Jurnal Peperangan Asimteris
Volume 8, Nomor 2 2022 E-ISSN 2830-0475

TEKNOLOGI *BLOCKCHAIN* DALAM KAJIAN PEPERANGAN ASIMETRIS: PERSPEKTIF INDONESIA

(*Blockchain Technology in The Asymmetric Warfare Study: Indonesian Perspective)*

Eri Suprayitno
Prodi Peperangan Asimetris, Fakultas Strategi Pertahanan,
Universitas Pertahanan RI
email; esupra@gmail.com

Abstrak – Terobosan di bidang teknologi mengubah wajah perang dan bagaimana kita mempersiapkan perang. *Blockchain* sebagai sebuah terobosan baru dalam bidang teknologi informasi membawa peluang yang masih luas untuk dikaji dan diimplementasikan pada berbagai bidang. Dengan metode deskriptif kualitatif, tulisan ini bertujuan untuk memberikan gambaran peluang dan ancaman yang dibawa oleh kehadiran teknologi *blockchain* dalam kajian peperangan asimetris. Hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan dalam pengambilan keputusan untuk mengadopsi teknologi *blockchain* pada bidang pertahanan di Indonesia sebagai strategi antisipasi terhadap peperangan asimetris. Indikator yang digunakan dalam mengeksplorasi permasalahan dalam penelitian ini adalah manfaat dan dampak negatif yang dibawa oleh kemunculan teknologi *blockchain.* Hasil penelitian ini menemukan bahwa teknologi *blockchain* dapat dimanfaatkan untuk meningkatkan keamanan siber, mengurangi titik kegagalan tunggal pada sistem pengambilan keputusan darurat, meningkatkan efisiensi operasi rantai pasokan dan logistik, meningkatkan transparansi audit pengadaan barang dan jasa, Perlindungan Sistem Senjata dan Infrastruktur Digital, Pengamanan Pesawat Tanpa Awak (*UAV*) dan Sistem Kawanan, serta memvalidasi perintah dan informasi di medan perang. Namun teknologi *blockchain* juga membawa dampak negatif karena juga berpotensi untuk dimanfaatkan pada berbagai tindak kriminal berkaitan dengan mata uang kripto di dunia maya (*cybercrime*).
Kata kunci: Teknologi Blockchain, Pertahanan, Peperangan Asimetris, Indonesia

Abstract *– Technological advances are changing the face of war and how we prepare for it. Blockchain, as a technological breakthrough in the field of information technology, opens up numerous opportunities for research and application in a variety of fields. Using a qualitative*

descriptive method, this paper aims to provide an overview of the opportunities and threats presented by the presence of blockchain technology in the study of asymmetric warfare. The study's findings are expected to be considered when making decisions to implement blockchain technology in the defense sector in Indonesia as an anticipatory strategy against asymmetric warfare. The benefits and negative impacts brought about by the emergence of blockchain technology are the indicators used in this research to explore the problems. According to the findings of this study, blockchain technology can be used to improve cybersecurity, reduce single points of failure in emergency decision-making systems, improve supply chain and logistics operations efficiency, increase transparency of audits of procurement of goods and services, protect weapon systems and digital infrastructure, secure unmanned aerial vehicle (UAV) and swarm systems, and validate orders and battle information. However, blockchain technology has a negative impact due to its potential to be used for various cryptocurrencies-related cybercrime.
Keywords: Blockchain Technology, Defense, Asymmetric Warfare, Indonesia

1. Pendahuluan

Perang didefinisikan sebagai konflik bersenjata antara dua atau lebih pemerintah atau negara. Perang adalah tindakan kekerasan yang dimaksudkan untuk memaksa lawan kita untuk memenuhi keinginan kita (Clausewitz, 1873). Perang juga didefinisikan sebagai "kondisi hukum yang memungkinkan dua atau lebih kelompok untuk melakukan konflik bersenjata secara seimbang" (Walzer, 2006).

Secara garis besar metode dan praktik perang atau peperangan dapat dibagi menjadi berbagai jenis, antara lain berdasarkan periode waktu (perang prasejarah, perang kuno, perang modern), berdasarkan arenanya (perang darat, perang laut, perang udara), berdasarkan jenis senjata yang digunakan (perang kapal selam, perang kimia, perang nuklir), berdasarkan pihak-pihak yang terlibat (perang Romawi, perang Cina dan perang Arab), atau berdasarkan taktik yang digunakan (perang gerilya, perang pengepungan, perang asimetris).

Mantan Menteri Pertahanan pada masa Presiden AS Bill Clinton, William J. Perry,adalah orang yang pertama menyatakan bahwa terobosan dalam bidang teknologi informasi akan merubah wajah perang ke depan. Dalam sebuah *quote* yang terkenal dia menyatakan bahwa kita hidup di zaman yang digerakkan oleh

informasi. Terobosan dalam bidang teknologi mengubah wajah perang dan bagaimana kita bersiap untuk perang. Perry menyadari bahwa banyak negara di dunia, termasuk Amerika Serikat, menggerakkan sumber daya strategis seperti tenaga listrik, aliran uang, lalu lintas udara, minyak bumi, gas, pelayanan publik dan sumber daya strategis lainnya melalui teknologi informasi yang kompleks.

Blockchain merupakan sebuah teknologi baru dalam bidang teknologi informasi. Teknologi *Blockchain* selalu dikaitkan atau dianggap identik dengan mata uang kripto (*cryptocurrency*), faktanya implementasi teknologi blockchain tidak hanya pada mata uang kripto saja tetapi sangat luas dan masih potensial untuk dikaji serta diterapkan pada berbagai bidang. Pada dasarnya *blockchain* adalah sebuah buku besar *(ledger)* atau struktur data terdesentralisasi dimana setiap pengguna dapat memantau setiap transaksi yang terjadi untuk memastikan tidak ada yang memanipulasi data maupun transaksi yang terjadi diantara para penggunanya. *Blockchain* adalah sebuah buku besar atau struktur data terdesentralisasi. Dapat juga disebut sebagai rangkaian blok dimana suatu blok merujuk pada blok sebelumnya. Setelah sebuah transaksi atau peristiwa dimasukkan ke dalam *blockchain*, tidak mungkin untuk merubah atau memanipulasi isinya karena setiap pengguna atau anggota dalam jaringan dapat memantau setiap transaksi yang terjadi (Chatterjee & Chatterjee, 2018).

Studi ini dilakukan untuk melihat peluang dan ancaman yang dibawa oleh kehadiran teknologi *blockchain* dalam kajian peperangan asimetris. Dengan membandingkan peluang dan ancaman yang ada diharapkan dapat menjadi bahan pertimbangan dalam pengambilan keputusan untuk mengadopsi teknologi *blockchain* pada berbagai bidang sebagai antisipasi terhadap peperangan asimetris.

2. Tinjauan Pustaka

2.1. *"The Militarisation of Blockchain Technologies: At The Forefront of Cyber Security Innovation? Or a Danger to International Stability"* Oleh Anggie Khayan

Tulisan ilmiah ini menggambarkan potensi pemanfaatan teknologi *blockchain* dalam bidang militer oleh Amerika Serikat dan China antara lain dalam perlindungan sistem persenjataan dan infrastruktur digital, pengamanan pesawat tanpa awak dalam sistem kawanan, validasi perintah dan informasi medan perang, pengelolaan logistik dan rantai pasokan, peperangan intelijen dan opini publik.

2.2. **"***Why Military Blockchain is Critical in the Age of Cyber Warfare: 4 ways blockchain can secure and defend key military assets and weapons systems"* oleh Dr. Victoria Adams

Tulisan ini memberikan empat gambaran bagaimana teknologi *blockchain* dapat diterapkan dalam pertahanan siber untuk melindungi dan mempertahankan aset-aset militer dan sistem persenjataan, antara lain sebagai pertahanan bagi sistem persenjataan kritis, pengelolaan sistem kerumunan terotomasi, validasi perintah dan informasi medan perang serta pengelolaan logistik dan rantai pasokan.

2.3. *"Strategic Information Warfare: A New Face of War"* oleh Roger C. Molander, Andrew Riddile, Peter A. Wilson

Tulisan ini menjelaskan bagaimana teknologi informasi dapat merubah wajah perang dalam bentuk perang informasi. Fitur-fitur dasar dari peperangan informasi yang menjadi sumber ancaman, antara lain berbiaya rendah, batas-batas yang tidak jelas, mudah dimanipulasi dan dipalsukan, rendahnya pengetahuan tentang kerentanan strategis informasi, permasalahan dalam sistem deteksi dan asesmen terhadap serangan serta kesulitan dalam membangun dan mempertahankan koalisi.

2.4. *"Blockchains In National Defense: Trustworthy Systems in A Trustless World"* oleh Neil B. Barnas

Tulisan ini menggambarkan bahwa pertahanan siber kontemporer sedang goyah, dan peningkatan bertahap tampaknya tidak mungkin untuk mengatasi ancaman siber yang tumbuh secara eksponensial. Oleh karena itu, diperlukan model yang sama sekali baru untuk strategi pertahanan siber. *Blockchain* adalah teknologi informasi baru yang membalikkan paradigma keamanan siber. Pertama, jaringan

blockchain tidak dapat dipercaya; mereka menganggap kompromi jaringan baik oleh orang dalam maupun orang luar. Kedua, *blockchains* secara transparan aman; mereka tidak bergantung pada rahasia yang rawan kegagalan, tetapi lebih pada struktur data kriptografis yang membuat perusakan menjadi sangat sulit.

3. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif. Metode deskriptif kualitatif adalah metode penelitian yang berdasarkan pada filsafat postpositivisme digunakan untuk meneliti pada kondisi objek yang alamiah (sebagai lawannya adalah eksperimen) dimana peneliti adalah sebagai instrument kunci teknik pengumpulan data dilakukan secara trigulasi (gabungan), analisis data bersifat induktif/kualitatif, dan hasil penelitian kualitatif lebih menekankan makna daripada generalisasi (Sugiyono, 2016). Penelitian deskriptif kualitatif bertujuan untuk menggambarkan, melukiskan, menerangkan,menjelaskan dan menjawab secara lebih rinci permasalahan yang akan diteliti dengan mempelajari semaksimal mungkin seorang individu, suatu kelompok atau suatu kejadian. Dalam penelitian ini penulis akan mendeskripsikan teknologi *blockchain* melalui dua sudut pandang dalam peperangan asimetris, yaitu sebagai peluang dan ancaman.

Teknik pengumpulan data yang digunakan adalah studi pustaka, dimana penulis menggunakan buku dan jurnal penelitian terkait teknologi *blockchain* dan pemanfaatannya baik dalam bentuk cetak maupun elektronik sebagai sumber utama data penelitian. Studi kepustakaan merupakan kajian teoritis, referensi serta literatur ilmiah lain yang berkaitan dengan nilai, budaya dan norma yang berkembang pada situasi sosial yang diteliti (Sugiyono, 2016).

4. Hasil Penelitian

4.1. Pemanfaatan *blockchain* untuk meningkatkan keamanan siber

Sistem informasi secara umum memiliki banyak kerentanan terhadap serangan siber. Kerentanan ini berpotensi dieksploitasi atau dimanfaatkan oleh penyusup untuk masuk kedalam jaringan dan mengambil alih akun pengguna yang digunakan untuk menjalankan perintah-perintah berbahaya seperti mencurian dan penghapusan data, mengendalikan infrastruktur kritis, mentransfer sejumlah uang atau mengambil alih sistem persenjataan (The Value Technology Foundation, 2020).

Teknologi *blockchain* menghadirkan cara yang unik untuk mengatasi hal tersebut. Sebagaimana disebutkan bahwa *blockchain* adalah *database* transaksi terdistribusi yang bersifat *append-only,* yang berarti hanya dapat menambahkan data dan tidak bisa merubah, menghapus atau mengurangi data. Tanggung jawab administratif dan kepercayaan terbagi dintara para operator dan setiap anggota dalam jaringan dapat memantau setiap penambahan transaksi yang terjadi.

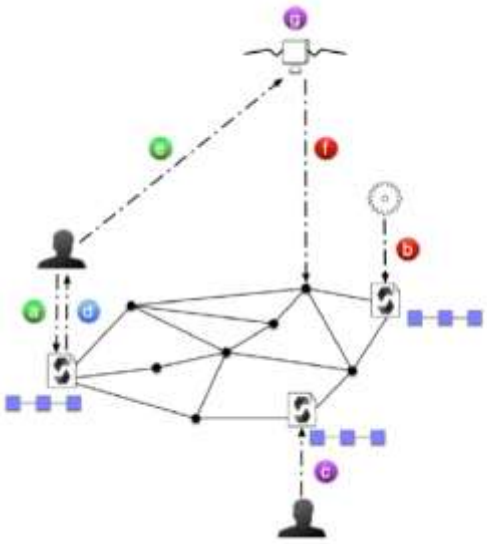
Sifat alami *tamper-proof* yang dimiliki oleh *blockchain* menjadikannya sulit untuk disusupi karena penyerang harus menguasai banyak anggota untuk dapat melakukan serangan. Karakteristik teknologi *blockchain* ini menjadikannya dapat diaplikasikan pada berbagai sistem informasi untuk meningkatkan keamanan dan mengurangi berbagai bentuk ancaman yang dapat terjadi.

Dalam laporan tersebut dicontohkan bahwa pengamanan komunikasi pada pesawat ruang angkasa saat ini masih belum sepenuhnya diimplementasikan, yang menyisakan vector ancaman terkait kendali pesawat ruang angkasa. Ancaman pada pada komunikasi pesawat ruang angkasa dan satelit pada umumnya identik dengan ancaman pada layanan internat, yaitu akses tidak sah (*hacking)* dan *denial of service (jamming radio communication).* Pesawat ruang angkasa dan sistem pengendali berbasis darat berisiko terkena serangan semacam itu.

Disebutkan pernah terjadi serangan berupa akses tidak sah terhadap "jaringan komputer yang mengendalikan pesawa ruang angkasa" di NASA *Jet Propulsion Laboratory* serta gangguan *jamming* terhadap Satelit Militer Amerika Serikat dengan menggunakan peralatan komersial yang mudah didapatkan oleh aktor negara maupun bukan negara. Dapat diasumsikan bahwa gangguan serupa juga dapat dialami oleh satelit komersial maupun aset ruang angkasa yang dikendalian oleh negara-negara lain.

Penggunaan teknologi *blockchain* sebagai sistem konfirmasi dapat digunakan untuk mengatasi masalah tersebut. *Blockchain* adalah sistem terdistribusi secara alami yang harus mencapai konsensus tentang informasi baru agar dapat beroperasi. Penambahan *arbitrary smart contract execution* memungkinkan pengguna blockchain untuk mengkodekan logika bisnis apa pun sesuai dengan kebutuhan.

Sebagai contoh, sebuah *smart contract* dibuat sehingga perintah yang ditujukan untuk pesawat ruang angkasa tidak akan dieksekusi dan masuk dalam *blockchain* sampai pengguna yang sah mengkonfirmasi validitas perintah yang dikeluarkan ke satelit melalui otentikasi multi-faktor atau beberapa pengguna yang sah mengonfirmasi validitas perintah. melalui otorisasi multi-pihak. Perintah juga dapat diperiksa kebenaran formatnya, kegunaannya dalam konteks operasional, atau pemeriksaan otomatis lainnya yang dapat dikodekan dalam *smart contract*. Hal ini ditunjukkan melalui diagram berikut. Diagram pemanfaatan otentikasi multi-faktor dan otorisasi multi-pihak dalam pengamanan komunikasi pesawat ruang angkasa menggunakan teknologi *blockchain* dapat dilihat dalam gambar 1.



Gambar 1. Contoh otentikasi multi-faktor dan otorisasi multi-pihak

Keterangan Gambar:

a — Operator mengajukan sebuah perintah untuk dikirimkan ke pesawat ruang angkasa

b — Sejumlah proses otomatis (nol atau lebih) mengkonfirmasi sintaks perintah dan aplikabilitasnya dalam konteks operasional

c — Sejumlah manusia (nol atau lebih) mengkonfirmasi bahwa perintah harus dilanjutkan

d — *Smart contract* menetapkan entri tabel persetujuan perintah yang terkait dengan nilai hash perintah ke Nilai *Boolean* ***True.***

e — Operator mengirimkan perintah ke pesawat luar angkasa dengan komputasi yang dapat diverifikasi serta mengirimkan bukti entri tabel persetujuan perintah yang telah ditetapkan.

f — Jika satelit menjalankan klien ringan, operator juga mengirimkan *Merkle path* ke status kontrak untuk tabel persetujuan

g — Pesawat ruang angkasa menjalankan perintah jika dan hanya jika perintah berhasil diverifikasi

Secara keseluruhan, manfaat utama dari pendekatan ini adalah menyediakan tingkat otentikasi dan/atau keamanan otorisasi yang jauh lebih tinggi. Seorang penyerang perlu mendapatkan kendali atas sejumlah akun pengguna yang berubah-ubah dan dapat menggunakan akun tersebut untuk melakukan tindakan di *blockchain* untuk mengonfirmasi perintah.

4.2. Pemanfaatan *blockchain* untuk mengurangi titik kegagalan tunggal (*single points of failure)* dalam sistem pengambilan keputusan darurat.

Titik kegagalan tunggal dalam teknologi adalah bagian dari sistem yang jika gagal akan menghentikan kerja seluruh sistem. *Blockchain* memberikan peluang dan tantangan ketika diterapkan untuk mengurangi titik kegagalan tunggal dalam sistem pengambilan keputusan darurat (The Value Technology Foundation, 2020).

Dalam pengambilan keputusan darurat atau bencana, praktik menangani situasi darurat secara efektif dengan meminimalisir kerugian harta benda dan nyawa yang disebabkan oleh suatu kejadian adalah sebuah hal biasa dalam medan perang. Saat ini dengan penemuan senjata nuklir, keputusan lebih cepat yang dibuat oleh lebih sedikit individu memiliki dampak pada perubahan populasi dunia dalam semalam.

Teknologi *Blockchain* mendatangkan bukti yang kuat untuk pengambilan keputusan yang meyakinkan. *Blockchain* menggunakan bukti kriptografis dari identifikasi dan perbaikan titik kegagalan tunggal di mana arsitektur data TI terpusat dan tradisional tetap terdampak oleh kelemahan ini. Selain itu, blockchain dapat membuat jaringan yang digunakan selama pengambilan keputusan darurat memiliki sifat *antifragile* yang signifikan.

Konsep *antifragile* adalah semakin meningkatkan ketahanan atau ketangguhan, dengan kata lain sistem ini akan semakin kuat ketika semakin banyak orang atau mesin yang merusaknya. Teknologi *blockchain* meningkatkan kemampuan ini dengan mengaktifkan satu versi kebenaran, kekekalan data dan proses otomatis. Menggabungkan teknologi blockchain dengan algoritma *machine learning* akan memungkinkan sistem dengan multi-stakeholder terus meningkatkan diri, bereaksi lebih baik terhadap tantangan di masa depan, dan bahkan mungkin mengantisipasi potensi masalah.

Teknologi *blockchain* dapat membantu memastikan keadaan dan efektifitas jaringan operasional dan ekosistem besar tetap berfungsi selama proses pengambilan keputusan dalam peristiwa darurat dan bencana. Banyak faktor yang harus dipertimbangkan dalam lingkungan pengambilan keputusan darurat, terutama ketika banyak aktor terlibat dalam pemeliharaan, pengaturan, penyediaan, dan penggunaan sistem ini.

Teknologi Blockchain dapat diprogram untuk membasmi, mengisolasi, dan memitigasi serangan yang bertujuan mengeksplotasi titik kegagalan tunggal pada setiap sistem jaringan. Hasil akhirnya adalah hierarki perintah dan kontrol yang dapat memfasilitasi kepercayaan tinggi dalam pengambilan keputusan berdasarkan keandalan data yang dihasilkan dari sistem yang digunakan.

4.3. Pemanfaatan *blockchain* untuk meningkatkan efisiensi operasi rantai pasokan dan logistik pertahanan.

Presiden Amerika Serikat ke-34, Dwight D. Eisenhower mengatakan bahwa akan sangat mudah membuktikan bahwa kemenangan atau kekalahan perang sangat tergantung pada logistik. Kekuatan yang luar biasa adalah elemen penting dari kesuksesan militer. Pasukan Amerika dilengkapi dengan sistem senjata dan alat pertahanan tercanggih di dunia, mulai dari daya tembak terbang jet Angkatan Udara hingga Teknologi *Near-infrared Signature Management* dalam Seragam Tempur Angkatan Darat yang membuat mereka tidak mudah terdeteksi oleh musuh.

Namun musuh memahami bahwa sistem ini merupakan tahap akhir dalam jaringan produksi dan pasokan yang sangat luas. Mereka memahami bahwa jauh lebih aman untuk diam-diam mengubah desain bilah rotor daripada menghadapi helikopter tempur. Mereka memahami bahwa menginfeksi rantai pasokan makanan siap saji (MRE) jauh lebih mengganggu daripada mengepung pasukan infanteri. Musuh yang paling kuat adalah yang pandai memunculkan keraguan pada lawannya dan tahu cara melakukan sabotase terhadap jaringan pasokan.

Dalam beberapa tahun terakhir terjadi peningkatan yang drastis atas risiko masuknya komponen palsu atau tidak sesuai ke dalam rantai pasokan Departemen Pertahanan AS. Komite Angkatan Bersenjata Senat dan Kantor Akuntabilitas Pemerintah (GAO) telah menerbitkan laporan dalam satu dekade yang merinci penyebaran ancaman pemalsuan, terutama yang berkaitan dengan manipulasi komponen oleh musuh asing. Risiko pemalsuan menjadi perhatian bagi sebagian besar rantai pasokan, namun faktor gabungan seperti tenaga kerja dan bahan luar negeri yang murah, pengurangan jumlah produsen dalam negeri, dan menjamurnya pengecer AS telah mengakibatkan kondisi akuisisi di bawah standar. Departemen Pertahanan membutuhkan pengawasan yang lebih baik dan kolaborasi yang lebih besar dengan produsen terpercaya untuk membantu mengamankan rantai pasokan komponen penting.

Teknologi *Blockchain* bertindak sebagai penjamin kepercayaan dalam ekosistem pengadaan dengan memungkinkan visibilitas dan kolaborasi yang lebih besar antara asal dan tujuan. Di seluruh dunia, perusahaan yang bergantung pada rantai pasokan beralih ke teknologi *blockchain*. Produsen, pengecer, dan perusahaan pengiriman lintas samudera menerapkan sistem "*track and trace*" berbasis *blockchain* yang memberikan visibilitas dan kepercayaan komponen makanan dan produk dari asalnya hingga konsumen akhir. Sistem ini menjadi rujukan bagi potensi pemanfaatan *blockchain* dalam rantai pasokan Departemen Pertahanan (The Value Technology Foundation, 2020).

Teknologi *blockchain* dapat membawa rantai pasokan pertahanan ke masa depan dengan menjembatani kesenjangan antara dunia fisik dan digital serta mengembangkan ekosistem logistik yang didorong oleh kolaborasi dan kepercayaan. Keunggulan yang dapat diberikan oleh teknologi *blockchain* kepada organisasi pertahanan antara lain:

a. Traceability

Verifikasi berdasarkan permintaan terhadap sumber, lokasi asal dan identitas dari perangkat lunak, perangkat keras, serta dokumentasi pendukung untuk komponen dan sistem.

b. Assurance

Jaminan terhadap kualitas dan spesifikasi produk serta kepatuhan terhadap standar industri dan peraturan.

c. Transparency

Kemampuan untuk berbagi, dengan izin khusus, terhadap catatan transaksi dan transfer yang permanen dan terverifikasi di seluruh ekosistem pemasok, mitra, dan pelanggan.

d. Fast Settlement

Kemampuan untuk menerapkan *smart contract* untuk transfer kepemilikan dan distribusi dana otomatis berdasarkan aturan bisnis yang disepakati.

e. Simplicity

Rekonsiliasi yang disederhanakan, penghapusan pengecualian, peningkatan kemampuan mendengar, pengurangan dokumen dan peningkatan kolaborasi dengan mitra ekosistem.

f. Secure Trading

Mengamankan pembelian dan penjualan komponen dan produk di seluruh rantai pasokan melalui pemahaman yang lebih baik tentang kredensial dan praktik mitra rantai pasokan.

4.4. Pemanfaatan *blockchain* untuk meningkatkan transparansi audit pengadaan barang dan jasa bidang pertahanan.

Sejak awal tahun 1990-an, manajemen kontrak oleh Departemen Pertahanan telah dimasukkan dalam daftar berisiko tinggi oleh Kantor Akuntabilitas

Pemerintahan AS karena kekurangannya di banyak bidang, termasuk akuisisi layanan yang tidak berubah sampai tahun 2017. Pemerintah di seluruh dunia telah menerapkan berbagai teknologi untuk meningkatkan integritas, efisiensi, dan nilai uang dalam proses pengadaan mereka. *Blockchain* adalah salah satu teknologi yang sedang diuji, terutama karena memiliki sifat *tamper-resistance, tamper-evidence* dan secara inheren menghasilkan satu sumber kebenaran yang dapat dipercaya dan digunakan sebagai tolok ukur untuk mendeteksi pemborosan, penipuan, dan penyalahgunaan (The Value Technology Foundation, 2020).

Keuntungan memasukkan teknologi *blockchain* ke dalam arsitektur sistem e-procurement adalah hadir dengan keunggulan buku besar yang *tamper-resistant* dan mampu diperbarui serta dibagikan secara real time di antara para peserta dalam jaringan untuk meningkatkan transparansi. Kemampuan unik blockchain untuk memvalidasi dan membentuk konsensus seputar keakuratan dan kelengkapan data yang dibagikan pada buku besar bersama di antara sekelompok pihak yang semi-terpercaya hingga tidak terpercaya, membuka banyak kemungkinan untuk meningkatkan e-procurement bagi pemerintah AS, yang akan menghasilkan pengurangan temuan utama yang merugikan dalam laporan Kantor Akuntabilitas Pemerintah AS.

Departemen Layanan Kesehatan dan Kemanusiaan (*HHS*) baru saja memperoleh persetujuan *Authority To Operate (ATO)* pertama untuk blockchain di dalam Pemerintah. Oki Mek, Chief Product Officer di divisi akuisisi di HHS membuat beberapa pengamatan tentang bagaimana kinerja *blockchain* dalam pengadaan. "Kami harus memenuhi persyaratan *FISMA [Federal Information Security Management Act].* Bagian dari persyaratan itu adalah bahwa semua sistem yang didanai federal harus diberi wewenang untuk beroperasi. Bagian dari proses itu adalah proses penilaian yang ketat dan otorisasi oleh pejabat yang berwenang. Kami telah membuktikan bahwa *blockchain* dapat diotorisasi untuk beroperasi di

Pemerintah Federal. Tidak hanya itu, kami menemukan bahwa *blockchain* meningkatkan keamanan siber."

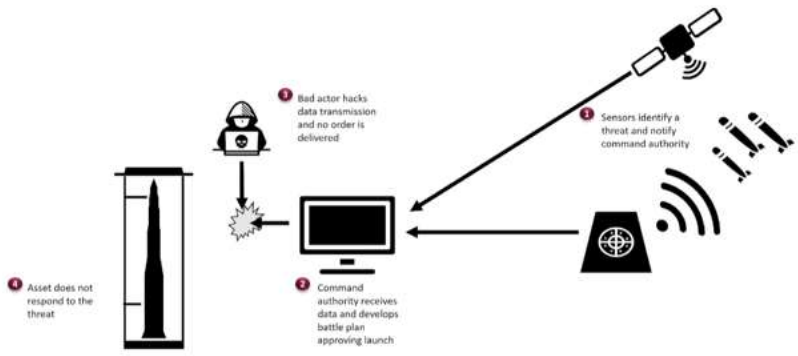
Masalah berikutnya yang diangkat oleh GAO yang akan dianalisis adalah ketidakmampuan Departemen Pertahanan untuk melacak dan mengelola anggaran layanan yang dikontrakkan secara memadai. Jika *blockchain* memungkinkan untuk berbagi data dengan pihak semi-tepercaya, data yang belum pernah dibagikan secara historis dapat dibagikan dengan menggunakan aturan yang ditetapkan di antara para peserta dalam jaringan. Karakteristik *blockchain* membantu meyakinkan orang lain bahwa akan ada peristiwa yang tercatat dari semua transaksi yang akan menghasilkan jejak audit yang memungkinkan semua aturan dan transaksi diaudit.

implementasi *blockchain* oleh *HHS* di dunia nyata dalam proses pengadaan merupakan contoh yang paling jelas untuk menggambarkan bagaimana masalah anggaran dapat diatasi. Michael McFarland, Direktur *Office of Acquisition Business Systems* di HHS, memberikan pengamatannya tentang bagaimana informasi harga dan anggaran dapat dibagikan ke seluruh peserta jaringan. Dia mencatat bahwa mereka sekarang akan memiliki akses yang belum pernah terjadi sebelumnya terhadap harga yang dibayarkan, data vendor, dan akuisisi lain yang telah terjadi sebagai hasil dari teknologi *blockchain* sehingga mereka akan dapat membuat keputusan dengan informasi yang jauh lebih banyak daripada yang mereka miliki sebelumnya. Keberhasilan HHS dalam implementasi *blockchain* membantu mendukung alasan pemerintah untuk menggunakan *blockchain*, terutama mengingat tantangan dan kekurangan yang diketahui yang dihadapi oleh departemen dan lembaga seperti yang dikutip oleh organisasi pengawas.

Terakhir, kemampuan untuk memiliki penghitungan inventaris waktu nyata yang akurat untuk permintaan pengadaan yang tepat dapat diaktifkan melalui buku besar terdistribusi yang dibagikan di seluruh rantai proses pengadaan dan membantu menghindari pemborosan dalam pengambilan keputusan tentang jumlah pesanan.

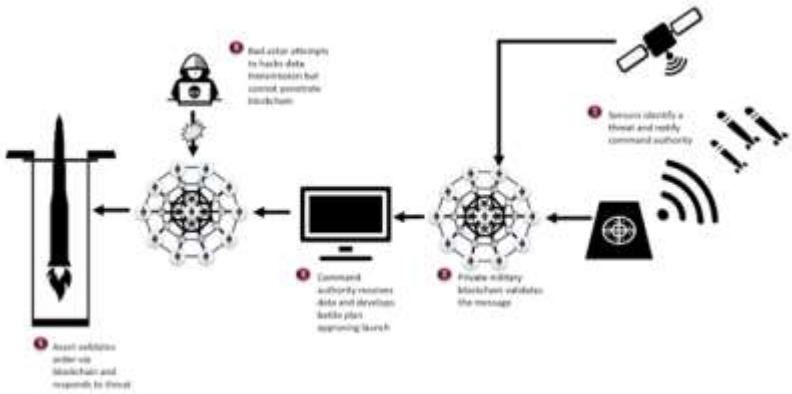
4.5. Pemanfaatan *Blockchain Dalam* Perlindungan Sistem Senjata dan Infrastruktur Digital

Pertahanan siber adalah salah satu bentuk aplikasi teknologi *blockchain* yang paling berjangka pendek, berbiaya rendah, dengan hasil tinggi (Barnas, 2016). Kompleksitas yang berkembang dalam sistem senjata modern membuat kerentanan "lebih mungkin dan kurang dapat dideteksi". Sistem pertama di bawah ini memberikan model abstrak tentang bagaimana sistem perintah dan kontrol dapat beroperasi di bawah sistem terpusat.



Gambar 2. Kendali Terpusat Sistem Persenjataan

Gambar 2. menunjukkan model abstrak tingkat tinggi tentang bagaimana perintah dan kontrol dapat berfungsi dalam sistem terpusat. Seperti yang dapat dilihat, sistem menerima data dari sensor yang kemudian memberi tahu otoritas komando tentang ancaman yang masuk yang kemudian mengarahkan sistem senjata untuk merespons ancaman tersebut. Namun, sifat sistem yang terpusat berarti bahwa ada satu titik kerentanan yang dapat diserang dari aktor jahat dari luar. Otoritas komando dan pengontrol otomatis atau manusia dari sistem senjata berpotensi rentan menerima informasi yang salah atau palsu. Hal ini dapat mengakibatkan penggunaan sistem senjata yang tidak sah atau kegagalan untuk menanggapi ancaman yang sesungguhnya.



Gambar 3. Kendali Terdesentralisasi Sistem Persenjataan Berbasis *Blockchain*

Gambar 3 menunjukkan bagaimana sistem ini dapat berfungsi menggunakan *blockchain*. Seperti dapat dilihat, transmisi data divalidasi melalui sistem terdistribusi yang menggunakan sistem konsensus untuk memvalidasi bahwa data berasal dari inisiator yang sah. Karena tanggung jawab untuk menyetujui transaksi memerlukan persetujuan oleh semua atau sebagian besar node dalam sistem, aktor jahat harus meretas semua node secara bersamaan. Karena setiap node independen dan dilindungi oleh kriptografi ekstensif asli dari node tersebut, daya komputasi yang diperlukan untuk meretas sistem menjadi sangat besar. Dengan node yang cukup, sistem bisa menjadi hampir tidak dapat diretas. Satu-satunya batasan pada jumlah node adalah waktu pemrosesan yang diperlukan untuk memvalidasi komunikasi dibandingkan dengan kebutuhan keputusan sistem.

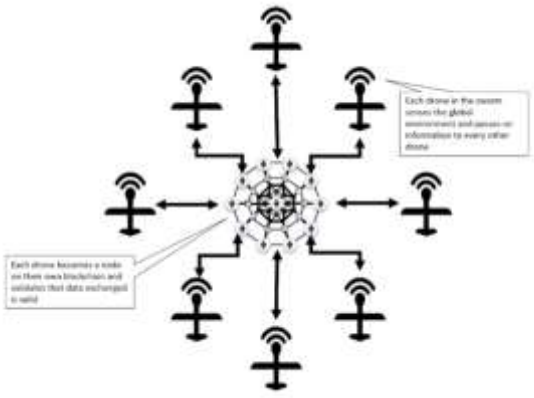
4.6. Pemanfaatan *Blockchain* Dalam Pengamanan Pesawat Tak Berawak (*UAV*) dan Sistem Kawanan

Sistem Robotika kawanan adalah pendekatan untuk mengkoordinasikan beberapa robot sebagai suatu sistem yang terdiri dari sejumlah besar robot fisik sederhana. Perilaku kolektif yang diinginkan muncul dari interaksi antara robot dan interaksi robot dengan lingkungan. Pendekatan ini muncul di bidang kecerdasan kawanan buatan, serta studi biologis serangga, semut, dan bidang lain di alam, di

mana perilaku kawanan terjadi. Dalam kasus robot militer, beberapa drone atau robot akan berfungsi secara paralel untuk mengatasi pertahanan lawan dan menghancurkan target (Adams, 2019).

Otonomi anggota individu dalam kawanan dan ketergantungan mereka pada komunikasi dan interaksi membuat mereka rentan terhadap peretasan. Salah satu batasan utama dalam pengelolaan robot dalam jumlah besar adalah apa yang dikenal sebagai "pengetahuan global". Artinya, kesadaran tidak hanya kondisi agen yang berdekatan tetapi juga populasi secara keseluruhan. Kebutuhan untuk komunikasi terkoordinasi utama antara setiap elemen dalam swarm berarti bahwa swarm terbuka untuk serangan dari aktor luar.

Blockchain menawarkan mekanisme untuk dapat melindungi komunikasi dan koordinasi intra-swarm (Gambar 4). Dalam sistem seperti itu, setiap elemen swarm akan menjadi node dalam blockchain mereka sendiri. Kawanan akan memvalidasi komunikasi secara internal menggunakan pendekatan pengambilan keputusan kolektif dan terdesentralisasi untuk mengelolanya beroperasi dan menyebarkan pengetahuan global ke masing-masing pihak. Dengan demikian, kawanan dapat berbagi pengetahuan global sambil melindungi diri dari serangan dunia maya (Adams, 2019).



Gambar 4. Pertahanan Kawanan *UAV* Berbasis *Blockchain*

4.7. Pemanfaatan *Blockchain* untuk memvalidasi Perintah dan Informasi di Medan Perang

Tentara di medan perang perlu untuk mengetahui bahwa informasi yang mereka terima valid dan akurat. Manajemen komunikasi digital yang terpusat mengeskpos pasukan terhadap serangan siber yang memalsukan perintah atau memberikan informasi palsu tentang kemajuan rencana pertempuran. Selain itu, jika beberapa bagian dari jaringan data mengalami kegagalan katastropik, integritas sistem perlu dilanjutkan. Hal Ini tidak dapat dijanjikan oleh sistem terpusat.

Blockchain menghadirkan solusi untuk tantangan ini. Dengan menyebarkan data secara horizontal, *blockchain* mendemokratisasikan ruang pertempuran dan menciptakan lingkungan yang aman di mana kegagalan salah satu node tidak akan mempengaruhi kelangsungan hidup jaringan secara keseluruhan. Selain itu, dengan mengandalkan sistem validasi terdesentralisasi dengan sistem keamanan bawaan berbasis *blockchain* dapat memastikan bahwa semua komunikasi dan transfer data terlindungi dari aktor jahat. Pasukan di medan perang dapat diyakinkan bahwa perintah yang dia terima adalah sah, dan bahwa data yang dikirimkan dari sensor atau bagian lain dari ruang pertempuran belum dirusak. *Blockchain* dapat menciptakan sebuah sistem yang kuat dan *hack-resistant* yang mendukung fluiditas dan koordinasi yang dibutuhkan olah perang digital (Adams, 2019).

4.8. Pemanfaatan Teknologi *Blockchain* Dalam Tindak Kriminal

"Teknologi *blockchain* dan *cryptocurrency* sendiri memiliki dampak negatif diantaranya dapat digunakan sebagai sarana pencucian uang (*money laundry*)(Sutrisno, 2018). Melakukan transaksi yang bersifat kriminal seperti pada kasus Ross Ulbricht yang mendirikan situs *Silk Road. Silk Road* merupakan pasar anonim di dunia maya yang merupakan surga bagi para bandar narkoba, pedagang senjata dan pemalsuan dokumen. Kasus lainnya adalah *ransomware* dimana sekelompok orang "menyandera" data penting institusi pemerintahan dan meminta

tebusan dalam bentuk *bitcoin*. Di sisi lain kasus bobolnya penyedia layananan *bitcoin* seperti MtGox dan BitFinex juga menyebabkan aspek keamanan cryptocurrency masih menjadi perhatian.

5. Diskusi dan Pembahasan

Berdasarkan temuan-temuan terkait implementasi dan pemanfaatan teknologi *blockchain* akan dibahas dengan sudut pandang negara Indonesia, dengan memisahkan keberadaannya sebagai peluang dan ancaman.

5.1. Teknologi *Blockchain* Sebagai Peluang.

Pemerintah Indonesia melalui Kementerian Pertahanan saat ini sedang melaksanakan pemutakhiran alat utama sistem persenjataan (alutsista) TNI untuk memperkuat postur kekuatan TNI sebagai alat pertahanan negara. Disamping pemutakhiran alutsista, pemerintah juga sedang membangun dan mengembangkan industri pertahanan untuk mengejar ketertinggalan penguasaan industri dan teknologi pertahanan dari negara-negara maju.

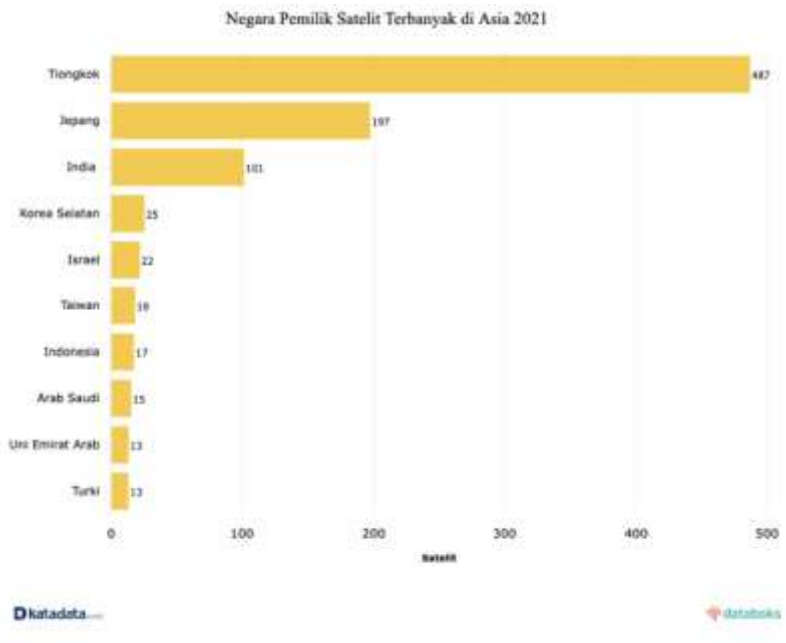
Dalam mewujudkan kebijakan pemerintah di bidang pengembangan industri pertahanan, maka saat ini Indonesia telah memiliki 10 industri strategis yang mendukung untuk memproduksi alat-alat pertahanan. Untuk mendukung industri strategis tersebut, peranan Pemerintah, Perguruan Tinggi, dan Lembaga-lembaga penelitian baik yang dikelola oleh pemerintah maupun swasta sangat diperlukan dalam melakukan penelitian, pengembangan, maupun penerapan (Marpaung, 2020).

Pemanfaatan teknologi *blockchain* dalam pengembangan teknologi dan industri pertahanan berpotensi membawa kemajuan pada teknologi pertahanan Indonesia beberapa langkah kedepan. Hal ini juga sejalan dengan arahan Presiden Joko Widodo dalam rapat pimpinan Kementerian Pertahanan tanggal 23 Januari 2020 di Jakarta, bahwa dalam pengembangan teknologi dan industri pertahanan perlu memperhatikan lompatan teknologi yang mungkin terjadi dalam jangka waktu 20,

30, 50 tahun yang akan datang. Salah satu bentuk nya adalah kemunculan teknologi *blockchain.*

Menteri Pertahanan Prabowo Subioanto dalam Taklimat yang disampaikan kepada Sivitas Akademika Universitas Pertahanan, pada tanggal 29 Oktober 2021, di Bogor menyatakan bahwa interkoneksi komunikasi antara pasukan darat, laut dan udata menjadi salah satu target utama dalam pengembangan teknologi pertahanan saat ini. Dengan adanya interkonektifitas, maka pasukan darat, laut dan udara yang bergerak dalam satu operasi dapat saling berkoordinasi untuk kesuksesan pelaksanaan operasi. Namun interkonektifitas komunikasi juga membawa kerentanan yang dapat dieksploitasi oleh musuh untuk memalsukan perintah dan informasi sehingga terjadi kekacauan dan kegagalan koordinasi di daerah operasi. Ancaman ini dapat dieliminasi dengan manfaatkan teknologi *blockchain* untuk memverifikasi perintah dan informasi di medan perang.

Berdasarkan data dari situs pelacak satelit N2YO.COM, situs katadata.com membuat daftar negara pemilik satelit terbanyak di Asia. Indonesia masuk dalam 10 Negara pemilik satelit terbanyak di Asia pada tahun 2021. Dengan jumlah satelit aktif sebanyak 17 buah, Indonesia berada pada urutan ke tujuh diatas Arab Saudi yang memiliki 15 satelit dan dibawah Taiwan yang memiliki 18 Satelit (Rizaty, 2021).



Gambar 5. Grafik Negara Pemilik Satelit Terbanyak di Asia Tahun 2021

Dengan kepemilikan jumlah satelit yang cukup banyak tersebut, pengelola Satelit Indonesia juga memiliki kerawanan yang sama dengan NASA terkait dengan komunikasi dan kendali pesawat ruang angkasa atau satelit. Potensi ancaman kendali tidak sah terhadap satelit-satelit milik Indonesia juga perlu menjadi perhatian.

Untuk mengatasi potensi ancaman tersebut teknologi *blockchain* memberikan peluang melalui fitur otentikasi multi factor dan otorisasi multi-pihak untuk memastikan bahwa perintah yang diberikan kepada satelit-satelit milik Indonesia benar-benar dikirimkan oleh pihak-pihak yang berwenang.

Peluang yang sama juga ditemukan pada potensi-potensi pemanfaatan teknologi *blockchain* dalam bidang pertahanan lainnya seperti pengamanan rantai pasokan dan logistik, kendali sistem senjata serta peningkatan transparansi pengadaan barang dan jasa bidang pertahanan.

5.2. Teknologi *Blockchain* Sebagai Ancaman

Dari sudut pandang ancaman, sampai saat ini potensi yang ditimbulkan oleh teknologi *blockchain* masih terkait dengan implementasi pada sektor ekonomi yaitu

pemanfaatannya sebagai basis mata uang kripto (*cryptocurrency)* yang dapat dimaatkan untuk kegiatan kriminal di dunia maya. Potensi pemanfaatannya sebagai sarana pencucian uang juga berpotensi dimanfaatkan untuk pendanaan terorisme di Indonesia. Selain itu perdagangan gelap senjata api, narkoba dan benda-benda terlarang lainnya juga dapat terjadi dengan memanfaatkan mata uang kripto karena bersifat anonim sehingga menyulitkan penelusuran oleh aparat penegak hukum.

Bank Indonesia selaku otoritas pembayaran di Indonesia telah menetapkan bahwa mata uang kripto tidak diakui sebagai alat pembayaran yang sah di Indonesia. Hal tersebut sesuai dengan ketentuan dalam Undang-Undang No. 7 tahun 2011 tentang Mata Uang yang menyatakan bahwa mata uang adalah uang yang dikeluarkan oleh Negara Kesatuan Republik Indonesia dan setiap transaksi yang mempunyai tujuan pembayaran, atau kewajiban lain yang harus dipenuhi dengan uang, atau transaksi keuangan lainnya yang dilakukan di Wilayah Negara Kesatuan Republik Indonesia wajib menggunakan Rupiah .

6. Kesimpulan

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa bahwa teknologi *blockchain* dalam kajian peperangan asimeris memberikan peluang pemanfaatan yang luas dalam perspektif negara Indonesia. Ancaman yang ditimbulkan oleh teknologi *blockchain* pada saat ini baru ditemukan sebatas pada pemanfaatannya sebagai basis mata uang kripto yang dapat dimanfaatkan dalam kegiatan kriminal di dunia maya, salah satunya berpotensi disalahgunakan dalam tindak pidana pendanaan terorisme.

Daftar Pustaka

Adams, V. (2019). Why Military Blockchain is Critical in the Age of Cyber Warfare: 4 ways blockchain can secure and defend key military assets and weapons systems. *Consensys*.

Barnas, N. B. (2016). *Blockchains In National Defense: Trustworthy Systems In A Truthless World*.

Chatterjee, R., & Chatterjee, R. (2018). An Overview of the Emerging Technology: Blockchain. *Proceedings - 2017 International Conference on Computational Intelligence and Networks, CINE 2017*, 126–127. https://doi.org/10.1109/CINE.2017.33

Clausewitz, C. von. (1873). *https://www.clausewitz.com/readings/OnWar1873/TOC.htm*. Clausewitz, On War Trans. COL James John Graham (London: N. Trübner, 1873).

Marpaung, C. O. P. (2020). *Kebijakan Pengembangan IPTEK Industri Pertahanan Untuk Pembangunan Nasional*.

Rizaty, M. (2021). *Daftar Negara Pemilik Satelit Terbanyak di Asia, Indonesia Peringkat Berapa?* Https://Databoks.Katadata.Co.Id/Datapublish/2021/09/27/Daftar-Negara-Pemilik-Satelit-Terbanyak-Di-Asia-Indonesia-Peringkat-Berapa.

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. PT. Alfabeta.

Sutrisno, B. (2018). *Blockchain dan Cryptocurrency: Peran Teknologi Menuju Inklusi Keuangan?. Repositori Penelitian Universitas Terbuka*.

The Value Technology Foundation. (2020). Potential-Uses-of-Blockchain-Technology-In-DoD. *Potential Uses of Blockchain By The U.S. Departement of Defense, Washington D.C.*

Walzer, Michael. (2006). *Just and unjust wars : a moral argument with historical illustrations*. Basic Books.