Analysis on Blockchain Algorithm Used in Bitcoin System = Analisis Algoritma Rantai Blok Yang Digunakan Dalam Sistem Bitcoin

Neil Endrigo Cardoso De Miranda, author

Abstrak

Proposal tesis ini bertujuan untuk mempelajari referensi yang digunakan oleh Satoshi Nakamoto untuk memahami prinsip-prinsip yang digunakan untuk memecahkan masalah pengeluaran ganda. Masalah pengeluaran ganda merupakan risiko mata uang digital dapat dikeluarkan dua kali. Hal tersebut merupakan masalah unik yang berpotensi pada mata uang digital karena informasi digital dapat digandakan dengan relatif mudah oleh individu yang memahami jaringan blockchain dan memiliki kekuatan komputer yang diperlukan untuk memanipulasinya.
Untuk memahami motifnya, semua kutipan yang disebutkan dalam karya tulis Satoshi Nakamoto dianalisis secara mendalam, sehingga kami sampai pada kesimpulan bahwa server stempel waktu yang juga dapat digunakan untuk mengesahkan keaslian serta tanggal penerbitan dokumen digunakan untuk menyelesaikan masalah pengeluaran ganda.
Stempel waktu adalah alat yang sangat penting, Kami menganalisis masalah pengeluaran ganda, serta mengapa setiap transaksi memiliki stempel waktu yang unik dan hadiah yang diterima oleh blok hanya dapat diterima setelah 120 blok ditambang.
Mengapa transaksi membutuhkan 120 blok agar token dapat diterima, mengapa prinsip stempel waktu yang digunakan dalam dokumen digital diterapkan dalam mata uang kripto untuk stempel waktu untuk menghasilkan blok dan mengapa dokumen digital juga dapat menjadi transaksi moneter.
Penolakan atas balasan penolakan layanan merupakan bukti kerja yang disarankan oleh Adam Back dalam bentuk tunai hash, karena merupakan inspirasi untuk
membuat protokol yang juga mempelajari secara mendalam untuk menghindari kekurangan dalam kode dan menolak serangan node.
Protokol pohon Merkle dianalisa untuk memahami cara kerja protocol sistem distribusi kunci publik.
Teori probabilitas dan aplikasinya dianalisis untuk menghitung kemungkinan penyerang membuat rantai lebih cepat daripada node yang sebenarnya, sebagaimana dipahami sebagai satu-satunya cara agar rantai blok dapat berhasil adalah dengan memastikan bahwa node yang sebenarnya ebih kuat daripada node yang dibuat oleh penyerang.
Kami juga akan merancang dan membuat rantai blok sederhana untuk memahami prinsip-prinsip utama yang disebutkan di atas yang dikarakterisasi oleh protokol rantai blok menggunakan bukti kerja; mengimplementasikan aplikasi rantai blok sederhana dalam Javscript menggunakan crypto-js dan mendiskusikan alasan di balik kegagalan kami dalam hasil dan kesimpulan kami dalam upaya membuat aplikasi pesan instan menggunakan rantai blok sederhana kami.
.....The thesis proposal is to study the references used by Satoshi Nakamoto to understand the principles he used to solve the double-spending problem. The doublespending problem is the risk that a digital currency can be spent twice. It is a potential problem unique to digital currencies because the digital information can be reproduced relatively easily by individuals that understand the blockchain network and have the

computer power necessary to manipulate it.
To understand his motives all citations mentioned in Satoshi Nakamoto whitepaper were deeply analyzed, where we came to the conclusion that a time stamping server that could also be used to certify the authenticity as well the date of issuing of a document was used to solve the double spending problem. Timestamps was a very important tool, the double spending problem is analyzed in our thesis as well why every transaction has a unique timestamp and the rewards received by blocks can be spent only after 120 blocks mined. Why a transaction requires
120 blocks for the token to be received, why timestamping principles used in a digital document were applied in cryptocurrencies to timestamp generated blocks and why a digital document can also be a monetary transaction.
A denial of service counter-measure, a proof-of-work suggested by Adam Back in Hash cash, as it was an inspiration to create the protocol was also deep studied to avoid flaws in the code and deny the attack of a node.
Merkle tree protocol analyzed to understand how the protocols for public key distribution systems works.
Probability theory and its applications is analyzed to calculate the probability of an attacker creating a chain faster than the honest node, as understood the only way for the Block chain to succeed was to make sure that the honest nodes were more powerful than dishonest nodes, attackers.
We will also design and create a simple blockchain to understand the main principles mentioned above that characterizes a blockchain protocol using proof-of-work; implement a simple blockchain application in Javscript using crypto-js and discuss the reasoning behind our failure in our results and conclusion on attempting to create an
instant messaging application using our simple blockchain.