Proceedings

Konferensi Nasional Sistem Informasi 2014

KNSI 2014

Konferensi Nasional Sistem Informasi 2014

STMIK DIPANEGARA MAKASSAR

27 Pebruari - 01 Maret 2014

Abstract Proceeding Edition

ISSN : 2355-1941

Pusat Penelitian dan Pengabdian Pada Masyarakat (P4M) STMIK Dipanegara Makassar
Jl. Perintis Kemerdekaan Km.9 Makassar, Telp. : 0411-587194 | Fax. : 0411-588283
Email : p4m@dipanegara.ac.id

SESI III, KELOMPOK 7, RUANG 202			
No.	No.KNSI	JUDUL MAKALAH	PENULIS
1	KNSI-272	Kombinasi Algoritma Genetik Dan K-Prototype Untuk Menentukan Jumlah Cluster Optimal Pada Data	I Made Ari Santosa, I Wayan Budi Sentana
2	KNSI-345	Perancangan Aplikasi Sistem Informasi Pelyanan Responsi di Laboratorium Teknik Informatika UNPAS	Muhammad Agung Rizkyana
3	KNSI-347	Analisis Mining System Pada Bitcoin	Ferry Mulyanto
4	KNSI-351	Model Implementasi Centralized Authentication Service Pada Sistem Software As A Service	Muhammad Arfan
5	KNSI-352	Aplikasi Pelacakan Ponsel Berbasis Windows Mobile Phone	Agustinus Noertjahyana
6	KNSI-370	Kajian Teori Flow Sebagai Sumber Motivasi Intrinsik Belajar Melalui Serious Game	Ririn Dwi Agustin

SESI III, KELOMPOK 8, RUANG 203			
No.	No.KNSI	JUDUL MAKALAH	PENULIS
1	KNSI-371	Model Pelatihan Tik	Nadya Safitri
2	KNSI-372	Analisis Penerimaan Sistem Informasi Kepegawaian Pengaruhnya Terhadap Kinerja Pengguna (Studi Kasus	Syachriani Syam
3	KNSI-373	Model Evaluasi Untuk Menilai Kualitas Requirement Sistem Informasi	Iwan Kurniawan, Sali Alas M
4	KNSI-374	Perancangan Sistem Informasi Dengan Menggunakan Pendekatan Knowledge Sharing Untuk Komunitas	Agung Aldhiyat, Shanti Herliani
5	KNSI-375	Mengukur Keberhasilan Penerapan Sistem Informasi Manajemen Menggunakan Model Operations	Dwi Vernanda, Sali Alas M
6	KNSI-396	Analisis Investasi Sistem Informasi Dengan Menggunakan Domain Teknologi - Metode Information	Leo Willyanto Santoso, Yulia

SESI III, KELOMPOK 9, RUANG 204			
No.	No.KNSI	JUDUL MAKALAH	PENULIS
1	KNSI-381	Studi dan Implementasi Algoritma Terinspirasi Sistem Imun: Clonal Selection Algorithm	Ayi Purbasari, Oerip Santoso
2	KNSI-384	Kontribusi Sistem Informasi terhadap Sistem Kerja Event Organizer	Asep Somantri
3	KNSI-387	Data Mining Kredit Usaha Mikro Di Bank Xxxx	Agus Hexagraha
4	KNSI-402	Emv Dan Pola Aliran Cairan Pada	Kartini
5	KNSI-406	Menyembunyikan Pesan Yang Tersembunyi: Bentuk Pengamanan Informasi	Frizka Ferina,
6	KNSI-410	Aplikasi Sistem Pakar Berbasis Mobile Untuk Mengenali Masalah Kesehatan Kewanitaan	Windarto, Hadi Setiawan

SESI III, KELOMPOK 10, RUANG 205			
No.	No.KNSI	JUDUL MAKALAH	PENULIS
1	KNSI-56	Analisis User Interface Media Pembelajaran Pengenalan Kosakata Untuk Anak Tunarungu	Adam Mukharil Bachtiar
2	KNSI-148	Pengenalan Konsep Sistem Informasi Pewarigaan (Sip) Sebagai Alat Bantu Dosen Dalam Menentukan	Ni Ketut Sriwinarti
3	KNSI-171	Perancangan Aplikasi Portal Sekolah Minggu Studi Kasus Gereja Masehi Injili di Minahasa	Stanley Karouw
4	KNSI-173	Adopsi Teknologi Internet Pada Usaha Mikro Kecil dan Menengah	Kartika Gianina Tileng, Rinabi Tanamal
5	KNSI-180	Sistem Registrasi Penyakit Dalam Mendukung Pelayanan Hiv/Aids Di Rumah Sakit	Guardian Yoki Sanjaya, Marthalena Erbin Nahak
6	KNSI-198	Analisis pada Layanan Learning Management System (Studi Kasus: Virtual Learning Politeknik Pos Indonesia)	Maniah

SESI III, KELOMPOK 11, RUANG 208			
No.	No.KNSI	JUDUL MAKALAH	PENULIS
1	KNSI-185	Implementasi Alternatif Layanan Komunikasi E-Kampus Berbasis Simplex Communication Method	S N M P Simamora
2	KNSI-229	Pengembangan Sistem Informasi Manajemen Pendonor Darah	Annisa Ristya Rahmanti, Lutfan Lazuardi
3	KNSI-357	Rancangan Sistem Pembangkit Anotasi Otomatis Untuk Kredibilitas Dan Reliabilitas Informasi Dalam	Yudi Wibisono
4	KNSI-4	Perancangan Aplikasi Real-Time Log Monitoring Via E-mail dan SMS pada Server Berbasis Linux	Madyana Patasik, novita Sambo
5	KNSI-37	Metode Most Prominent Ridge Line Pada Pengukuran Rangka Atlet Jalan Cepat	
6	KNSI-2	Klasifikasi Karakter Manusia Menggunakan Algoritma Nave Bayes untuk Rekomendasi Motif Karawo berbasis Budaya	Arip Mulyanto

ANALISIS *MINING SYSTEM* PADA BITCOIN

Ferry Mulyanto[1], M Tirta Mulia[2]

[1,2] Teknik Informatika, Fakultas Teknik, Universitas Pasundan
[1] ferry@unpas.ac.id, [2] tirta.mulia@unpas.ac.id

Abstrak

Bitcoin digunakan secara luas sebagai mata uang digital dan sudah banyak dipakai oleh ratusan bahkan ribuan merchant diseluruh dunia secara online, sebagai mata uang yang diakui. Sistem bitcoin sendiri berbasiskan *cryptocurrency*, terlepas dari regulasi pemerintah dan ter desentralisasi. Teknologi yang digunakan berbasiskan peer-to-peer networking dan cryptography untuk menjaga integritas datanya. Walaupun penggunaan bitcoin masih belum dikenal secara luas, akan tetapi dari tahun ke tahun mengalami peningkatan pengguna yang cukup tinggi. Dalam penelitian ini akan dikaji mengenai cara mendapatkan bitcoin melalui salah satu cara yaitu mining.

Kata kunci : *bitcoin, cryptography, merchant, mining, peer-to-peer networking.*

1. Pendahuluan

Latar Belakang

Dengan meningkatnya jumlah pengguna komputer diseluruh dunia dan terhubung melalui jaringan internet, pemanfaatan teknologi World Wide Web dalam melakukan transaksi perdagangan online semakin meningkat. Hal ini menimbulkan jumlah peredaran uang di dunia maya cukup besar, mengingat tidak adanya batasan geografis. Akan tetapi sistem mata uang fiat yang sekarang ini digunakan sebagai transaksi online masih terbatas oleh aturan regulasi suatu negara yang memiliki keterbatasan dalam hal privacy, biaya transaksi, inflasi, dsb. Dari segala keterbatasan inilah muncul suatu jenis mata uang baru yang berbasis pada cryptography, yang tidak tergantung lagi pada pihak ketiga dalam mengelola peredaran uang.

Bitcoin adalah salah satu dari beberapa mata uang digital yang pertama kali muncul pada tahun 2009, sebagai mata uang digital berbasiskan cryptography. Hingga sekarang, penggunaan bitcoin sebagai mata uang digital sudah banyak digunakan oleh para pelaku bisnis online sebagai alat pembayaran. Keuntungan yang didapat dari penggunaan bitcoin ini yaitu salah satunya tidak ada batasan atau aturan baku dalam melakukan transaksi jual/beli, dimana baik penjual maupun pembeli, akan sangat sulit di lacak keberadaanya atau bersifat anonymous. Oleh karena itu, bitcoin biasanya banyak sekali digunakan sebagai alat pembayaran dalam melakukan transaksi perdagangan illegal, seperti obat-obatan terlarang. Salah satu cara untuk mendapatkan bitcoin yaitu melalui metode mining.

Tujuan

Pada tulisan ini, akan dikaji mengenai cara menghasilkan bitcoin (bitcoin mining) dengan menggunakan metode pooled mining.

Metodologi Penelitian

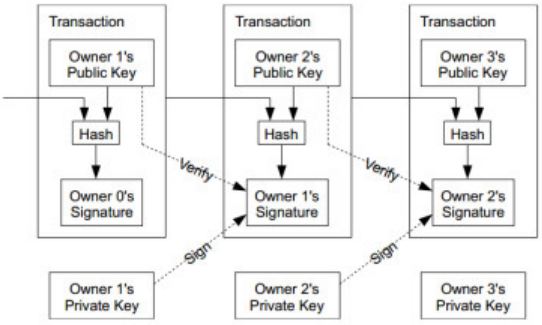
Metode yang digunakan dalam melakukan penelitian, melalui tahapan sebagai berikut :

1. Studi pustaka, untuk mendapatkan data mengenai pemahaman dasar mengenai bitcoin, penggunaan, dan bitcoin mining.
2. Eksplorasi perangkat, tahapan ini dilakukan dengan melakukan uji perangkat yang diperlukan dalam menjalan proses mining pada bitcoin.

2. Landasan Teori

2.1 Pengertian Bitcoin

Bitcoin atau disingkat dengan “BTC” adalah mata uang digital, yang tidak dikeluarkan oleh lembaga, organisasi ataupun pemerintah dalam regulasinya. Bitcoin memanfaatkan jaringan peer-to-peer network sebagai media distribusinya dengan menggunakan protokol kriptografi canggih. Pertama kali di cetuskan pada tahun 2008 oleh Satoshi Nakamoto [2], software bitcoin dibuat dan mulai dijalankan di tahun 2009. Sebuah nilai bitcoin (electronic coin) merupakan rangkaian dari sebuah tanda tangan digital. Pembahasan detail mengenai cara kerja bitcoin diluar dari cakupan tulisan ini. Pada gambar berikut dapat dilihat sebuah blok rantai transaksi yang digunakan untuk menyimpan informasi berupa informasi pemilik bitcoin tersebut.



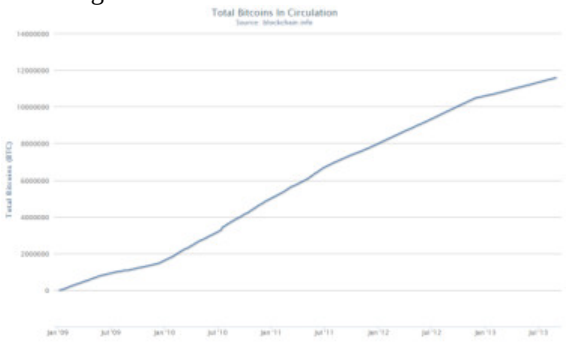
Gambar 1. Blok transaksi bitcoin [2]

Jumlah peredaran bitcoin dapat diprediksi dengan nilai yang dibatasi sebesar 21 juta bitcoin, dan nilai 21 juta bitcoin tesebut akan dicapai sekitar tahun 2040 [7], hingga saat tulisan ini dibuat baru sekitar 11 juta bitcoin [6] yang telah dihasilkan dan beredar.

2.2 Cara Mendapatkan Bitcoin

Bitcoin Mining

Mining adalah proses penambahan record transaksi pada jurnal catatan tansaksi bitcoin sebelumnya. Jurnal catatan transaksi bitcoin sebelumnya ini dikenal dengan sebutan "block chain". Mining merupakan salah satu cara untuk mendapatkan bitcoin melalui proses pencarian sebuah blok baru yang harus dikerjakan oleh seorang miner. Setiap blok baru yang berhasil ditemukan, maka seorang miner akan diberikan reward sebesar 25 BTC. Pada awalnya besar reward yang diberikan yaitu sebesar 50 BTC, akan tetapi terjadi engurangan sebesar setengah kali dari jumlah BTC sebelumnya bila telah mencapai kelipatan blok 210.000 [8]. Pada saat tulisan ini dibuat, jumlah blok yang telah berhasil ditemukan yaitu sekitar 255.048 [5]. Lama waktu pencarian untuk sebuah blok cukup bervariasi, tergantung dari seberapa cepat hardware yang dimiliki, dihitung dengan satuan Mhash/s. Berikut tren pertumbuhan jumlah bitcoin yang telah berhasil di mining.



Gambar 2. Jumlah bitcoin beredar [11]

Pasar Bitcoin

Untuk mendapatkan bitcoin, salah satu cara lainnya yaitu membeli bitcoin melalui pasar jual beli online, salah satu layanan online yang menyediakan jual/beli bitcoin yaitu MtGox yang sudah cukup lama dan terpercaya, nilai sebuah bitcoin memiliki harga jual yang sangat bervariatif, tergantung dari kondisi pasar saat itu. Pada tanggal 31 agustus 2013, nilai jual bitcoin terhadap dolar cukup tinggi yaitu pada kisaran harga $134.999 [9]. Berikut nilai jual bitcoin dari waktu ke waktu.

Gambar 3. Nilai jual bitcoin [10]

Komisi Pembayaran

Bisnis online yang beredar sekarang ini, banyak menawarkan untuk pembayaran komisi melalui mata uang bitcoin ini, sehingga memungkinkan bagi para pencari bitcoin, tanpa perlu bersusah payah mempunyai modal untuk investasi perangkat mining maupun uang untuk mulai menghasilkan bitcoin. Cukup dengan mengikuti program bisnis online yang ditawarkan, maka setiap komisi yang akan dibayarkan bisa melalu bitcoin ataupun mata uang lainnya.

2.3 Penggunaan Bitcoin

Penggunaan bitcoin sudah cukup meluas, mulai dari pembayaran untuk transaksi pembelian barang di toko-toko online hingga pembayaran transaksi jual/beli barang-barang terlarang. Dari sekian banyak manfaat dan kerugian yang ditimbulkan, tentu saja bitcoin menjadi salah satu pilihan alternatif bagi para pebisnis online. Adapun alasan yang melatar belakanginya yaitu :

1. Tidak perlu khawatir mengenai masalah keamanan, karena setiap transaksi bitcoin akan diverifikasi oleh ribuan node yang saling terhubung satu sama lain melalui jaringan peer-to-peer diseluruh dunia.
2. Bitcoin yang dimiliki akan aman, selama wallet yang disimpan oleh pemilik bitcoin tersebut, tidak jatuh ketangan orang lain.
3. Bitcoin tidak dikelola oleh organisasi, perusahaan perbankan maupun pemerintahan, tidak seperti mata uang konvensional pada umumnya. Sehingga tidak perlu khawatir apabila terjadi masalah pada lembaga pengelola tersebut. Hal ini menjadi salah satu faktor kecemasan para pebisnis online pada umumnya, dimana mereka menginginkan uang yang mereka miliki sepenuhnya aman. Kasus kecurangan pada pengelola mata uang online ini pun pernah terjadi pada Liberty Reserve sebagai salah satu layanan Online Payment Processor yang ditutup oleh FBI karena

dianggap telah melakukan praktik pencucian uang.

4. Bitcoin adalah mata uang murni yang tidak di sandarkan pada benda berharga fisik seperti emas, dollar, dsb. Sehingga kemungkinan terjadinya inflasi sangat kecil, dikarenakan jumlah bitcoin yang beredar terprediksi yaitu tidak akan melebih 21 juta bitcoin.

3. Bitcoin Mining

Teknik Mining

Ada 2 cara teknik mining yang dapat dilakukan yaitu:

1. Mining Pool

Untuk mendapatkan sebuah bitcoin apabila melakukan mining secara sendiri, tentunya akan memakan waktu cukup lama. Sehingga perlu dilakukan pembagian kerja secara tim yang dikenal dengan istilah pool. Mining pool adalah teknik mining yang dilakukan dengan cara tergabung dalam sebuah pool yang terdiri dari puluhan hingga ratusan orang. Teknik ini dilakukan melalui bantuan pool operator atau jasa pihak ketiga yang menyediakan layanan mining pool dengan potongan biaya untuk setiap blok yang berhasil ditemukan. Setiap orang yang tergabung dalam pool ini akan diberikan reward atau jumlah bitcoin yang berbeda tergantung dari seberapa besar kontribusi dari masing-masing dalam menemukan blok bitcoin tersebut. Setiap mining pool memiliki konsep sharing profit yang berbeda untuk setiap blok yang berhasil ditemukan. Berikut beberapa mining pool yang cukup populer

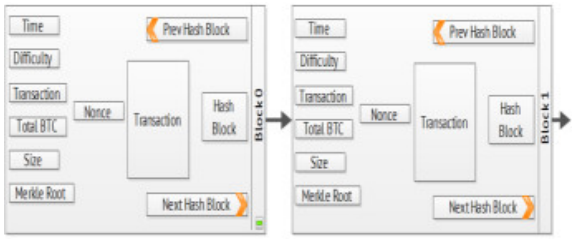
- 50BTC
- BTC Guild
- BitMinter
- Slush's Pool

2. Solo Mining

Teknik ini kurang populer dan tidak banyak digunakan, bila memiliki keterbatasan kemampuan pada perangkat keras yang dimiliki, karena cukup memakan waktu lama hanya untuk menghasilkan 1 bitcoin.

Cara kerja Mining

Proses mining dilakukan dengan cara membuat sebuah rangkaian struktur data atau dikenal dengan istilah "block chain" yang saling terkait satu dengan yang lainnya. Setiap block memiliki nilai hash dari block sebelumnya. Sehingga block ini saling terkait satu dengan yang lainnya. Berikut informasi yang tersimpan didalam sebuah block.



Gambar 4. Block diagram Bitcoin (block chain)

Dari gambar diatas, block 0 merupakan genesis block atau disebut dengan block pertama yang berhasil ditemukan. Pada dasarnya, proses mining sendiri hanyalah menemukan susunan blok baru, dimana blok ini nantinya akan digunakan untuk mencatat setiap transaksi yang terjadi pada nilai bitcoin itu sendiri. Berikut contoh isi record dari block yang mengacu pada website http://blockexplorer.com.

Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

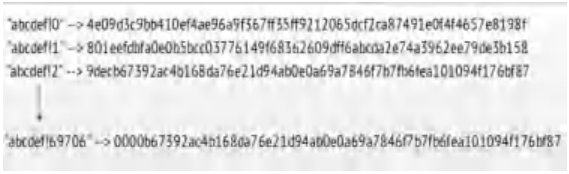
Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

Gambar 5. Block diagram Bitcoin (block chain) [12]

Proses mining dilakukan dengan cara mencari nilai sebuah hash block berdasarkan pada algoritma SHA-256. Panjang sebuah hash block terdiri dari 64 bit nilai heksadesimal. Sebuah string akan diberikan secara acak untuk dicari nilai hash-nya berdasarkan protokol bitcoin menggunakan algoritma SHA-256, nilai string ini nantinya akan ditambahkan dengan sebuah angka secara incremental atau yang disebut dengan nonce, sehingga akan dihasilkan sebuah nilai hash yang akan bervariasi. Nilai hash yang valid yaitu nilai hash yang mengandung angka '000' diawal hashnya. Apabila nilai hash ini terpenuhi, maka block tersebut berhasil ditemukan dan miner tersebut mendapatkan komisi saldo BTC yang besarnya variatif. Sebagai contoh, nilai string yang harus dicari "abcdef", string ini harus ditambahkan nilai nonce sehingga menjadi "abcdef!0". berikut gambaran proses hash string tersebut.



Gambar 6. Proses hashing string

Dari hasil pencarian didapatkan nilai nonce 69.706 yang berarti nilai hash berhasil ditemukan setelah melakukan percobaan sebanyak 69.706 kali kemungkinan. Peluang kemungkinan untuk mendapatkan nilai hash ini diatur oleh protokol bitcoin, yang berarti semakin banyak yang melakukan proses mining ini, maka akan semakin sulit peluang kemungkinan hash ini ditemukan atau disebut dengan nilai difficulty.

Perangkat Keras Mining

Untuk menjalankan bitcoin client ini, tidak diperlukan spesifikasi hardware yang terlalu tinggi, baik untuk Processor, memory dan hardisk. Akan tetapi sangat diperlukan spesifikasi yang cukup tinggi untuk perangkat GPU (VGA). Namun untuk menjaga stabilitas dari keseluruhan sistem komputer, sangat disarankan untuk menyiapkan perangkat keras yang memiliki spesifikasi cukup tinggi baik processor, memory dan harddisk. Berikut spesifikasi hardware yang digunakan untuk menjalankan bitcoin client.

Komponen	Keterangan
Power Supply	650 Watt
Motherboard	Asus P5K
CPU	Intel Core 2 Quad Q6600 @2.4Ghz
Memory	8GB DDR3
Graphics Card	Ati Radeon HD5870
Storage	80GB WDC

Faktor Pengaruh GPU Terhadap Mining

GPU dalam hal ini sangat berperan penting terhadap proses mining dibandingkan dengan CPU. GPU memiliki arsitektur yang berbeda dengan CPU, CPU dirancang khusus untuk melakukan pekerjaan yang membutuhkan banyak pengambilan keputusan. Sedangkan GPU dirancang untuk melakukan pekerjaan yang berulang. GPU Ati Radeon 5870 memiliki spesifikasi

Faktor yang mempengaruhi lamanya waktu yang diperlukan untuk menemukan sebuah blok baru pada bitcoin yaitu :

1. Difficulty
2. Jumlah blok saat ini
3. Hash Rate (hash/second)

4. Kesimpulan

Dengan semakin maraknya penggunaan bitcoin sebagai alat tukar digital, cukup menarik banyak perhatian para pebisnis online untuk mulai menggunakan uang digital ini sebagai alternatif pembayaran mereka. Disamping itu juga, sekarang ini banyak yang berlomba-lomba untuk mendapatkan bitcoin dengan cara me-mining. Dengan semakin banyaknya jumlah orang yang melakukan mining ini, tentunya akan meningkatkan tingkat difficulty dari network bitcoin tersebut. Sehingga jumlah waktu yang diperlukan untuk mendapatkan bitcoin akan semakin meningkat seiring dengan kenaikan difficulty network yang terus bertambah. Penetilian yang dibahas pada paper ini masih belum sempurna, mengingat cukup kompleksnya cara kerja dari teknologi bitcoin ini.

5. Acknowledgement

Penulis mengucapkan terima kasih banyak kepada Jurusan Teknik Informatika Universitas Pasundan Bandung yang telah mendukung penulis dalam penelitian ini dan juga kepada Bapak Husni Sastramihardja yang telah memberikan bimbingan dan arahan selama pembuatan tulisan ini.

Daftar Pustaka:

[1] R. Grinberg, "Bitcoin: An Innovative Alternative Digital Currency," Hastings Science & Technology Law Journal, 2011.
[2] S. Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System," 2008.
[3] M. Rosenfeld, "Analysis of Bitcoin Pooled Mining Reward," 17 November 2011.
[4] J. A. Kroll, I. C. Davey and E. W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries".
[5] "Blockchain," [Online]. Available: http://blockchain.info. [Accessed 30 Agustus 2013].
[6] "Blockchain," [Online]. Available: http://blockchain.info/charts/total-bitcoins. [Accessed 30 8 2013].
[7] D. R. Sterry, "Introduction to Bitcoin Mining," 2012, p. 12.
[8] D. Drainville, An Analysis of the Bitcoin Electronic Cash, University of Waterloo, 2012.
[9] "Mtgox," [Online]. Available: https://www.mtgox.com. [Accessed 31 Agustus 2013].
[10] "Blockchain," [Online]. Available: http://blockchain.info/charts/market-price?timespan=all. [Accessed 2013 Agustus 31].
[11] "Blockchain," [Online]. Available: http://blockchain.info/charts/total-bitcoins?timespan=all. [Accessed 2013 Agustus 31].
[12] "Blok Explorer," [Online]. Available: http://blockexplorer.com/b/0. [Accessed 13 1 2014].