nasional, itu belum bisa menjamin seluruh warga Indonesia bisa mengaksesnya. Mengingat jaringan internet yang ada di Indonesia masih belum menjangkau secara merata ke seluruh penjuru negeri. Jadi peneliti yakin hanya di kota-kota besar, teknologi tersebut dapat dimanfaatkan secara maksimal. Hal tersebut sejalan dengan rencana E-KTP digital miliki pemerintah yang nantinya hanya bisa diakses melalui aplikasi di *gadget* yang terhubung ke jaringan internet.

Dan permasalahan terakhir adalah sistem keamanan data di Indonesia masih mudah untuk diretas oleh *hacker*. Walaupun teknologi *blockchain* ini memberikan jaminan keamanan, tetap saja Indonesia masih belum memiliki tingkat keamanan data yang baik. Hal ini ditunjukkan dengan banyaknya kasus kebocoran data pribadi di Indonesia, seperti terjadinya peretasan data warga Indonesia sebanyak 2,3 juta yang berhasil diretas dari penyimpanan data lembaga KPU. Informasi data tersebut terdiri dari nama, alamat, tanggal lahir, NIK, NKK, dan lain sebagainya. Kebocoran data milik KPU ini diduga berasal dari data 2013 hingga 2021. Di samping karena lemahnya sistem keamanan Indonesia, sebesar 54% kebocoran data yang terjadi di Indonesia itu disebabkan oleh *human error, system error,* maupun serangan *malware* dan *hacker*. Kejadian seperti pencurian, kebocoran, penjualan data yang terjadi di Indonesia menunjukkan bahwa saat ini Indonesia telah memasuki kondisi darurat kebocoran data pribadi.

Tentu saja permasalahan tersebut harus segera diatasi oleh pemerintah dengan memberlakukan pengujian sistem dan tes simulasi serangan *cyber crime* secara berkala bagi sistem milik lembaga pemerintah maupun swasta. Di samping itu juga, diperlukan adanya payung hukum yang benar-benar tegas dalam melindungi data pribadi. Kabar baiknya adalah mulai dari tahun 2019 sedang dibahas RUU Perlindungan Data Pribadi (PDP) di DPR, tetapi sampai tahun 2022 RUU PDP tersebut masih belum disahkan. Untuk itu pemerintah harus segera mengesahkan RUU PDP tersebut agar pengamanan data pribadi milik warga Indonesia bisa menjadi lebih aman dan ke depannya kebocoran data tidak akan terulang lagi (Veratika, 2021).

KESIMPULAN

Melihat banyaknya permasalahan yang ada pada penerapan E-KTP di Indonesia ini membuat pemerintah harus segera mengatasinya dengan membentuk sistem identitas digital nasional yang baru bernama E-KTP digital. Nantinya E-KTP digital ini akan dikeluarkan dalam bentuk sebuah aplikasi identitas yang bernama Digital ID, fungsi E-KTP digital ini ke depannya akan lebih memudahkan bagi warga Indonesia untuk menerima pelayanan pemerintah maupun swasta tanpa perlu memfotokopi berkas yang dibutuhkan. Hal ini dikarenakan E-KTP digital sudah termasuk sistem identitas digital yang multifungsi, sebab datanya sudah terintegrasi dan terverifikasi dengan NIK. Jadi semua data yang terintegrasi dengan NIK akan termuat langsung di dalam aplikasi E-KTP digital tersebut. Sehingga warga Indonesia akan merasakan kemudahan dalam mengakses berbagai layanan pemerintah maupun swasta.

Di samping itu juga, diperlukan penggunaan teknologi blockchain untuk menyediakan sistem keamanan yang susah untuk diretas. Sehingga keamanan data warga Indonesia menjadi terjamin dan tidak mudah untuk disalahgunakan. Walaupun begitu, pemerintah Indonesia juga harus segera mengesahkan RUU PDP agar warga Indonesia merasa aman dan nyaman akan keamanan data pribadi mereka.

Dengan adanya perlindungan data ini juga dapat membentuk kepercayaan warga dalam menyediakan data dan informasi pribadi tanpa harus khawatir datanya akan disalahgunakan dan mereka juga akan merasa privasinya tetap terjaga.

Yang tidak kalah penting adalah penggunaan sistem identitas digital nasional di Indonesia memberikan manfaat yang signifikan bagi individu, sektor publik, maupun swasta. Bagi individu, penggunaan sistem identitas digital ini memberikan kenyamanan dan pengalaman yang luar biasa, mengurangi biaya dalam mengakses pelayanan, serta meningkatkan inklusi warga negara. Sedangkan bagi sektor publik, penggunaan sistem identitas digital ini membuat pelayanan publik semakin hemat biaya. Sementara bagi sektor swasta, adanya sistem identitas digital ini membuka peluang pendapatan baru yaitu dengan semakin banyaknya startup baru khususnya di bidang IT dan keamanan. Selain itu juga, perizinan mendirikan usaha juga menjadi lebih mudah untuk dilakukan.

Saran

Melihat masih terdapat beberapa permasalahan dalam pembentukan sistem identitas digital nasional ini, peneliti memberikan beberapa saran yang diharapkan dapat membantu pemerintah Indonesia dalam menyelesaikan permasalahan tersebut, yaitu:

1. dengan dikeluarkannya sistem identitas digital nasional berupa E-KTP digital, pemerintah harus memberikan usaha yang terbaik dalam pembentukan E-KTP digital ini agar fungsi-fungsi yang diberikan oleh E-KTP digital bisa benar-benar berguna di penerapan sehari-harinya;
2. karena E-KTP digital ini masih dalam tahap uji coba, akan lebih baik jika pemerintah melengkapi sistem E-KTP digital ini dengan menggunakan teknologi blockchain di dalamnya, misalnya bisa dengan merekrut tenaga ahli untuk menerapkan model sistem seperti yang diusulkan oleh Xiaohui Yang dan Wenjie Li. Agar keamanan dan fungsi E-KTP digital ini bisa lebih berkualitas dan tidak menimbulkan kerugian;
3. seperti yang sudah disampaikan sebelumnya bahwa di Indonesia perlu untuk memulai memberikan edukasi tentang teknologi sesegera mungkin kepada pelajar Indonesia. Agar ke depannya Indonesia bisa memiliki SDM yang lebih berkualitas dengan menguasai teknologi canggih, sehingga kemampuan tersebut dapat bersaing dengan negara lain; dan
4. SDM yang lebih berkualitas dengan menguasai teknologi canggih, sehingga kemampuan tersebut dapat bersaing dengan negara lain; dan
5. tidak kalah penting adalah DPR harus sesegera mungkin mengesahkan RUU PDP agar hak warga Indonesia bisa mendapatkan perlindungan terkait data pribadi mereka. Sehingga data mereka tidak disalahgunakan oleh lembaga pemerintah maupun swasta. Dan ketika RUU PDP tersebut telah disahkan, pemerintah harus menegakkannya dengan tegas tanpa pandang bulu dan memberikan sanksi yang sesuai.

REFERENCES

Adi, M. S., & Hendra. (2016, February). Warga Pekanbaru Harus Tahu, e-KTP Berlaku Seumur Hidup » BertuahPos. *Bertuahpos*.

Aji Nugroho, A., & Fitri Azmi, I. (2021). Alleviating Society's Economic Crisis: Narrative Policy on Social Safety Nets Policy Process During Covid-19 Pandemic. *Policy & Governance Review*, *5*(2), 113. https://doi.org/10.30589/pgr.v5i2.443

Angga, D., Setyawan, P., F, H., Amin, I., & Fuad, H. (2019, January). Hidup Kian Repot dengan Banyak Kartu. *Sindonews*.

Aujla, G. S., Singh, M., Bose, A., Kumar, N., Han, G., & ... (2020). Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications. *IEEE …*. https://ieeexplore.ieee.org/abstract/document/9055743/

Dewan, S., & Singh, L. (2020). Use of blockchain in designing smart city. *Smart and Sustainable Built Environment*. https://doi.org/10.1108/SASBE-06-2019-0078

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*. https://www.sciencedirect.com/science/article/pii/S0306457320309584

Fadhil, H., & Atriana, R. (2017, March). Ini Alur Pembahasan Anggaran Proyek e-KTP di DPR. *Detiknews*.

Gobel, T. (2020, December). *NEWS : Mengapa Indonesia Perlu Sistem Identitas Digital Nasional?* Cyberthreat.

Hardiansyah, Z., Nistanto, R. K., & Rafie, B. T. (2022, January). *E-KTP Digital Berbeda dengan E-KTP Biasa, Sudah Tahu Perbedaannya? - Page all*.

Jemadu, L., & Prastya, D. (2022, February). Kominfo Siapkan Sistem Identitas Digital Nasional untuk Kelola Data Masyarakat. *Suara*.

Kundu, D. (2019). Blockchain and trust in a smart city. *Environment and Urbanization ASIA*. https://doi.org/10.1177/0975425319832392

LAN RI. (2022, April). *ASN di Era VUCA: Memilih Kompetensi Hard Skills atau Soft Skills? – LAN RI*.

Lin, X., Wu, J., Mumtaz, S., Garg, S., Li, J., & ... (2020). Blockchain-based on-demand computing resource trading in IoV-assisted smart city. *IEEE Transactions on …*. https://ieeexplore.ieee.org/abstract/document/8985250/

Middleton, C. A. (2007). *Understanding the Benefits of Broadband: Insights for a Broadband Enabled Ontario A paper prepared for the Ministry of Government Services, Ontario*.

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly*, *37*(2), 101442. https://doi.org/10.1016/J.GIQ.2019.101442

NZ Digital government. (2022, February). *Digital identity system*.

Orecchini, F., Santiangeli, A., Zuccari, F., Pieroni, A., & ... (2018). Blockchain technology in smart city: A new opportunity for smart environment and smart mobility. *... Conference on Intelligent …*. https://doi.org/10.1007/978-3-030-00979-3_36

PERPRES No. 67 Tahun 2011 tentang Perubahan Kedua atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional, Pub. L. No. 67 (2011).

Prihadi, S. D. (2017, March). Mengenal Fungsi Biometrik & Chip di e-KTP. *CNN INDONESIA*.

Rathee, T., & Singh, P. (2022). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5782–5796. https://doi.org/10.1016/J.JKSUCI.2021.03.005

Redaksi Majalah ICT. (2022, May). *Inilah 7 Kelemahan e-KTP*. Majalah ICT.

Rheny, S. (2022, September). *Apa Itu Blockchain, Teknologi di Balik Bitcoin dan Crypto*. Ekrut Media.

Rivera, R., Robledo, J. G., Larios, V. M., & ... (2017). How digital identity on blockchain can contribute in a smart city environment. *... International Smart …*. https://ieeexplore.ieee.org/abstract/document/8090839/

SE Mendagri Nomor 471.13/1826/SJ hal Pemanfaatan eKTP dengan Menggunakan Card Reader, Pub. L. No. SE Mendagri Nomor 471.13/1826/SJ (2013).

Sharma, P. K., Kumar, N., & Park, J. H. (2018). Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Transactions on Industrial …*. https://ieeexplore.ieee.org/abstract/document/8579189/

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., & ... (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and …*. https://www.sciencedirect.com/science/article/pii/S2210670720305850

Stephanie, C., & Nistanto, R. K. (2021, July). 3 Negara dengan KTP Elektronik Canggih, Tak Perlu Fotokopi Halaman all - Kompas.com. *Kompas*.

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, *2*(2), 100014. https://doi.org/https://doi.org/10.1016/j.bcra.2021.100014

Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723–731. https://doi.org/10.1016/J.CLSR.2018.05.015

Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, *39*(1), 101625. https://doi.org/https://doi.org/10.1016/j.giq.2021.101625

Techopedia. (2021, June). *What is a Digital Identity? - Definition from Techopedia*. Techopedia.

UU No. 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Pub. L. No. 24 (2013).

Veratika, I. (2021, November). *RUU Perlindungan Data Pribadi Perlu Atur Sanksi bagi Pengumpul Data jika Bocor*. Universitas Katolik Parahyangan.

Wahyudi, A. A., Widowati, Y. R., & Nugroho, A. A. (2022). STRATEGI IMPLEMENTASI SMART CITY KOTA BANDUNG. *Jurnal Good Governance*, *18*(1).

Windley, P. (2023, January). *Defining Digital Identity*.

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers and Security*, *99*. https://doi.org/10.1016/j.cose.2020.102050

Yona, M., Birfir, G., & Kaplan, S. (2021). Data science and GIS-based system analysis of transit passenger complaints to improve operations and planning. *Transport Policy*, *101*, 133–144. https://doi.org/https://doi.org/10.1016/j.tranpol.2020.12.009