# Review Paper Tentang Blockchain - Putri

| **Judul Paper** | A survey of cyber attacks on blockchain based IoT systems  for industry 4.0 |
| --- | --- |
| **Tentang** | Aarju Dixit, Aditya Trivedi, dan W. Wilfred Godfrey  DOI: 10.1049/blc2.12017 |
| **Abstrak** | Revolusi industri 4.0 dipimpin oleh teknologi seperti buku besar digital terdistribusi, teknik pemrosesan data besar, otomatisasi, dan internet of things (IoT). Minat terhadap industrial internet of things (IIoT) telah berkembang pesat dengan area internet yang sangat luas seperti penelitian, akademisi, dan industri. Melalui pendekatan terdesentralisasi dan terdistribusi, blockchain dan IIoT memastikan keamanan maksimum. Dalam pendekatan terdistribusi, setiap blok dirangkai satu sama lain. Makalah ini menyajikan survei tentang industri 4.0 dan sistem berbasis blockchain. Integrasi blockchain, perangkat IoT, dan industri 4.0 memberikan keamanan, transparansi, dan skalabilitas ke sistem. Makalah ini juga membahas banyak jenis serangan dunia maya dan kemungkinan solusi untuk sistem industri internet of things (IOT) berbasis blockchain. |
| **Pendahuluan** | Salah satu komponen penting dari industri 4.0 disebut sebagai industrial internet of things (IIoT). Selanjutnya, di  masa depan, pilar industri 4.0 diproyeksikan menjadi  teknologi blockchain.  Pendahuluan paper ini menjelaskan tentang masa depan blockchain untuk industri 4.0. Ini membahas teknologi IOT yang semakin meningkat pesat, karena Di industri 4.0, alat dan teknik manufaktur canggih digunakan saling berhubungan dengan perangkat IoT yang menghasilkan dan menganalisis data. Pengaturan seperti itu perangkat sensor di pabrik dapat membantu memvisualisasikan seluruh lini produksi untuk membuat sistem bergantian. Namun, terdapat masalah disini, yaitu masalah keamanan dan privasi di industri 4.0 yang telah meningkat berkali-kali lipat, mengakibatkan interkoneksi liberal antar perangkat dan hal itu membuat aplikasi semakin rentan terhadap kebocoran informasi, pelanggaran data, dan kerugian finansial. Dengan tidak adanya arsitektur aman yang kuat, kerahasiaan dan integritas aplikasi tersebut dapat dirugikan oleh DDoS, serangan spoofing protokol resolusi alamat (ARP), perubahan kecepatan data, kemacetan jaringan, manipulasi, gangguan kebisingan, phishing, dan ancaman konfigurasi.  Dalam paper ini, membahas deskripsi sistem industrial IOT berbasis blockchain umum, studi kasus dari sistem yang digunakan industri 4.0, blockchain dan IOT, dan gambaran tentang beberapa tantangan keamanan serta kemungkinan solusi untuk IOT-nya. |
| **Konten** | Adapun pembahasan dalam paper ini adalah terkait:   * Industri IOT berbasis blockchain. Dalam hal ini penulis menjelaskan tentang jenis-jenis lapisan arsitektur IoT industri yang diaktifkan blockchain dan Arsitektur sistem industri IO berbasis blockchain. * Kemungkinan serangan terhadap sistem IOT industri berbasis blockchain. Dalam hal ini penulis menjelaskan tentang (1)serangan-serangan yang mengeksploitasi arsitektur blockchain, protokol, dan komponennya. Adapun serangan-serangan yang disebutkan adalah Serangan berbasis kontrak cerdas (DAO), (2)Serangan berbasis buku besar konsensus. Hal ini mencakup serangan 51 persen, Serangan Finney dan Serangan ras. Selanjutnya (3)Serangan jaringan peer to peer mencakup Serangan Distributed denial of service (DDoS), Serangan Sybil, dan Serangan gerhana. Tidak hanya itu, Penulis juga membahas tentang (4)Serangan jaringan lainnya, yaitu serangan penyadapan dan serangan rute. (5)Serangan pada perangkat lunak seperti virus, kuda troya, cacing logika, cacing, dan DoS. (6) Serangan fisik yaitu serangan kekerasan dan serangan buffer overflow. (7) Serangan main-in-the-middle (MITM). (8) Serangan on-off. (9)Serangan penolakan layanan (DNS) meliputi serangan cryptojacking, serangan double spending, serangan liveness, kelenturan transaksi. (10)Serangan terhadap light-client blockchain yaitu serangan pengelabuan dan serangan amnesia. * Studi kasus. (1) Sistem reputasi anonim berbasis blockchain. (2) Sistem pemantauan status perangkat lunak berbasis blockchain. (3) Sistem rantai pasokan berbasis blockchain. Setiap studi kasus membahas pengaplikasian sistem reputasi, Kesimpulan dan kemungkinan serangan dari arsitektur yang dipilih, dan sistem arsitektur dari sistemnya. * Terakhir, penulis menuliskan saran dan menjelaskan tentang pencegahan terhadap setiap jenis serangan. |
| **Kesimpulan** | Paper ini melakukan studi tentang IIoT dan blockchain. Kombinasi kedua teknologi ini telah dijadikan BIIoT. Makalah ini mencakup sebagian besar poin penting tentang blockchain, IIoT mengenai kemungkinan serangan, industri di mana sistem BIIoT digunakan, dll. Penelitian yang ada yang telah dilakukan di bidang sistem BIIoT, paper ini memberikan survei tentangnya. Representasi umum arsitektur dan komponen BIIoT telah diberikan dalam makalah ini. Setelah mempelajari sistem IIoT berbasis blockchain, dapat dikatakan bahwa sistem BIIoT sangat tangguh terhadap peretasan dan serangan luar lainnya. Risiko kehilangan data mereka sangat kecil. Itu dapat menyimpan semua node di blockchain. |
| **Opini** | Paper ini telah membahas tentang serangan siber pada sistem IoT berbasis blockchain untuk industri 4.0. Dalam paper tersebut, penulis melakukan survei terhadap berbagai serangan yang dapat menargetkan sistem IoT berbasis blockchain, serta memberikan penjelasan tentang mekanisme blockchain yang dapat digunakan untuk mencegah serangan tersebut.  Kelebihan dari paper ini adalah memberikan tinjauan menyeluruh tentang serangan siber pada sistem IoT berbasis blockchain. Selain itu, paper ini juga memberikan penjelasan rinci tentang mekanisme blockchain yang dapat digunakan untuk melindungi sistem tersebut dari serangan.  Namun, kelemahan dari paper ini adalah tidak memberikan solusi atau rekomendasi yang konkret tentang cara melindungi sistem IoT berbasis blockchain dari serangan siber. Selain itu, paper ini juga cenderung fokus pada teknologi blockchain, sehingga kurang membahas tentang aspek-aspek non-teknis seperti faktor manusia dan kebijakan keamanan yang dapat mempengaruhi keamanan sistem IoT berbasis blockchain. |

| **Judul Paper** | Regional Blockchain for Vehicular Networks to Prevent 51% Attacks |
| --- | --- |
| **Tentang** | Akesh Shrestha dan Seung Yeob Nam.  DOI: 10.1109/ACCESS.2019.2928753 |
| **Abstrak** | Kendaraan generasi berikutnya akan bersifat otonom, terhubung, elektrik, dan cerdas dengan kebutuhan yang berbeda seperti mobilitas tinggi, latensi rendah, aplikasi real-time, konektivitas tanpa batas, dan keamanan. Blockchain dapat memberikan solusi yang baik untuk masalah penyebaran pesan yang aman atau berbagi informasi yang aman di jaringan kendaraan dengan hubungan kepercayaan yang lemah di antara node. Dalam makalah ini, kami menyelidiki desain blockchain regional untuk VANET, di mana blockchain dibagi di antara node di area yang dibatasi secara geografis. Kami menyelidiki cara merancang blockchain regional sambil mencapai probabilitas keberhasilan serangan 51% yang rendah. Kami memperoleh kondisi yang menjamin probabilitas keberhasilan serangan 51% yang rendah dalam hal jumlah node baik dan node jahat, waktu pengiriman pesan, dan waktu komputasi teka-teki. Kondisi tersebut dapat memberikan pedoman yang berguna untuk pemilihan beberapa parameter kontrol yang menjamin operasi blockchain yang stabil. Kami menjalankan beberapa simulasi untuk menunjukkan validitas kondisi dan menyelidiki pengaruh berbagai parameter pada probabilitas keberhasilan serangan 51%. Hasil analisis dan simulasi kami menunjukkan bahwa mempertahankan waktu pengiriman pesan yang rendah untuk node yang baik sangat penting dalam melindungi stabilitas sistem blockchain. |
| **Pendahuluan** | Membahas tentang perkembangan kendaraan pintar dan otonom, serta peran jaringan kendaraan dalam mengontrol lalu lintas dan manajemen parkir. Menguraikan tentang penggunaan sensor yang terpasang pada kendaraan untuk mengidentifikasi perubahan jalur, peringatan tabrakan, dan batasan jangkauan sensor. Selain itu juga menjelaskan tentang komunikasi kendaraan-ke-kendaraan (V2V) dan kendaraan-ke-infrastruktur (V2I) yang penting dalam pertukaran pesan antara kendaraan. Namun, terdapat risiko keamanan dalam komunikasi VANET, seperti serangan penyadapan, jamming, dan spoofing. Oleh karena itu, dibutuhkan mekanisme keamanan yang dapat mengatasi masalah tersebut. Salah satu solusinya adalah menggunakan teknologi blockchain untuk menyimpan riwayat peristiwa lalu lintas atau kecelakaan. Dengan menggunakan teknologi blockchain, semua informasi dapat disimpan secara transparan dan dibagikan secara global, sehingga dapat memastikan keamanan dan privasi dalam aplikasi tersebut. |
| **Konten** | Bagian II menyajikan latar belakang dan penelitian terkait tentang blockchain. Bagian III membahas blockchain regional dan penggunaannya dalam VANET. Bagian IV membahas tentang penyerang model penyerang yang menargetkan blockchain regional. Bagian V menurunkan kondisi untuk probabilitas keberhasilan yang rendah dari kekekalan serangan, dan memberikan pedoman untuk pemilihan yang berbeda parameter kontrol. Pada Bagian VI, kami menjelaskan lingkungan simulasi dan mendiskusikan hasil numerik. Bagian VII menyelidiki masalah-masalah utama yang berkaitan dengan penundaan pesan, dengan kemungkinan penanggulangan untuk blockchain regional. Akhirnya, Bagian VIII menyimpulkan makalah ini. |
| **Kesimpulan** | Blockchain regional adalah jenis blockchain yang digunakan oleh anggota di area terbatas. Keuntungan dari penggunaan blockchain regional adalah waktu pengiriman pesan menjadi lebih singkat dan waktu perhitungan teka-teki juga dapat dikurangi. Namun, belum ada panduan mengenai waktu komputasi teka-teki baru untuk blockchain regional. Dalam penelitian ini, para peneliti mengeksplorasi cara merancang blockchain regional yang aman untuk jaringan kendaraan menggunakan beberapa parameter blockchain. Mereka menunjukkan bahwa waktu komputasi teka-teki mempengaruhi keamanan blockchain terutama dalam hal serangan kekekalan atau 51%. Mereka menemukan kondisi stabilitas yang dapat menjamin probabilitas keberhasilan serangan kekekalan yang rendah dengan memperhatikan jumlah node yang baik dan jahat, waktu pengiriman pesan, dan rata-rata waktu komputasi teka-teki. Mereka juga meneliti pengaruh setiap faktor kontrol pada probabilitas keberhasilan serangan kekekalan secara rinci melalui simulasi. Para peneliti menemukan bahwa penundaan pengiriman pesan antara node baik dan node jahat sangat penting dalam menjaga stabilitas blockchain regional. Mereka juga menyelidiki cara untuk mewujudkan penundaan pengiriman pesan yang rendah di antara node yang baik di jaringan kendaraan. Namun, penelitian ini hanya mengasumsikan kedalaman rantai awal yang cukup besar untuk menjaga stabilitas sistem blockchain. Hubungan matematis antara kedalaman rantai awal dan probabilitas keberhasilan serangan kekekalan akan diselidiki lebih lanjut di masa depan. |
| **Opini** | Kekurangan dari paper ini adalah bahwa analisis stabilitas sistem blockchain hanya dilakukan melalui simulasi dan belum diuji coba di dunia nyata. Selain itu, paper ini hanya mengeksplorasi beberapa faktor kontrol untuk mencapai stabilitas sistem blockchain, dan masih memerlukan penelitian lebih lanjut untuk mengungkap faktor lain yang mungkin mempengaruhi stabilitas.  Namun, kelebihan dari makalah ini adalah membahas solusi untuk mengatasi masalah keamanan pada jaringan kendaraan, yaitu serangan 51%. Penggunaan blockchain regional dianggap dapat mengurangi waktu pengiriman pesan dan waktu perhitungan puzzle yang memungkinkan solusi ini lebih cepat dan efektif dalam mengatasi serangan 51%. Selain itu, paper ini memberikan panduan dalam merancang blockchain regional yang aman untuk jaringan kendaraan.  Namun, meskipun paper ini menunjukkan potensi solusi yang menarik, tetap diperlukan penelitian lebih lanjut untuk menguji dan memvalidasi solusi ini sebelum diimplementasikan secara luas di dunia nyata. |