XVI CEEL - ISSN 2178-8308
Universidade Federal de Uberlândia
05 a 09 de novembro de 2018

ANÁLISE DA VIABILIDADE DE MINERAÇÃO DE CRIPTOMOEDAS UTILIZANDO UM COMPUTADOR PESSOAL

Aldo Henrique Silva Junior*[1], Mariana Cardoso Melo[1], Gustavo Moreira da Silva[1]

[1]Uniube – Universidade de Uberaba

Resumo **- Para o funcionamento das criptomoedas como o bitcoin e monero, é essencial o processo de mineração. A mineração de criptomoedas é responsável por manter as transações seguras e pela fabricação de novas moedas. Qualquer pessoa pode disponibilizar um computador pessoal ou montar um computador dedicado para mineração e receber uma comissão por isso. Este trabalho irá verificar a viabilidade em disponibilizar um computador pessoal e um computador com placa de vídeo dedicada a mineração, os fatores analisados serão consumo de energia elétrica, capacidade de processamento de cada computador e retorno financeiro.**

Palavras-Chave **– Bitcoin, Monero, Mineração, Criptomoedas.**

ANALYSIS OF THE FEASIBILITY OF A CRYPTOCURRENCY MINING SYSTEM USING A PERSONAL COMPUTER

Abstract **- For the good working of cryptocurrencies like bitcoin and monero, the mining process is essential. Cryptocurrency mining is responsible for keeping transactions safe and produce new coins. Anyone can make a personal computer available or setup a dedicated computer for mining and get a commission. This work will verify the feasibility in providing a personal computer and a computer with video card dedicated to mining, the factors analyzed will be electric power consumption, each computer's processing capacity and profit.**

Keywords **– Bitcoin, Monero, Mining, Criptocurrencies.**

I. INTRODUÇÃO

Em um sistema monetário convencional toda produção e distribuição de moedas e notas são controladas por governos. O dinheiro é um ativo que é usado como valor de troca, geralmente utilizado em notas, moedas ou transações online [1].

É necessário um sistema organizado e eficiente, no qual todas as transações sejam feitas com segurança [3]. Um conceito de moedas vem adquirindo cada vez mais espaço, as criptomoedas, diferente do sistema tradicional, não existem em meio físico, as transações são feitas exclusivamente com o uso da internet.

*aldohj@gmail.com

Através de uma carteira digital qualquer pessoa pode transferir qualquer quantia para qualquer lugar no mundo sem necessitar de um órgão central para regular ou autorizar está transferência. A pioneira e mais conhecida é o *bitcoin*, um sistema de dinheiro eletrônico que faz pagamentos online diretamente de uma parte para outra [1].

Todas as transações são criptografadas e colocadas em uma cadeia de blocos denominada *blockchain*. A *blockchain* é como um livro de registro em que todas as transações são armazenadas, cada transação gera uma *hash* que é uma complexa sequência de números e letras, uma *hash* é gerada através de uma função *hash*, um algoritmo recebe dados de qualquer tamanho e através de uma função *hash* transforma estes dados em um código de tamanho fixo, cada *hash* da *blockchain* é concatenada na *hash* da transação anterior gerando assim uma cadeia de *hashes* interligadas que formam um bloco. Não é possível alterar uma *hash* ou um bloco sem refazer toda a cadeia [3].

Um processo de mineração consiste em computadores ligados à uma rede que contém uma cópia da *blockchain* o qual processa complexos códigos matemáticos sempre que uma transação é solicitada. O processo de mineração é fundamental para que a maioria das criptomoedas funcione de forma honesta. Esse processo permite uma forma de negócio em que qualquer pessoa pode disponibilizar seu computador ou montar uma rede de computadores para mineração e receber uma comissão em criptomoedas por isso.

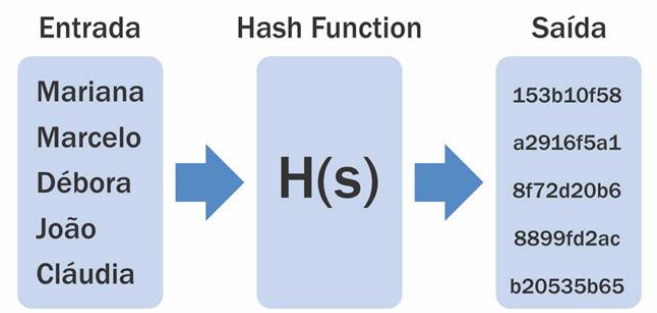
Baseado nisso, neste estudo serão analisados a viabilidade em utilizar um computador pessoal para mineração de criptomoedas e um computador com uma placa de vídeo que foi desenvolvida especificamente para mineração de criptomoedas.

II. MINERAÇÃO DAS CRIPTOMOEDAS

Segundo Fonseca (2009), a moeda possui um determinado valor de interesse a todos e pode servir como intermediário de troca, medida de valor e reserva de valor [4]. Em um sistema monetário convencional, o estado detém o monopólio sobre a moeda vigente e cabe ao estado administrar a liquidez e a produção da moeda. Qualquer tipo de moeda precisa ser

controlada para evitar que seja fraudada, um sistema convencional tem alto gasto em recursos para produção, prevenção de falsificação, transporte, segurança para transportar e armazenar em bancos. Diferente de moedas convencionais as criptomoedas não são impressas, existem somente em forma digital, todas as transações são realizadas com o uso da internet, o armazenamento das criptomoedas depende de um computador ou dispositivo eletrônico. Criptomoedas necessitam de um sistema com alta segurança para evitar que sejam falsificadas e evitar o duplo dispêndio, segundo Narayanan, 2016 para evitar esse tipo de fraude criptomoedas fazem uso de criptografia. Todas transações são codificadas em protocolos matemáticos e existem regras para criação de novas moedas. Essas criptomoedas utilizam *hashes* para criptografia em suas transações. Estas possuem uma entrada que produz uma saída codificada, na qual o valor de saída não é deduzível ou revertível como pode ser visto na Figura 1.

Figura 1: Criptografia Hash.

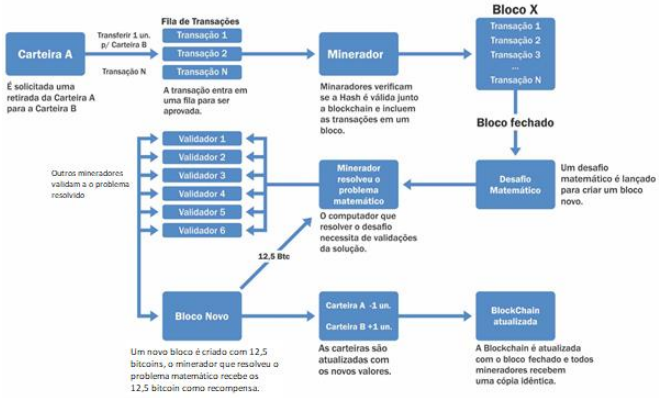


A. Bitcoin

Utilizando poder computacional, o *bitcoin* tem como proposta evitar fraudes como gasto duplo, falsificação de dinheiro e descentralizar o sistema fiduciário, reduzindo gastos com instituições financeiras.

Um servidor irá carimbar cada transação com a data e hora atual, a qual será introduzida na *hash* gerada, e será interligada com o final da *hash* anterior gerando uma cadeia. O fluxo de transferência de criptomoedas está descrito na Figura 2.

Figura 2: Fluxograma transferência de criptomoeda.



III. MATERIAIS E MÉTODOS

Para que as criptomoedas funcionem de forma segura e eficiente, a mineração é um processo em que qualquer pessoa pode ingressar utilizando um computador e recebendo comissão por isso. Assim, essa seção compara a potência consumida por um computador pessoal com um computador dedicado na mineração de criptomoedas.

Para realização deste trabalho foram utilizados seis computadores com configurações iguais e um computador com configurações diferentes dos demais. Seis computadores utilizaram o processador para validar as hashes das transações, a quantidade de hashes que cada computador pode processar depende de quão rápido seja o processador e a quantidade de núcleos que o processador tem.

Um computador foi montado com uma placa de vídeo que foi desenvolvida especificamente para mineração de critomoedas, a placa de vídeo Asus Mining RX470. Através de um script os computadores ingressaram em um pool computacional, através do site minergate.com, foram configurados o script e a carteira pessoal que receberá a comissão pela mineração.

Foram utilizados os seguintes materiais.

1. Seis computadores, equipados com processador i5-3230, 4gb de memória ram ddr3, HD 500gb, fonte de alimentação 250W.
2. Um computador com processador i5-4570, 12gb de memória ram ddr3, HD 1000gb, fonte de alimentação 600W, placa de vídeo Radeon RX470 Mining.

A. Ingresso em Pool Computacional

O primeiro passo foi cadastrar em um pool computacional, nesse caso foi utilizando o site minergate.com, um script é executado para se conectar em um protocolo TCP, um aplicativo do pool computacional transforma o computador em um nó na rede p2p através do endereço stratum+tcp://xmr.pool.minergate.com e pela porta 45700.

É possível selecionar a quantidade de núcleos que o processador irá trabalhar, quanto mais núcleos mais hashes são processadas.

Para o computador com uma placa de vídeo específica para mineração, alguns parâmetros foram alterados para direcionar o processamento das hashes para a placa de vídeo . Durante o processo de mineração com a placa de vídeo o processador não foi utilizado para validar as hashes, é possível utilizar tanto a placa gráfica quanto o processador para trabalharem em conjunto.

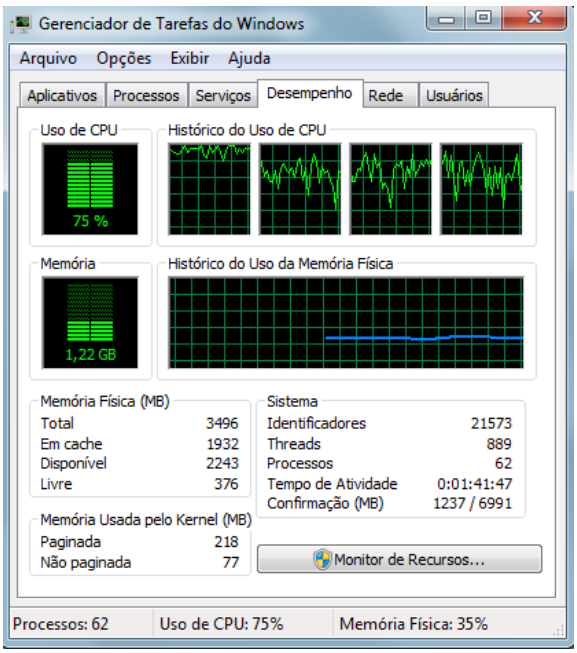
B. Computador Pessoal Para Mineração

Seis computadores pessoais ingressaram como nó na rede p2p para processar transações da criptomoeda monero, estes computadores utilizam o processador para validar cada transação que recebe.

Os computadores utilizados possuem quatro núcleos de processamento, porém foram utilizados três núcleos para que o processador não trabalhasse no limite, pode ser visto na figura 11 que o processador trabalha com 75% da capacidade

total, quando os 4 núcleos estão trabalhando o processador aparece com 100% de uso conforme mostra a Figura 3.

Figura 3: Desempenho computacional



C. Computador Com Placa de Vídeo Dedicada a Mineração

Um computador com uma placa de vídeo que foi desenvolvida especificamente para mineração de criptomoedas foi ingressado em uma rede p2p para processar transações da criptomoeda monero, todas hashes foram direcionadas para a placa de vídeo que por ter 2048 núcleos, consegue processar mais *hashes* do que um processador comum.

A Placa de vídeo pode ser observada na Figura 4.

Figura 4: Placa de vídeo utilizada

D. Processamento de Dados

Assim que o script é executado em um computador, é verificado o endereço da carteira para onde a comissão será creditada, é configurado o número de núcleos que fará o processamento dos dados, então o computador ingressa no pool computacional pelo IP 176.9.147.178 e porta 45560, e pelo IP 78.46.23.253 e porta 45560.

Após a conexão ter sido confirmada, o processador começa a receber as *hashes* em formato de *json* (JavaScript Object Notation) que é um formato que permite troca de dados de linguagens de programação diferentes, o computador minerador verifica na *blockchain* se a *hash* recebida é válida ou não, então retorna uma mensagem de confirmação através de um id que é devolvido à rede.

E. Capacidade de Processamento.

Um log é gerado com informações como a quantidade de hash que está sendo processada por segundo, porém este log possui um arquivo muito extenso devido ao alto número de informações que são registradas. Para filtrar as linhas necessárias para análise foi utilizado o programa excel.

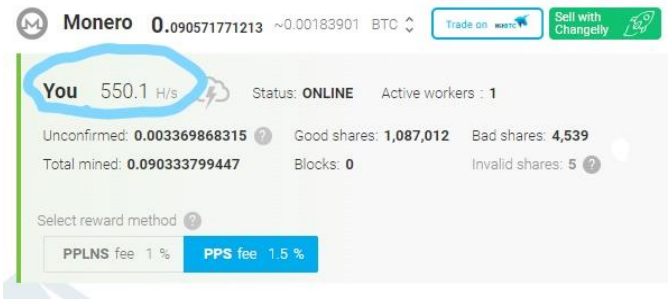
Três informações foram extraídas do log, quantidade de hashes processadas por segundo, tempo de trabalho na rede p2p e tamanho do arquivo que foi processado.

Devido a grande quantidade de informações geradas, foram utilizados vinte arquivos de log de somente um computador, o programa o excel foi utilizado para gerar gráficos de dispersão, taxa média e desvio padrão, para analisar a velocidade de processamento.

O log do script que processou as hashes na placa gráfica possui especificações diferentes e não armazenaram informações como a quantidade de hashes processadas a cada segundo e tamanho dos arquivos processados.

Algumas telas foram capturadas com a velocidade de processamento que era registrada na carteira de mineração como se pode ver na Figura 5.

Figura 5: Taxas das hashes processadas



F. Consumo de Energia Elétrica

O consumo elétrico foi estimado de acordo com a soma do consumo de todos os componentes do computador, processador, disco rígido, memória ram, placa mãe, fonte de tensão e placa de vídeo.

O consumo foi calculado de acordo com a potência que o aparelho consome multiplicado pelo tempo de uso do aparelho em horas.

O valor gasto de energia elétrica é o consumo total multiplicado pela tarifa utilizada da concessionaria Cemig que em 2018 foi definida como R$ 0,49414.

‘

G. Quantidade de Arquivos Processados.

No final de cada log ficou registrado o tamanho total do arquivo que foi processado para colaborar com a montagem de parte de um bloco, esta informação foi separada e somada utilizando o excel.

H. Comissão Gerada.

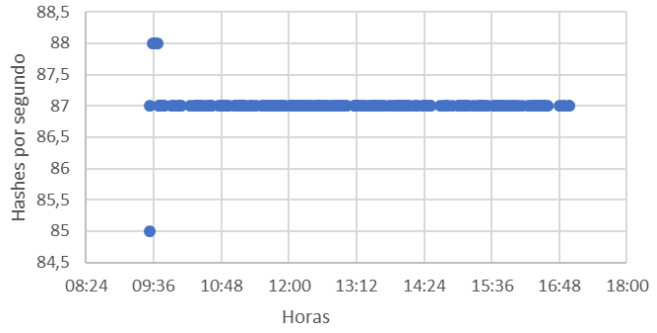
Toda comissão é creditada em poucos minutos de processamento, ela acontece de forma crescente à medida que o computador está trabalhando no processo de mineração.

Pode ser acessada de qualquer dispositivo com acesso à internet, e ser transferida para qualquer outra carteira.

IV. RESULTADOS E DISCUSSÕES

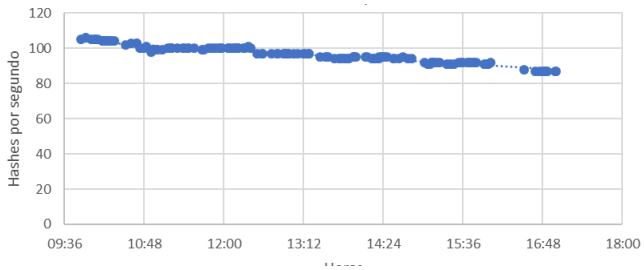
Foram usados dados de dois dias distintos para gerar gráficos de dispersão, em que um mostra uma constância na taxa de hashes que pode ser observado na Figura 6.

Figura 6: Taxa de processamento das hashes - Dia 1



Um segundo dia foi medida a taxa de hashes processadas e mostra que houve um decaimento ao longo do dia que pode ser observada na Figura 7.

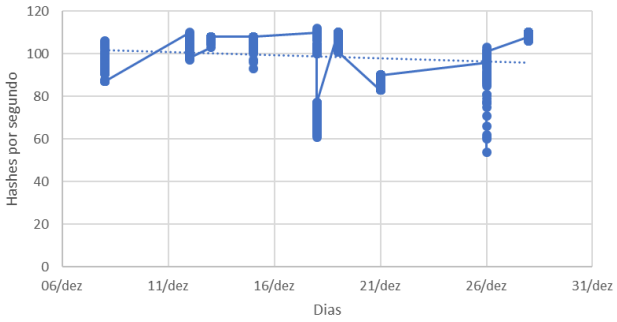
Figura 7: Taxa de processamento das hashes - Dia 2



Uma quantidade maior de dados foi tomada para o período de um mês como mostra a Figura 8, na qual se pode observar oscilações, porém a linha de tendência mostra um decaimento, as oscilações podem ser causadas por variação na velocidade da internet e subsequente decaimento da taxa de processamento já que os pacotes a serem processados terão mais dificuldade para serem recebidos.

Pode ser pelo uso de outras tarefas no computador em trabalho paralelo com o processo de mineração rodando

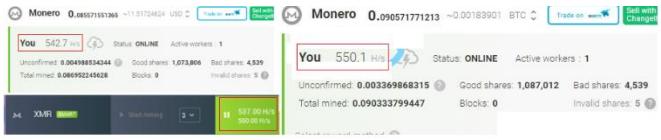
Figura 8: Taxa de processamento das hashes - Diária



Foi calculado a média padrão, utilizando 3987 amostras da taxa de hashes processadas por segundo e tendo como resultado uma média de 98 hashes processadas a cada segundo, e desvio padrão de 12,0942.

O script que foi utilizado para placa gráfica não registrou nos logs a velocidade de processamento, algumas capturas de tela foram tiradas mostrando a velocidade de processamento como pode ser visto na Figura 9.

Figura 9: Hashes processadas por segundo placa gráfica



Além da taxa de processamento também deve se avaliar o consumo de energia elétrica, no qual cada componente do computador pode ser visto na Tabela 1, os valores variam de acordo com o uso de cada componente, foram utilizados valores aproximados de consumo.

Tabela 1: Consumo do computador pessoal.

Componente	Consumo (W)
Placa mãe	40
Processador	80
Memória RAM	10
HD	20
Fonte de alimentação	40
Total	190

Para calcular o consumo de energia elétrica pode-se utilizar a seguinte formula:

$$\text{Consumo} = \frac{\text{Qpc x Pot x H x D}}{1000} \quad (1)$$

Em que:
Qpc é a quantidade de computadores utilizados.
Pot é a potência consumida pelo computador.
H é o número de horas utilizados por dia.
D é a quantidade de dias.

Assim, o consumo computador pessoal foi medido utilizando seis computadores durante 65 dias de mineração com uma média de uso de 5 horas por dia.

$$\text{Consumo 1} = \frac{6 \text{ x } 190 \text{ x } 5 \text{ x } 65}{1000} = 370{,}5\text{KW/h} \qquad (2)$$

Multiplicando o valor do consumo pelo valor da tarifa de R$0,49.

$$\text{Valor gasto} = 370{,}5 \text{ x } 0{,}49 = \text{R\$}181{,}55. \qquad (3)$$

Para o computador com placa gráfica foi utilizada a Tabela 2 para medir o consumo total.

Tabela 2: Consumo do computador com placa gráfica

Componente	Consumo (W)
Placa mãe	40
Processador	80
Memória RAM	10
HD	20
Fonte de alimentação	40
Placa gráfica	110
Total	300

Este computador minerou durante 34 horas tendo o seguinte consumo.

$$\text{Consumo 1} = \frac{1 \text{ x } 300 \text{ x } 34 \text{ x } 1}{1000} = 10{,}2\text{KW/h} \qquad (4)$$

Multiplicando o valor do consumo pelo valor da tarifa de R$0,49.

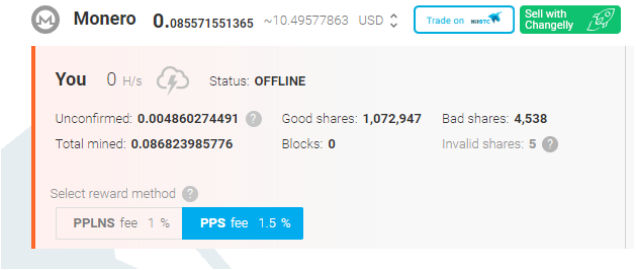
$$\text{Valor gasto} = 10{,}2 \text{ x } 0{,}49 = \text{R\$}5{,}00. \qquad (5)$$

O lucro obtido foi acumulado em uma carteira digital no próprio site usado para o pool de mineração, o valor da criptomoeda convertida para reais oscilou muito durante o período de mineração, a carteira chegou a registrar lucro de US$30,00 cerca de R$110,00 quando a monero atingiu uma cotação de US$494,00 que pode ser vista na Figura 10, então houve queda e a cotação da moeda caiu de forma acentuada, atingindo uma cotação em 26/06/2018 de US$122,00.

Figura 11: Cotação Monero-Dolar

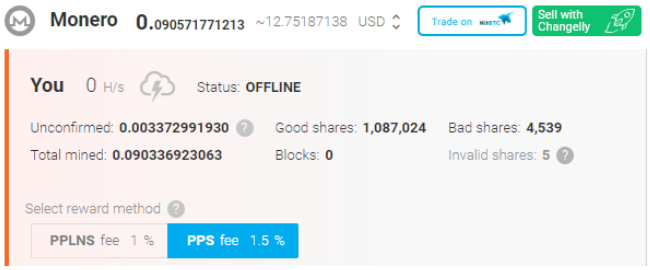
Foi minerado uma quantidade de 0,086823985776 e o lucro obtido com o uso dos computadores pessoais foi de US$10,49 que convertido para reais corresponde a R$41,02 pode ser observado na Figura 11.

Figura 10: Carteira Digital com lucro usando computador pessoal



Após o uso da placa gráfica para mineração, foi incrementada uma quantidade de 0,003512937287 em monero, o valor da certeira em dólares aumentou US$2,25 em uma conversão direta para reais é de R$8,80, pode se observar o valor atual na Figura 12.

Figura 12: Carteira digital após uso placa gráfica.



O computador com placa dedicada gastou de 10,2KW/h para minerar uma quantidade de 0,003512937287 moneros, os computadores de uso pessoal gastaram 15KW/h para minerar a mesma quantidade em monero.

V. CONCLUSÕES

As criptomoedas utilizam tecnologias promissoras, cada vez mais ganham adeptos e investidores. O processo de mineração é essencial para manter o funcionamento da rede de forma honesta e evitar que aconteçam fraudes.

Disponibilizar um computador de uso pessoal somente para o processo de mineração é pouco rentável, o gasto com consumo de energia elétrica é bem superior ao valor recebido de volta em comissão. Como é possível configurar a quantidade de processamento que se deseja dedicar ao processo, pode utilizar o processo de mineração com algum trabalho feito em paralelo que não demande muita potência do processador.

Um computador com hardware dedicado para mineração mostra que é possível obter lucro com o processo de mineração. O lucro obtido pode ser ainda maior, o computador montado utilizou somente uma placa gráfica específica para mineração, existem outras peças como placa mãe e memorias que foram desenvolvidas para mineração e podem otimizar o sistema aumentando o lucro obtido.

REFERÊNCIAS

[1] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. Bitcoin and Criptocurrency Technologies. Princeton. Princeton University, 2016.

[2] Gouvêa, Joaquim Osvaldo Pereira de. Mercado de Capitais e Derivativos. São Paulo. Pearson Education do Brasil, 2013.

[3] Pereira, Cleverson Luiz. Mercado de Capitais. 1. Ed. Curitiba. Intersaberes, 2013.

[4] Fonseca, José Wladimir Freitas da. Mercado De Capitais. Curitiba. Iesde Brasil S.A., 2009.

[5] Neto, José Luís de Castro; Gomes, Renata Sena. Análise De Risco e Crédito. Curitiba. Iesde Brasil S.A., 2009. 212 P.

[6] Bitcoin. Disponível em <Https://Bitcoin.Org/Pt_Br/> Acesso em 19/06/2018.

[7] Block Chain. Disponível em < Https://Blockchain.Info/Pt/> Acesso em 19/06/2018.

[8] Instituto Nacional De Estatística (2003). *Índices de Preços na Produção Industrial*. Acessado em 24 de Novembro de 2003, Em: Http://Www.Ine.Pt.

‘