Blockchain Proof-of-Work Threat: 51% Attack

Luthfi Eko Trinowo

Makalah Keamanan Informasi

***Abstract*— Teknologi Blockchain memiliki sistem tersendiri dalam melakukan konsensus yang dibutuhkan, metode ini dinamai dengan metode Proof-of-Work. Metode ini memiliki suatu kelemahan tersendiri yang dikenal dengan nama 51% Attack. 51% Attack adalah suatu fenomena di mana terdapat suatu miner group yang memiliki atau mengontrol lebih dari 50% network hashing power yang ada, sehingga kelompok ini dapat mencegah atau menunda konfirmasi dari suatu transaksi yang ada. Lebih jauh lagi, metode ini dapat mengembalikan transaksi yang sudah selesai sehingga akan terdapat kondisi double-spend dalam suatu transaksi.**

Metode penyerangan ini memiliki kemungkinan terjadi yang cukup kecil pada penerapan teknologi blockchain yang telah berkembang cukup besar seperti Bitcoin. Namun sayangnya, pada cryptocurrency lain yang lebih sering dikenal dengan nama altcoin, kemungkinan penyerangan dengan metode ini masih cukup tinggi dikarenakan biaya yang harus dikeluarkan untuk memiliki lebih dari 50% network hashing power tidak akan sebesar biaya yang diperlukan untuk mengakuisisi milik Bitcoin yang telah memiliki jaringan cukup luas di seluruh dunia.

Keywords: 51% Attack, Blockchain, Mining, Double-Spending Attack

I. *INTRODUCTION*

Bitcoin berkembang dan menjadi lebih populer di Indonesia pada sekitar tahun 2017 dengan adanya *Ransomware Virus* yang mengharuskan terdampak membayar kepada organisasi yang menyebarkan virus ini agar virus tersebut dapat dihilangkan dari perangkat terdampak. Kejadian ini menjadi titik awal yang menyebabkan sistem keuangan desentralisasi seperti bitcoin ini menjadi topik obrolan dan studi yang mulai hangat dibicarakan khususnya di Indonesia. *Bitcoin* sendiri dapat diperoleh dengan teknik yang dinamakan *mining*, bukan *mining* seperti pada umumnya, simpelnya kegiatan *mining* ini dilakukan dengan cara melakukan verifikasi pada sebuah transaksi dan memberikan kunci khusus yang menjadi bagian besar dari *chain of block.* Namun, *bitcoin* sendiri bukanlah suatu teknologi namun

merupakan suatu mata uang digital atau yang lebih sering disebut dengan *cryptocurrency* yang memanfaatkan teknologi *blockchain* dalam keberlangsungannya.

Blockchain adalah teknologi paling dasar atas penggunaan dan perkembangan bitcoin. Secara jelas, *blockchain* akan jauh lebih mudah untuk dimanfaatkan untuk menjadi suatu hal lainnya. Sifatnya yang terdesentralisasi dan terbuka terhadap penggunanya, menjadikan *blockchain* menjadi salah satu teknologi yang digadang-gadang dapat digunakan untuk berbagai macam kepentingan, hal ini membuat penggunaan dan pengembangan *blockchain* menjadi suatu topik yang sedang naik daun. Tentunya, ketika suatu teknologi diimplementasikan, salah satu aspek yang harus diperhatikan adalah aspek keamanan. *Blockchain* sendiri bukan berarti tanpa celah keamanan, faktanya terdapat beberapa jenis *attack* yang dapat ditujukan secara langsung ke dalam fungsionalitas *blockchain* seperti *51%-Attack*, *Eclipse Attack* dan *Physical Attack*.

Pada makalah kali ini, saya akan membahas mengenai apa itu *51%-Attack* dan bagaimana cara yang mereka lakukan untuk dapat memanipulasi hasil yang terdapat pada sistem *blockchain* walaupun sistem ini bersifat terbuka dan terdesentralisasi. Pembahasan kali ini tidak akan terlalu dalam mengenai solusi yang diberikan untuk mengatasi serangan tersebut, namun penulis akan memberikan sedikit gambaran cara pencegahan yang dapat dilakukan untuk menghindari adanya serangan yang membuat *trust issue* tersebut.

II. *PRELIMINARY AND BASIC CONCEPT*

Pada bagian ini, saya akan membahas mengenai dasar-dasar apa saja yang harus dimengerti sebelum kita menelaah lebih jauh lagi mengenai *blockchain*, termasuk istilah-istilah apa saya yang ada dan maksud dari istilah tersebut. Dengan demikian, diharapkan pembaca memiliki pemahaman yang sama sehingga dapat memahami hal-hal yang akan dibahas pada makalah ini secara sempurna.

A. *Blockchain and Mining*

Blockchain merupakan representasi aplikasi dari *cryptography* yang menjawab sebuah masalah besar mengenai penyimpanan suatu data transaksi yang cenderung tersentralisasi dan juga memiliki beban yang cukup berat pada entitas yang memberikan validasi. Seperti namanya, *blockchain* merupakan suatu kumpulan *blok* yang terhubung satu sama lainnya. Penghubung antar blok ini sering disebut

dengan *chain.* Satu hal yang paling menarik dari *blockchain* adalah *mining* dan *fee* yang diberikan kepada entitas yang melakukan tindakan *mining* tersebut.

Mining sendiri adalah sebuah istilah yang menyatakan sebuah tindakan verifikasi transaksi yang menggunakan teknologi *blockchain.* Dengan algoritma khusus, entitas dapat memvalidasi suatu transaksi dan memberikan kunci yang menutup blok tersebut. Apabila serangkaian kegiatan tersebut telah dilakukan, maka entitas yang melakukan validasi tersebut akan diberikan sebuah *fee* (selanjutnya disebut sebagai *consensus tip)* berupa mata uang *online* yaitu bitcoin.

Konsep *blockchain* dan *mining* ini menjadi menarik bagi banyak kalangan karena sifatnya yang susah untuk dimanipulasi. Contohnya, apabila sebuah transaksi telah selesai dilaksanakan dan terdapat sebuah entitas yang ingin mengganti nilai dari suatu transaksi tersebut, maka tindakan tersebut secara otomatis akan membuka kunci blok dan akan disadari oleh entitas lain yang terdapat dalam jaringan *blockchain* tersebut.

B. *Consensus Rules*

Hal inilah yang membuat *blockchain* menjadi suatu teknologi yang dipercaya dapat digunakan untuk mengamankan data dan mengurangi risiko adanya perubahan data. Fenomena ini dikarenakan ketika suatu entitas dapat memberikan suatu validasi atas sebuah transaksi dan menyegel blok tersebut dengan suatu kode, maka seluruh partisipan yang terdapat dalam jaringan tersebut harus menyetujui hal itu. Sehingga, ketika terjadi sebuah kecurangan atau perubahan data maka akan ada banyak entitas yang harus menyetujui dan hal ini membuat kecurangan sangat mudah sekali terlihat.

Algoritma yang digunakan dalam konsensus ini merupakan algoritma bernama *Proof of Work* yang akan dijelaskan lebih lanjut pada bab berikutnya. Secara sederhana, apabila ada sebuah entitas yang telah menyelesaikan pekerjaannya, maka dia akan dianggap sebagai seorang *miner*, kebalikannya, apabila seorang *attacker* benar-benar menyelesaikan pekerjaan tersebut, maka *attacker* tersebut sesungguhnya telah menghabiskan banyak waktu dan uang untuk menyerang sistem ini. Hal ini dikarenakan *Proof of Work* membutuhkan perangkat keras yang cukup mahal untuk dapat secara efektif melakukan penambangan.

C. *Proof of Work Algorithm*

Seperti yang telah disebutkan pada sub-bab sebelumnya, *proof of work* merupakan suatu algoritma khusus yang digunakan oleh *blockchain* agar dapat

memberikan kepercayaan kepada seluruh entitas yang berada pada jaringan tersebut. Dilakukan dengan cara menemukan sebuah *cryptographic hash* yang akan dijadikan segel dari blok tersebut. *Hash* ini nantinya harus memenuhi kriteria dan juga merupakan suatu nilai yang valid untuk dapat digunakan pada blok selanjutnya. Dalam pemrosesannya, algoritma ini membutuhkan suplai daya yang besar pada suatu proses komputasi sehingga ketika *attacker* berusaha menyerang sistem ini akan terasa sia-sia.

D. *Proof of Stake Algorithm*

Proof of Stake (PoS) adalah mekanisme atau algoritma konsensus yang mengotorisasikan blok-blok berdasarkan jumlah uang yang dikeluarkan oleh penambang. Penambang yang memiliki jumlah koin lebih besar maka dia akan lebih kuat jika dibandingkan dengan peserta yang lainnya. Algoritma ini memiliki keuntungan dan kerugian sendiri jika dibandingkan dengan algoritma *proof of work.*

Namun penggunaan algoritma ini bisa dikatakan cukup minim pada realisasinya. PoS cukup rentan karena sistem yang digunakan adalah terpusat (berbeda dengan sistem terdesentralisasi) dan juga memungkinkan entitas dengan jumlah kekayaan atau jumlah koin yang lebih banyak untuk dapat mengeruk keuntungan lebih mudah dibandingkan dengan entitass yang lainnya.

E. *Transaction and Transaction Fee*

Transaksi yang terdapat pada *blockchain* merupakan *input* dan *output*. *Chain* yang dibentuk dari sistem *blockchain* dimulai dari sini. *Output* dari blok sebelumnya akan digunakan sebagai *input* dari blok yang digunakan sekarang, dan *output* dari blok yang digunakan sekarang akan menjadi *input* bagi blok berikutnya. Hal ini berlangsung secara terus menerus yang membuat blok-blok ini saling memiliki keterkaitan antara satu dengan yang lainnya. Dengan kata lain, mengubah isi atau kunci dari suatu blok harus mengubah kunci pada blok lain secara keseluruhan.

Bagi siapa saja, yang dapat memverifikasi suatu transaksi dan menghasilkan suatu *cryptograpic hash* yang tepat untuk blok tersebut, maka entitas tersebut akan mendapatkan imbalan atau *fee* atas jasa yang diberikan. Hal ini menjadi cukup penting karena biaya yang dikeluarkan oleh para *miner* untuk melakukan verifikasi transaksi tidaklah sedikit. Hal ini membuat banyak entitas berlomba-lomba menyediakan perangkat keras terbaik yang dapat digunakan untuk melakukan

verifikasi transaksi demi imbalan yang dikembalikan berupa *cryptocurrency* (secara umum yang masih digunakan adalah *bitcoin* sebagai imbalan mengingat nilai jualnya yang cenderung stabil jika dibandingkan dengan *altcoin* lainnya).

F. *Sybil Attack*

Penyerangan dengan metode ini dilakukan dengan cara membuat *node* palsu yang ditaruh ke dalam jaringan asli dengan memberlakukan adanya identitas palsu untuk dapat membuat *node* tersebut. Namun sayangnya, penyerangan dengan metode ini tidak dapat berlaku dalam keseluruhan blok karena terdapat beberapa blok yang membutuhkan biaya yang cukup tinggi untuk diserang.

G. *BGP Hijack*

Serangan dengan metode ini memanfaatkan perbedaan pandangan antara sistem yang dimiliki oleh *blockchain* dengan pandangan yang dimiliki oleh *router*. Walaupun jaringan *blockchain* acapkali disebut sebagai jaringan yang terdesentralisasi, namun dari sudut pandang *internet router* jaringan *blockchain* merupakan jaringan sentral karena terdapat sekitar 100 *IP Prefixes* yang mengelola 20% *bitcoin host*.

Dengan mengetahui hal tersebut, salah satu skenario penyerangan dengan metode ini adalah dengan cara membajak *IP prefixes* yang memiliki kemungkinan untuk dapat mencegah atau membatalkan transaksi yang terjadi pada jaringan.

H. *DDoS Attack*

Penyerangan dengan metode ini kurang lebih mirip dengan penyerangan *DDoS* pada umumnya yaitu penyerang membanjiri *traffic* secara *extreme,* Penyerangan jenis ini adalah salah satu yang paling sering dilakukan ke dalam teknologi blockchain dengan tujuan untuk menghalangi transaksi sehingga transaksi tersebut tidak dapat dieksekusi.

Namun karena sifat terdistribusi yang dimiliki oleh *blockchain*, maka serangan dengan metode ini tidak akan berdampak pada keseluruhan aktivitas jaringan namun hanya pada beberapa tingkat tertentu saja.

I. *Blockchain Attacks*

Terdapat beberapa jenis *attacks* yang terkenal dalam dunia *blockchain* antara lain *Eclipse Attacks, Selfish Miner Attack* dan yang akan kita bahas pada makalah ini yaitu 51%-*Attack.* Pada sistem *blockchain*, para entitas yang melakukan validasi (untuk seterusnya akan disebut penambang), hanya akan menyebarkan blok baru kepada seluruh penambang yang terdapat pada jaringan dan hal ini cukup

berbahaya karena akan dapat dimonopoli oleh *attackers* (selanjutnya akan disebut dengan penyerang). Adalah sebuah hal yang berbahaya ketika seorang penyerang memonopoli koneksi masuk dan keluar blok, maka akan terjadi isolasi pada penambang yang terdapat dalam suatu jaringan tersebut. Terlebih, apabila blok ini memiliki kunci yang strategis terhadap banyak blok lainnya, penambang akan membutuhkan lebih banyak daya komputasi yang pada akhirnya akan digunakan untuk membantu kebutuhan si penyerang ini. Penyerangan seperti ini disebut dengan *Eclipse Attack.*

Berbeda dengan *Eclipse Attack, Selfish Miner Attack* merupakan sebuah cara di mana penyerang dalam suatu kondisi tertentu mendapatkan *reward* yang tidak proporsional. Dalam konteks hal ini, penyerang dapat menjaga suatu blok agar bersifat *private* hingga blok ini tumbuh cukup besar, lalu ketika ada suatu cabang dari blok mendekat, para penyerang akan menyebarkan blok-blok yang telah disimpan secara *private* tadi sehingga dalam kondisi ini penyerang dan penambang akan sama-sama menghabiskan banyak *resources*. Namun dalam kondisi ini, penyerang tentu mendapatkan keunggulan persaingan jika dibandingkan dengan penambang.

III. PROBLEM DEFINITION

Seperti yang telah dijelaskan sebelumnya, *blockchain* memiliki beberapa sifat seperti *open* (terbuka) dan *decentralized* (terdesentralisasi), sehingga memungkinkan semua orang dapat menjadi bagian dari penambang yang terdapat pada jaringan tersebut. Dengan adanya sifat *blockchain* ini, tentu sisi keamanan tidak bisa dilupakan, atau bahkan akan selalu menjadi perhatian bagi para pengembang yang ingin memanfaatkan teknologi *blockchain* ini agar dapat menangkal serangan-serangan seperti yang telah dijelaskan sebelumnya.

Namun, perlindungan terhadap serangan ini tentu akan memiliki beberapa faktor di dalamnya seperti jenis serangan, jenis atau kondisi jaringan, dan beberapa hal lainnya. Namun, pada makalah kali ini, saya akan berfokus untuk mengupas lebih dalam mengenai serangan dengan jenis *51%-Attack* serta protokol dari *blockchain* sendiri.

A. 51% Attack

Metode ini adalah metode penyerangan dengan kondisi penyerang menguasai lebih dari 50% *hashing power* yang terdapat dalam jaringan tersebut. Dimulai dengan membuat suatu *private* blok yang pada nantinya blok ini akan dibuka kepada seluruh penambang pada jaringan yang sama sehingga memaksa adanya *double-spending*.

Dengan memiliki lebih dari 51% *hashing power*, penyerang dapat memaksa para penambang untuk mengikuti alur *chain* yang telah ia buat dan penyerang memiliki kemungkinan untuk sukses yang lebih tinggi jika dibandingkan dengan yang lainnya. Masalah utamanya adalah, penyerang dengan *hash power* kurang dari 50% tetap dapat melaksanakan rencana ini, hanya saja memiliki tingkat kesuksesan yang lebih rendah sehingga kemungkinan *loss* yang dimiliki juga akan semakin lebih tinggi.

Penyerangan dengan memanfaatkan metode seperti ini sebenarnya tidak akan mampu bertahan ketika *hashing power* yang dimiliki oleh keseluruhan jaringan terdapat dalam jumlah yang banyak, karena ketika kondisi ini terjadi, maka *cost* atau biaya yang dibutuhkan akan menjadi lebih besar lagi.

B. Proof of Work Weaknesses

Proof of Work (PoW) merupakan algoritma yang digunakan dalam hal mekanisme konsensus yang diinisiasi oleh *bitcoin*. Setelah itu, algoritma ini baru digunakan secara masif oleh banyak *cryptocurrencies.* Penambang adalah pilar atau pendukung utama dari algoritma ini yang berperan dalam memverifikasi dan merekam sebuah transaksi.

Konsensus jenis ini menggunakan sebuah asumsi bahwa setengah dari penambang yang ada pada jaringan merupakan *honest miners*, maka dari itu, memiliki lebih dari setengah *hashing power* dapat membuat mekanisme ini menjadi lebih rentan akan tindakan serangan yang dapat berujung pada *trust issue*.

Penambangan pada metode ini dapat dibilang berlangsung cukup lambat jika dibandingkan dengan metode lainnya seperti *Proof of Stake* maupun *Delegated Proof of Stake* beberapa *pool* yang tersedia didominasi oleh kekuatan penambangan yang cukup besar, sehingga penyerangan terhadap *pool* tersebut dapat menyebab disrupsi yang cukup besar pada nilai dan keberadaan dari *bitcoin* itu sendiri.

Metode konsensus seperti ini akan lebih berbahaya terhadap *51% Attacks* apabila memiliki tipe *low hashing cryptocoins*. Lebih lanjut, metode ini juga cukup

rentan terhadap adanya serangan lain seperti *Sybil Attack, DDoS Attack* dan juga *BGP Hijacking*.

C. Majority Hash Problem

Pada bagian ini, saya akan lebih banyak membahas permasalahan yang terdapat pada mekanisme *majority hash* serta bagaimana hal tersebut akan membawa ke dalam suatu masalah lain seperti *Double-Spending Issue*.

a. The Majority Hash Attacks

Penyerangan dengan metode seperti ini dapat dilakukan dengan beberapa cara yang ada antara lain adalah dengan *51%-Attack* dan juga *Selfish Mining.* Hal seperti ini dapat menjadi suatu masalah yang serius karena dapat membawa sebagian besar penambang pada ya jaringan yang sama akan mengikuti *chain* yang telah dibuat atau dimiliki oleh pemilih *hash* tertinggi, hal ini berujung pada aktivitas berbahaya yang dapat melibatkan penambang demi keuntungan penyerang.

b. Double-Spending Issue

Permasalahan ini dimulai dari adanya kesuksesan eksploitasi yang dijalankan oleh penyerang, hal seperti ini akan berujung pada penyerang yang dapat melakukan pembatalan transaksi dan menggunakan koin yang sama lagi. Penyerang pertama harus menggunakan koin mereka dalam suatu *chain* yang terbukti (bukan bagian dari serangan), lalu pada waktu yang bersamaan membuat *private chain* yang pada nantinya akan ditunjukkan kepada penambang pada jaringan tersebut.

Karena *chain* yang dimiliki lebih panjang dari *chain* yang digunakan sekarang, maka *chain* tersebut akhirnya dianggap sebagai *chain* yang asli dan digunakan oleh seluruh penambang pada jaringan tersebut

IV. PROBLEM MITIGATION

Pada bab ini saya akan membahas beberapa teknik atau metode yang dapat digunakan sebagai tindakan atau upaya preventif dalam menghadapi penyerangan terhadap *blockchain* terutama penyerangan dengan menggunakan metode *51% Attack.* Beberapa metode ini ditemukan setelah adanya eksploitasi yang terjadi terhadap beberapa *cryptocurrency* yang menggunakan teknologi *blockchain* di dalamnya.

A. Delayed Proof of Work by Komodo

Metode ini merupakan solusi keamanan yang dikembangkan oleh Komodo. Komodo sendiri merupakan sebuah perusahaan yang bergerak pada bidang *multi-chain platform* dengan memanfaatkan teknologi *blockchain* di dalamnya. Komodo juga menyediakan layanan *end-to-end blockchain development* yang dapat digunakan untuk pengembangan bisnis.

Metode keamanan ini dikembangkan oleh Komodo dengan tujuan melindungi atau mengantisipasi adanya tindakan *double-spending* dan berlaku pada metode blok UTXO. Salah satu hal yang penting di sini adalah, Komodo tidak mengenali aturan rantai terpanjang, sehingga hal ini dapat menghindari kegiatan duplikasi *chain* yang digunakan secara *private* lalu disebar ke seluruh jaringan untuk menggantikan *chain* yang asli. Ide utama yang digunakan adalah, Komodo mendaur ulang *hashrates* yang dimiliki oleh jaringan bitcoin untuk melindungi integritas data yang ada pada *blockchain*. Hal ini memungkinkan adanya cadangan data pada suatu blok individu yang disebar ke *blockchain* lain termasuk *bitcoin* itu sendiri.

B. Penalty System for Delayed Block Submission by Horizen

Metode ini merupakan solusi keamanan yang dikembangkan oleh Horizen. Horizen sendiri adalah sebuah perusahaan yang menyediakan platform pengembangan bisnis secara masif yang mengadopsi dan memanfaatkan teknologi *blockchain* di dalamnya baik yang bersifat publik maupun *private*.

Ide utama dari metode ini adalah membuat biaya yang dibutuhkan oleh penyerang bertambah secara masif sehingga harapan untuk mendapat keuntungan menjadi sia-sia. Penalti yang diberikan dilakukan berdasar parameter berupa waktu yang digunakan untuk menyembunyikan blok dari jaringan *blokchain* itu sendiri. Dengan kata lain, metode ini berfokus pada penanganan penambangan blok pribadi yang disembunyikan dari jaringan utama *blockchain*.

V. KESIMPULAN

Blockchain adalah sebuah teknologi yang dapat menyelesaikan beberapa masalah integritas data yang dimiliki oleh beberapa teknologi lainnya. Dengan menerapkan sistem terbuka dan terdesentralisasi, data yang tersimpan di dalam teknologi ini dapat diawasi oleh seluruh anggota yang terdapat pada jaringan sehingga integritasnya bisa jauh lebih terjaga.

Namun, penggunaan *Satoshi Consensus* rentan terhadap serangan yang diberlakukan dengan metode *50% Attack* karena penggunaan *Satoshi Consensus* menerapkan sebuah asumsi bahwa sebagian besar anggota yang terdapat pada jaringan merupakan *honest miner,* sehingga asumsi ini tidak dapat menanggulangi adanya kemungkinan sebagian besar anggota bukan *honest miner*.

Penggunaan metode sebagai tindakan preventif belum cukup untuk menanggulangi adanya serangan dengan berbagai metode yang ada dikarenakan tiap metode pencegahan ini memiliki fokus yang tersendiri sehingga dibutuhkan studi lebih lanjut untuk menentukan metode baru dengan tujuan mengatasi kelemahan yang dimiliki oleh *Satoshi Consensus* ini.

REFERENSI

[1] C. Ye, G. Li, H. Cai, Y. Gu and A. Fukuda, "Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting," 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, 2018, pp. 15-24.

[2] K. D. Gupta, A. Rahman, S. Poudyal, M. N. Huda and M. A. P. Mahmud, "A Hybrid POW-POS Implementation Against 51 percent Attack in Cryptocurrency System," 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Sydney, Australia, 2019, pp. 396-403.

[3] Sayeed, Sarwar & Marco-Gisbert, Hector. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Applied Sciences. 9. 1788. 10.3390/app9091788.

[4] C. Ye, G. Li, H. Cai, Y. Gu and A. Fukuda, "Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting," 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, 2018, pp. 15-24.

[5] X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 261-265.