Jurnal Nasional Teknologi Komputer
Vol.2; No: 1; Januari 2022
Website: publikasi.hawari.id/index.php/jnastek
E-ISSN: 2808-4845; P-ISSN: 2808-7801

Makalah Penelitian

MENGGUNAKAN TEKNOLOGI BLOCKCHAIN UNTUK MEMASTIKAN KEAMANAN

Nesterenko R.V.[1], Maslova M.A.[2]

[1,2]Sistem Komputer, Universitas Pembangunan Panca Budi

Corresponding Author: Nesterenko R.V.

ABSTRACT

The use of Blockchain in the Internet of Things networks is an innovative approach that can make communication between devices of such a network distributed, autonomous and secure. The blockchain in this context is a set of cryptographically connected blocks. Transactions in the network act as the main carriers of information about the state of the nodes, as well as the output information of the nodes themselves for the autonomous functioning of the network. A node is a "smart" device, a sensor, or a microcontroller that connects a group of sensors. Blockchain will be used to provide secure data transmission and processing of devices in the Internet of Things network. This article discusses the main opportunities and challenges in the application of technology in distributed networks.
Keywords: Internet of Things, Blockchain, peer-to-peer network, proof of authentication, a Decentralized Network

ABSTRAK

Penggunaan Blockchain dalam jaringan Internet of Things adalah pendekatan inovatif yang dapat membuat komunikasi antar perangkat jaringan seperti itu terdistribusi, otonom, dan aman. Blockchain dalam konteks ini adalah sekumpulan blok yang terhubung secara kriptografis. Transaksi dalam jaringan bertindak sebagai pembawa utama informasi tentang keadaan node, serta informasi keluaran dari node itu sendiri untuk fungsi jaringan yang otonom. Node adalah perangkat "pintar", sensor, atau mikrokontroler yang menghubungkan sekelompok sensor. Blockchain akan digunakan untuk menyediakan transmisi data yang aman dan pemrosesan perangkat di jaringan Internet of Things. Artikel ini membahas tentang peluang dan tantangan utama dalam penerapan teknologi pada jaringan terdistribusi.

Kata Kunci: Internet of Things, Blockchain, jaringan peer-to-peer, bukti otentikasi, Jaringan Terdesentralisasi

1. Pendahuluan

Dengan kemajuan teknologi komunikasi dan pengenalan jaringan 5G di mana-mana, teknologi Internet of Things mulai berkembang pada tingkat yang eksponensial. Rumah pintar, kota pintar, e-Health, Internet of Things untuk perusahaan industri, intelijen terdistribusi, dan sistem lainnya adalah cara yang efektif dan akrab bagi masyarakat untuk meningkatkan banyak proses, misalnya, proses irigasi tanaman berdasarkan sensor dan proses lain yang dapat menjadi otomatis. Pendekatan proses seperti itu mengurangi pengaruh faktor manusia dan berkontribusi pada peningkatan efisiensi perusahaan, di mana ada semua prasyarat untuk penggunaan teknologi IoT. Terlepas dari semua efektivitas dan prevalensinya, teknologi Internet of Things memiliki banyak tantangan dan masalah yang terkait dengan keamanan dan konfigurasi perangkat IoT yang aman. Keberadaan sejumlah besar perangkat semacam itu penuh dengan bahaya, karena penyerang dapat mengendalikannya dan mengatur

serangan DDoS dan manipulasi lalu lintas lainnya menggunakan perangkat IoT, yang mengirim perangkat ini ke server. Salah satu contoh serangan terpadu pada beberapa perangkat IoT adalah botnet. Botnet adalah kumpulan perangkat yang disusupi di bawah kendali penyerang. Mirai adalah worm dan botnet yang dibentuk oleh perangkat yang diretas (disusupi) seperti Internet of Things (pemutar video, webcam pintar, dll.). Botnet ini meretas perangkat dengan menebak kata sandi untuk port 23 (telnet). Dalam sistem IoT terpusat, terkadang cukup untuk meretas server atau mikrokontroler yang bertanggung jawab untuk komunikasi antara sekelompok besar perangkat agar dapat mengontrol semua perangkat yang berkomunikasi melalui protokol terpusat dengan server yang dikompromikan [1, 3, 8].

2. Tinjauan Pustaka

pendekatan terdesentralisasi terhadap internet of things. Pemusatan sistem tata kelola IoT dapat menjadi kerentanan, karena arsitektur seperti itu secara signifikan mengurangi waktu yang diperlukan untuk semua perangkat dalam jaringan semacam itu untuk dikendalikan oleh penyerang.

Jalan keluarnya adalah dengan menggunakan pendekatan terdesentralisasi untuk mengatur jaringan seperti itu, di mana setiap perangkat bertindak sebagai simpul independen. Dalam kasus komunikasi seperti itu, penyerang harus mengkompromikan setiap perangkat, bukan hanya server pusat. Penggunaan protokol komunikasi terpusat dalam jaringan terdesentralisasi tidak cukup aman dan efektif.

Menggunakan teknologi Blockchain untuk mengatur komunikasi antar perangkat dalam jaringan seperti itu adalah solusi yang paling tepat, karena bagaimana informasi akan ditransfer dalam bentuk transaksi yang aman dan ditandatangani yang harus dicatat dalam buku besar yang didistribusikan di setiap node.

Pendekatan ini memberikan manfaat berikut dan properti interaksi perangkat dalam jaringan terdistribusi [5, hal. 3].

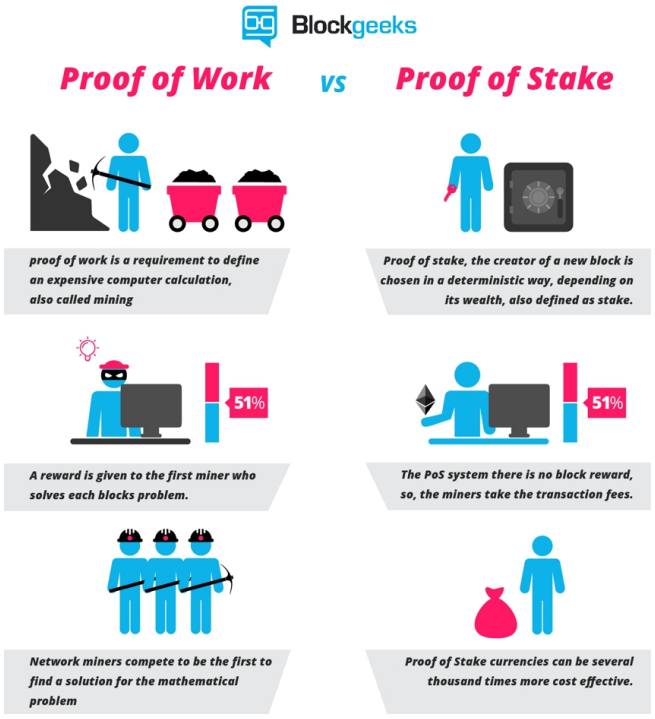
a. decentralization;
b. safety;
c. identification;
d. network flexibility;
e. autonomy of the network;
f. reliability of information.

Desentralisasi melibatkan menghilangkan masalah keamanan dari pendekatan terpusat untuk mengatur Internet of Things, meningkatkan margin kesalahan, tetapi juga meningkatkan efektivitas jaringan dan keamanan tersebut. Transaksi antar node aman, ditandatangani dengan kunci rahasia node pengirim dan diverifikasi oleh node penerima, sehingga keamanan dan identifikasi terjamin. Setiap saat, sejumlah perangkat dapat dihubungkan ke jaringan, yang akan menerima salinan buku besar terdistribusi terbaru - sehingga memastikan fleksibilitas jaringan. Otonomi kerja terdiri dari ketidakmungkinan menangguhkan operasi seluruh jaringan, menonaktifkan salah satu komponennya, seperti yang dapat terjadi di jaringan terpusat ketika server rusak. Keandalan informasi dalam jaringan terletak pada kenyataan bahwa blok buku besar yang didistribusikan hanya akan berisi transaksi yang diverifikasi oleh penambang atau sebaliknya, yang berisi informasi keluaran perangkat [2, 4].

Desentralisasi dan organisasi jaringan peer-to-peer menunjukkan tingkat keamanan, keandalan, fleksibilitas jaringan yang tinggi, dan kemungkinan operasi otonom dari bagian-bagiannya.

3. Hasil dan Pembahasan

Pertimbangkan konsensus yang efektif dan penyimpanan buku besar yang didistribusikan. Dengan semua Tantangan berikut tetap relevan dengan keuntungan jaringan terdesentralisasi: bagaimana menyimpan buku besar terdistribusi pada sebuah node dan algoritma konsensus mana yang digunakan untuk operasi jaringan yang efisien.



Gambar 1. Bukti Kerja dan Bukti Saham

Proof-of-work (bukti kerja) adalah algoritme jaringan Bitcoin standar yang memungkinkan, berdasarkan bukti beberapa perhitungan kompleks, untuk membuktikan pekerjaan yang dilakukan untuk memverifikasi transaksi dan menutup blok secara kriptografis. Dalam jaringan yang sangat besar, algoritma konsensus ini ternyata sangat mahal dalam hal energi yang dikeluarkan untuk perhitungan verifikasi dan penutupan blok.

Jaringan Internet of Things harus menyediakan komunikasi dan pengambilan keputusan dalam mode waktu nyata. Persyaratan ini membuat bukti kerja tidak efektif untuk memecahkan masalah. Karena dalam jaringan Internet of Things tertutup, bukti kerja perangkat itu sendiri harus digunakan - pengoperasian jaringan semacam itu dapat terganggu karena beban tinggi pada perangkat saat menghitung bukti kerja.

Seorang penambang dianggap sebagai anggota jaringan yang tertarik untuk mempertahankan kinerja. jaringan seperti itu untuk beberapa hadiah. Dimungkinkan untuk mengatur jaringan terdistribusi berdasarkan bukti kerja hanya dengan membuat Internet of Things terbuka untuk penambang eksternal. Dalam kasus seperti itu, Anda harus memastikan keterlibatan penambang yang cukup tinggi sehingga tidak ada penundaan dalam pembuatan blok baru dan tidak ada beban tambahan pada node dalam jaringan.

Solusi lain mungkin memilih algoritma konsensus bobot yang lebih ringan. Misalnya, Proof-of-Stake atau bukti bagian. Algoritme konsensus ini lebih sedikit menuntut sumber daya daripada bukti kerja (lihat Gambar 1). Namun, sesuai dengan [7, hal. 2], algoritma konsensus yang disukai dan ringan untuk internet terdistribusi adalah Proof-of-Authentication.

Untuk mengimplementasikan algoritma ini, perlu untuk menyimpan dalam tabel komunikasi umum yang cocok dengan kunci publik dan alamat MAC perangkat.

Bukti otentikasi dapat diimplementasikan sebagai berikut [6, p.9]:

a. Node tepercaya dipilih.
b. Node yang tidak dipercaya mengumpulkan transaksi ke dalam blok.
c. Node yang tidak dipercaya menandatangani blok dan mengirimkannya ke semua node tepercaya.
d. Node tepercaya cocok dengan kunci publik node dan alamat MAC-nya.
e. Jika semua node terpercaya telah berhasil mengotentikasi node yang mengirim blok, maka blok ini dikirim ke semua node jaringan.
f. Saat menerima blok, node lainnya menemukan hash dari header dan membuka blok baru dengan nilai hash ini di bidang "Hash sebelumnya".

Jika node tepercaya tidak dapat mengotentikasi blok dan node yang mengirim blok, maka peringkat kepercayaan turun 1. Dengan peringkat kepercayaan rendah, penugasan ulang terjadi pada host tepercaya di jaringan. Algoritme ini memungkinkan Anda untuk sangat mengurangi beban pada perangkat, serta memberikan verifikasi keaslian informasi yang dikirim menggunakan mekanisme EDS. Menggunakan algoritme di atas selain konsensus algoritme yang kuat juga membantu meningkatkan keamanan data yang disimpan.

Penyimpanan buku besar terdistribusi dapat diimplementasikan di cloud, sehingga setiap node memiliki kemampuan untuk mengakses bagian cloud-nya. Dengan demikian, data tidak akan menempati ruang pada perangkat itu sendiri.

Dimungkinkan juga untuk menyimpan tidak semuanya, tetapi hanya blok yang paling relevan dengan data di perangkat. Metode ini akan memungkinkan Anda untuk menolak berinteraksi dengan cloud, dan juga akan menghemat memori node itu sendiri.

4. Kesimpulan

Penerapan teknologi Blockchain dalam organisasi jaringan terdistribusi yang aman, Internet of Things adalah teknologi yang sangat menjanjikan dan inovatif. Pendekatan dalam jaringan terdistribusi organisasi ini memungkinkan untuk memastikan, pertama-tama, otonomi node, tingkat keamanan infrastruktur dan elemen Internet of Things yang tinggi, serta identifikasi dengan menggunakan EDS. Namun, penerapan teknologi ini memiliki beberapa keterbatasan:

algoritma konsensus standar tidak sesuai karena keterikatannya dengan penambang eksternal atau karena konsumsi daya yang tinggi, namun, bukti algoritma otentikasi dapat diandalkan sebagai algoritma konsensus untuk jaringan di mana node dari jaringan itu sendiri bertindak sebagai penambang. Algoritma ini mampu memberikan kecepatan perangkat dan komunikasi yang dibutuhkan secara real time. Penyimpanan data dapat diimplementasikan dengan dua yang diusulkan dalam artikel ini. cara:

a. menyediakan akses node ke bagian cloud tempat salinan registri akan disimpan,
b. menyimpan hanya blok yang paling relevan dalam memori node itu sendiri, memberikan kemudahan registri tersebut.

REFERENSI

[1] Afonkin A.Yu., Nozdrina N.A. Prospects for the development of blockchain technology in the near future // Scientific trends: Questions of exact and technical sciences / Collection of scientific papers based on the materials of the XVI International Scientific Conference. 2018. p. 20-21.

[2] Goncharenko Yu.Yu., Arzamassev D.A. Program module for monitoring and maintaining electronic document management based on blockchain technology. Research Result. Information Technologies. Vol. 5, No. 3, 2020

[3] Goncharenko Yu.Yu., Pavo F.N. Development of a decentralized application for implementing digital identity using blockchain technology // Bulletin of the Ural Federal District No. 3 (29), 2018, pp. 23-28.

[4] Mikhalenko Yu.A., Kryukova A.A. Blockchain as one of the elements of state digitalization // Bulletin of Eurasian Science, 2018 No. 1, https://esj.today/PDF/10ECVN118.pdf

[5] Alam, Tanweer. (2019). Blockchain and its Role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 151-157. 10.32628/CSEIT195137.

[6] Deepak Puthal and Saraju P. Mohanty and Venkata P. Yanambaka and Elias Kougianos (2020). PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks

[7] Puthal, Deepak & Mohanty, Saraju. (2019). Proof of Authentication: IoT-Friendly Blockchains. IEEE Potentials. 38. 26-29. 10.1109/MPOT.2018.2850541.

[8] Gorshkova S. New technologies in the service of intellectual property law: blockchain, artificial intelligence, virtual reality. // Collection of scientific papers of the IX International Legal Forum (IP Forum). // egal protection of intellectual property: Problems of Theory and Practice Moscow, February 12-13, 2021.

******