KOMPUTASI UBIQUITOUS DAN PERVASIF

51% ATTACK PADA BLOCKCHAIN

222L1

Disusun Oleh :

Chosmas Marzuki	09021182025003
Karinda Amelia	09021282025054
Tiara Aprisa	09021182025005

Dosen Pengampu:

Adi Hermansyah, S.Kom., M.T.

Huda Ubaya, M.T.

SEMESTER GENAP 2022/2023

JURUSAN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

51% ATTACK PADA BLOCKCHAIN

Judul jurnal :

1. *Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack*
2. *Regional Blockchain for Vehicular Networks to Prevent 51% Attacks*
3. *Short Selling Attack: A Self-Destructive But Profitable 51% Attack On PoS Blockchains*

A. Pendahuluan

Blockchain adalah teknologi yang berbasis pada jaringan tersentralisasi, di mana informasi dan transaksi disimpan secara terbuka dan transparan. Blockchain adalah platform komputasi tersentralisasi dan terdistribusi yang muncul yang mendukung aplikasi cryptocurrency seperti Bitcoin, dan dapat memberikan keamanan dan privasi untuk aplikasi tersebut.

Salah satu keunggulan dari teknologi blockchain adalah keamanan yang terjamin, karena setiap transaksi harus diverifikasi dan diotorisasi oleh jaringan node yang terhubung. Setiap perubahan pada blockchain bersifat transparan dan dapat dilihat secara publik oleh semua node jaringan, dan informasi yang terekam tidak dapat dipalsukan dengan mudah.

Seperti teknologi lainnya, blockchain juga memiliki kelemahan yang dapat dimanfaatkan oleh penyerang. Salah satu jenis serangan siber yang paling serius dan mematikan bagi blockchain adalah 51% attack. Serangan 51% adalah teknik yang bermaksud untuk melakukan fork pada blockchain untuk melakukan pembelanjaan ganda. Musuh yang mengendalikan lebih dari setengah kekuatan hashing total jaringan dapat melakukan serangan ini. Karena biaya serangan yang sangat besar untuk melakukan serangan 51%, itu dianggap sangat tidak mungkin untuk waktu yang lama. Namun, belakangan ini, serangan itu sering terjadi, menelan biaya jutaan dolar untuk berbagai mata uang kripto. Strategi serangan 51% bervariasi berdasarkan mekanisme konsensus yang diadopsi oleh mata uang kripto tertentu, dan ini memungkinkan penyerang untuk membelanjakan koin kripto yang sama, membatasi transaksi, membatalkan blok, dan bahkan memiliki kontrol penuh atas harga mata uang kripto. Koin kripto dengan kekuatan hashing rendah selalu terancam oleh serangan 51% karena hashing yang mudah dicapai.

B. Teknologi Blockchain dan Mekanisme Konsensus

1. Teknologi Blockchain : Konsep Digital

Blockchain adalah teknologi yang revolusioner dalam hal penyimpanan dan pengiriman data digital. Konsep dasar dari blockchain adalah menciptakan suatu database yang tersentralisasi dan terbuka, dimana transaksi dan informasi disimpan dalam blok-blok terpisah dan saling terkait satu sama lain secara kriptografis. Teknologi Blockchain terdiri dari catatan data yang disebut sebagai buku besar. Ini

menggunakan sistem terdistribusi untuk verifikasi catatan. Blok diverifikasi oleh ribuan peserta jaringan di seluruh dunia untuk menjaga jaringan tetap aktif.

Dalam konsep digital, blockchain dapat dijelaskan sebagai berikut:

1. Terdesentralisasi
   Pada sistem tradisional, data biasanya disimpan secara terpusat di satu lokasi atau server. Namun, blockchain memperkenalkan konsep terdesentralisasi, di mana data dan transaksi disimpan di banyak tempat atau node yang terhubung dalam jaringan. Setiap node memiliki salinan lengkap dari database, sehingga tidak ada satu pihak pun yang memiliki kontrol penuh atas data tersebut.
2. Terbuka
   Blockchain juga menggunakan konsep terbuka, di mana setiap orang dapat mengakses dan melihat data di dalam database. Informasi yang disimpan dalam blok-blok tersebut tidak dapat diubah atau dimanipulasi secara sembarangan, sehingga pengguna dapat memastikan integritas dan keaslian data.
3. Transparan
   Setiap transaksi yang dilakukan pada blockchain dicatat dan disimpan dalam blok terpisah. Setiap blok memiliki nomor urut yang saling terkait dan dienkripsi dengan kunci kriptografi. Informasi transaksi yang disimpan dalam blok terbuka untuk dilihat oleh publik, sehingga tidak ada transaksi yang dapat disembunyikan atau diubah.
4. Aman
   Keamanan pada blockchain didasarkan pada algoritma kriptografi yang kompleks dan jaringan terdesentralisasi. Informasi yang disimpan dalam blok-blok tersebut dienkripsi dengan kunci kriptografi dan hanya dapat diakses oleh pengguna yang memiliki kunci tersebut. Selain itu, setiap blok terhubung secara kriptografis dengan blok sebelumnya, sehingga tidak mungkin untuk mengubah atau memanipulasi blok yang telah disimpan di dalam blockchain.
5. Tanpa Otoritas Tunggal
   Blockchain tidak memiliki otoritas tunggal yang mengendalikan jaringan. Setiap node di dalam jaringan memiliki hak yang sama dan bekerja bersama-sama untuk memverifikasi dan memvalidasi transaksi. Dalam hal terjadinya perselisihan atau konflik, keputusan diambil berdasarkan konsensus mayoritas di antara pengguna jaringan.

2. Mekanisme Konsensus

Mekanisme konsensus adalah protokol yang ada untuk memastikan bahwa semua peserta dalam jaringan blockchain mematuhi aturan yang disepakati. Ini memastikan bahwa transaksi muncul dari sumber yang sah dengan meminta setiap peserta menyetujui keadaan buku besar yang didistribusikan. Blockchain publik adalah teknologi terdesentralisasi, dan tidak ada otoritas terpusat yang mengatur tindakan yang diperlukan. Oleh karena itu, jaringan memerlukan otorisasi dari peserta jaringan untuk verifikasi dan otentikasi aktivitas apapun yang terjadi di jaringan

blockchain. Seluruh proses dilakukan berdasarkan konsensus peserta jaringan, dan itu menjadikan blockchain sebagai teknologi yang tidak dapat dipercaya, aman, dan andal untuk transaksi digital. Mekanisme konsensus yang berbeda mengikuti prinsip yang berbeda, yang memungkinkan peserta jaringan untuk mematuhi aturan tersebut. Beberapa mekanisme konsensus telah diperkenalkan dengan mempertimbangkan persyaratan transaksi digital yang aman. Namun, bukti kerja (PoW), bukti kepemilikan (PoS), dan bukti kepemilikan yang didelegasikan (DPaS) adalah beberapa protokol konsensus yang digunakan oleh mata uang kripto utama.

D. 51% Attack

1. Pengertian

51% attack adalah jenis serangan pada jaringan blockchain, di mana seorang penyerang berhasil menguasai lebih dari 50% dari kekuatan komputasi pada jaringan blockchain. Dengan menguasai 51% atau lebih dari total kekuatan komputasi pada jaringan, penyerang dapat memanipulasi transaksi dan mencegah transaksi lainnya dari diproses. Misalnya, penyerang dapat menggandakan transaksi atau mengubah informasi dalam transaksi, termasuk membatalkan transaksi yang telah terjadi. Serangan 51% juga memungkinkan penyerang untuk menghentikan atau memperlambat proses penambangan pada jaringan, dan dapat menghasilkan double spending atau pengeluaran ganda.

Dalam sebuah jaringan blockchain, transaksi dikonfirmasi oleh jaringan node yang saling berinteraksi dan memvalidasi transaksi secara kolektif. Dengan memiliki lebih dari setengah kekuatan komputasi pada jaringan, seorang penyerang dapat menghentikan transaksi yang tidak diinginkan, menolak validasi transaksi, dan bahkan membuat transaksi palsu.

Sebagai contoh, jika seorang penyerang memiliki kontrol penuh atas jaringan Bitcoin, maka mereka dapat mengirim koin yang sama kedua orang berbeda (disebut double-spending), karena mereka memiliki kontrol atas validasi transaksi. Hal ini dapat menyebabkan kerugian finansial bagi pihak yang menerima koin palsu dan merusak kepercayaan pada jaringan secara keseluruhan.

Namun, untuk melakukan serangan 51%, penyerang harus menginvestasikan jumlah besar uang dan daya komputasi untuk membeli dan mengoperasikan perangkat keras dan perangkat lunak yang diperlukan. Karena itu, serangan semacam itu jarang terjadi pada jaringan blockchain besar dan mapan seperti Bitcoin.

2. Mekanisme 51% Attack

Serangan 51% adalah teknik yang terjadi ketika penyerang memiliki 51% kekuatan hashing. Serangan ini dimulai dengan membuat rantai blok secara pribadi, yang sepenuhnya terisolasi dari yang asli versi rantai. Pada tahap selanjutnya, rantai yang diisolasi disajikan ke jaringan untuk ditetapkan sebagai rantai asli. Inilah yang memungkinkan serangan pembelanjaan ganda. Karena kebijakan blockchain mematuhi aturan rantai terpanjang, jika penyerang bisa mendapatkan 51% kekuatan hashing atau lebih, mereka akan berada dalam posisi untuk menggerakkan rantai terpanjang dengan membujuk node jaringan untuk mengikuti rantai mereka. Namun,

tidak sepenuhnya diperlukan untuk mendapatkan 51% dari kekuatan hashing; jika penyerang mendapatkan kurang dari setengah kekuatan hashing, serangan pembelanjaan ganda masih mungkin dilakukan tetapi dengan kemungkinan keberhasilan yang lebih kecil. Semakin banyak kekuatan hashing yang terdiri dari seluruh jaringan blockchain, semakin mahal serangannya . Dengan demikian, cryptocurrency dengan hashing jaringan yang tinggi dianggap lebih aman terhadap serangan 51%.

3. Dampak 51% Attack

Serangan 51% pada blockchain memiliki dampak yang sangat serius pada keamanan dan stabilitas jaringan. Seorang penyerang yang berhasil melakukan serangan ini dapat mengendalikan jaringan dan memanipulasi transaksi dengan bebas. Beberapa dampak negatif dari serangan 51% pada blockchain antara lain sebagai berikut :

1. Double-spending: Penyerang dapat melakukan double-spending dan mengirim koin yang sama kedua orang berbeda. Ini dapat menyebabkan kerugian finansial bagi pihak yang menerima koin palsu dan merusak kepercayaan pada jaringan secara keseluruhan.
2. Memblokir transaksi: Penyerang dapat memblokir transaksi dengan mengontrol validasi transaksi pada jaringan. Ini dapat memperlambat atau bahkan menghentikan aktivitas bisnis yang tergantung pada jaringan blockchain.
3. Membuat transaksi palsu: Penyerang dapat memanipulasi data dan membuat transaksi palsu pada jaringan. Ini dapat mengganggu aktivitas bisnis dan merusak reputasi jaringan.

4. Mengapa 51% attack pada blockchain belum dapat diatasi ?

Meskipun para pengembang blockchain terus berusaha meningkatkan keamanan dan mencegah serangan 51% attack, namun sayangnya hingga saat ini, serangan ini masih belum dapat sepenuhnya diatasi. Beberapa alasan mengapa 51% attack pada blockchain belum dapat diatasi adalah sebagai berikut:

1. Kemampuan komputasi semakin meningkat: Semakin berkembangnya teknologi, maka semakin mudah juga bagi penyerang untuk membeli atau menyewa daya komputasi yang cukup besar untuk menyerang jaringan blockchain. Seiring dengan semakin meningkatnya kekuatan komputasi, maka semakin sulit pula untuk mencegah serangan 51% attack.
2. Pembaruan protokol yang sulit: Pembaruan protokol pada blockchain dapat memerlukan persetujuan mayoritas node dalam jaringan. Oleh karena itu, sulit untuk memperbarui protokol secara drastis untuk mencegah serangan 51% attack. Selain itu, pembaruan protokol juga dapat memerlukan perubahan dalam kode sumber, yang dapat menghasilkan kesalahan dan mengancam keamanan jaringan.
3. Biaya yang mahal: Mencegah serangan 51% attack memerlukan biaya yang cukup besar, seperti meningkatkan kekuatan komputasi jaringan,

meningkatkan jumlah node, atau mengubah mekanisme konsensus. Namun, biaya yang dibutuhkan dapat menjadi sangat mahal dan dapat menghalangi pengembang untuk mengambil tindakan yang dibutuhkan.

4. Motivasi keuntungan: Pada akhirnya, serangan 51% attack pada blockchain dapat dipicu oleh motivasi keuntungan, seperti mencuri cryptocurrency atau memanipulasi harga. Motivasi ini dapat mendorong para penyerang untuk terus mencari cara-cara baru untuk menyerang jaringan blockchain dan mencari celah keamanan yang belum teridentifikasi.

E. Mekanisme Konsensus dan 51% Attack

Salah satu cara untuk menghindari serangan 51% attack pada blockchain adalah dengan menggunakan mekanisme konsensus yang andal dan efektif. Mekanisme konsensus digunakan untuk memastikan bahwa semua node dalam jaringan blockchain setuju pada keadaan yang sama dan transaksi yang dilakukan sah.

Beberapa mekanisme konsensus yang dapat digunakan untuk menghindari serangan 51% attack antara lain:

1. Proof of Work (PoW): PoW adalah mekanisme konsensus yang saat ini digunakan oleh Bitcoin. Mekanisme ini memerlukan node dalam jaringan untuk menyelesaikan tugas matematika yang rumit untuk memvalidasi transaksi. Tugas ini membutuhkan daya komputasi yang besar dan memakan waktu, sehingga serangan 51% attack akan memerlukan daya komputasi yang sangat besar dan mahal untuk dilakukan.
2. Proof of Stake (PoS): PoS adalah mekanisme konsensus alternatif yang digunakan oleh cryptocurrency seperti Ethereum. PoS tidak memerlukan daya komputasi yang besar seperti PoU, tetapi node dalam jaringan harus menyetor sejumlah cryptocurrency sebagai jaminan untuk memvalidasi transaksi. Jika node melanggar aturan, maka cryptocurrency yang dijamin dapat diambil oleh jaringan. Dengan PoS, serangan 51% attack akan lebih sulit dilakukan karena penyerang harus memiliki sejumlah besar cryptocurrency untuk dijamin.
3. Delegated Proof of Stake (DPaS): DPaS adalah varian dari PoS yang digunakan oleh cryptocurrency seperti EOS. DPoS memungkinkan pemilik cryptocurrency memilih sejumlah node validator yang akan memvalidasi transaksi. Node-node validator ini dipilih oleh pemilik cryptocurrency dengan memberikan suara. DPoS memiliki keamanan yang lebih baik karena penyerang harus mengambil alih sejumlah besar node validator untuk melakukan serangan 51% attack.
4. Proof of Authority (PoA): PoA adalah mekanisme konsensus yang digunakan oleh beberapa blockchain swasta. PoA memerlukan sejumlah node validator yang dipercayai untuk memvalidasi transaksi. Node validator dipilih oleh pemilik blockchain berdasarkan kepercayaan dan reputasi mereka. Serangan 51% attack pada PoA akan sangat sulit dilakukan karena penyerang harus memiliki akses ke sejumlah besar node validator yang dipercayai.

Dalam pengembangan blockchain, memilih mekanisme konsensus yang tepat dapat membantu menghindari serangan 51% attack. Namun, tidak ada mekanisme konsensus yang sempurna dan setiap mekanisme konsensus memiliki kelebihan dan kelemahan sendiri. Oleh karena itu, para pengembang blockchain terus mencari cara-cara baru untuk meningkatkan keamanan jaringan dan mencegah serangan 51% attack.

REFERENSI

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc.

Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Zohar, A. (2016). On scaling decentralized blockchains. Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research, 1-14.

Kiayias, A., Miller, A., & Zindros, D. (2017). Non-Interactive Proofs of Proof-of-Work.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain research: a review. International Journal of Financial Studies, 4(3), 23.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 13(3), 352-375.