MANUAL DO INICIANTE EM CRIPTOMOEDAS

NATANAEL ANTONIOLI

FÁBRICA DE NOOBS

1 SUMÁRIO

2 Introdução 3
2.1 O que você encontrará aqui?.....3
2.2 O que são criptomoedas? 3
2.2.1 Criptomoedas x dinheiro virtual 3
2.2.2 Eis que surge o Bitcoin... 4
2.2.3 E então surgiram outras moedas... 5
3 O funcionamento das criptomoedas 6
3.1 Critpomoedas e dinheiro real.....6
3.2 O que possibilita que as criptomoedas sejam utilizadas como dinheiro? .8
3.3 A mineração 11
3.4 Compra, venda e negociações.....15
4 Manuseando criptomoedas 17
4.1 Conhecendo o projeto 17
5 Carteiras 19
5.1 Tipos de carteiras 19
5.1.1 Wallet-core 19
5.1.2 Wallets leves.....21
5.1.3 Wallets online.....22
5.1.4 Wallets de papel 23
5.2 Manuseando uma carteira 25
5.2.1 Operações básicas 25
5.2.2 Encriptando sua wallet 31

5.2.3 Exportando um backup 33
5.2.4 Restaurando um backup 33
5.3 Como manter sua carteira segura? 34
6 Suas primeiras moedas 36
6.1 Faucets 36
6.2 Comprando criptomoedas 38
7 Mineração 43
7.1 Tipos de mineração 43
7.2 Mineradores 45
7.3 Mineração em pool 47
7.4 Cuidados durante a mineração 54
7.5 Técnicas de arrefecimento 56
7.5.1 Dissipadores de calor 56
7.5.2 Ventoinhas 57
7.5.3 Cooolers 59
7.5.4 Refrigeração com água 59
8 Negociando criptomoedas 61
8.1 Depositando suas primeiras moedas 61
8.2 Compreendendo as negociações 63
8.3 A primeira negociação 66
8.4 Dicas para negociação 69
8.4.1 Gráficos em candlestick 69
8.4.2 Padrões em candles 73

2 INTRODUÇÃO

2.1 O QUE VOCÊ ENCONTRARÁ AQUI?

Você provavelmente já ouviu falar em Bitcoins. Seja ao pesquisar sobre a Deep Web, ao tomar conhecimento do ataque massivo do vírus WannaCry, ou ao ler notícias a respeito da incomum valorização da moeda ocorrida em maio deste ano.

Também já deve ouvido falar em alguns investidores sortudos que compraram Bitcoins no início do projeto e se viram ricos após a alguns anos. Podemos citar, por exemplo, o caso do norueguês Kristoffer Koch, que adquiriu o equivalente a 55 reais em Bitcoins como parte de sua tese sobre criptografia e, 6 anos depois, possuía uma quantia equivalente a 8,5 milhões de reais – o suficiente para comprar um apartamento no bairro mais rico de Oslo (https://pro.tecmundo.com.br/bitcoin/91673-homem-compra-r-66-bitcoins-esquece-eles-valem-r-8-5-milhoes.htm).

Junto dessas notícias, também surge a promessa de investimentos lucrativos e, por consequência, dinheiro fácil. É o que a maioria daqueles que se propõe a explicar a respeito de criptomoedas faz: um vídeo irrebobinável de meia hora em uma página chamativa, com alguém prometendo ensinar um método fantástico para ganhar direito. Não é isso que você encontrará aqui.

O objetivo deste material é lhe transmitir as informações necessárias para que você se torne apto para lidar com todo o espectro que envolvem criptomoedas, desde a instalação e gerenciamento das carteiras até os processos de mineração, compra e venda de criptomoedas. Também lhe mostrarei as melhores formas de se relacionar com este mercado e planejar um possível investimento na área.

Bons estudos!

2.2 O QUE SÃO CRIPTOMOEDAS?

2.2.1 Criptomoedas x dinheiro virtual

Apesar de muitas matérias denominarem indistintamente criptomoedas como moedas virtuais, existem algumas diferenças. As moedas virtuais surgiram em meados da década de 90, juntamente com a popularização da informática, e não ofereciam nenhuma forma de segurança ou descentralização.

Na realidade, tratavam-se apenas de sistemas nos quais o usuário poderia adquirir vouchers numerados – comprados com dinheiro oficial – e gastá-los online, inserindo seus respectivos números para efetuar suas compras.

Em um contexto no qual a segurança para transações na Internet era escassa, tais recursos se popularizaram, uma vez que a inserção de cartões de crédito online não era necessária.

Pouco tempo depois, com o avanço nas tecnologias de internet banking e transações seguras, as moedas virtuais perderam espaço, pois não era mais cômodo se deslocar até um estabelecimento (muitas vezes uma loja de conveniência) para adquirir o voucher, e só depois gastá-lo.

2.2.2 Eis que surge o Bitcoin...

Em 2009, um programador japonês – ou uma equipe de programadores – denominado Satoshi Nakamoto apresentou o Bitcoin. Tratava-se de um complexo sistema descentralizado no qual os usuários poderiam adquirir e enviar unidades da moeda para outros usuários.

A invenção de Nakamoto era controlada unicamente através de software, o qual seria responsável por liberar um total de 21 milhões de Bitcoins, ao longo de aproximadamente vinte anos. A cada dez minutos, as moedas seriam distribuídas através de um processo semelhante a uma loteria, na qual mineradores deveriam "jogar" sucessivamente e o que tivesse o computador mais rápido seria recompensado.

Nos anos seguintes ao lançamento do sistema, o interesse dos usuários foi aumentando, fazendo com que mais e mais usuários se interessassem em minerar a moeda, o que culminou para o surgimento de casas de câmbio, que permitiriam que qualquer pessoa pudesse adquirir Bitcoins a partir de dinheiro oficial.

Gradualmente, vendedores também começaram a aceitar Bitcoins, fazendo com que o valor de cada Bitcoin aumentasse expressivamente. Poucos anos depois, Nakamoto havia construído uma nova moeda, capaz de ser utilizada em transações, minerada, vendida ou comprada.

Ainda hoje, a identidade de Nakamoto permanece um mistério. Entre 2009 e 2011, o programador realizou algumas postagens a respeito do assunto, até se desligar completamente do projeto e desaparecer. Entretanto, seu legado já estava lá, e não poderia ser desligado – lembre-se da descentralização do sistema.

Desde então, o Bitcoin passou a ser aceito e utilizado como moeda, chegando a incrível cotação de 3 mil dólares.

2.2.3 E então surgiram outras moedas...

Inspirados no algoritmo criado por Nakamoto, outros programadores criaram novas criptomoedas, com funcionamento semelhante. Por tratar-se de um código de livre acesso, a modificação do mesmo é extremamente fácil, permitindo que qualquer pessoa com relativo conhecimento possa lançar sua própria criptomoeda.

Das principais, podemos citar a Dogecoin, a Litecoin, a Ethereum e a Darkcoin, sendo essas as mais comumente aceitas no mercado. Porém, existem atualmente cerca de 700 criptomoedas distintas, algumas com características no mínimo curiosas, outras com projetos descontinuados e, ainda, outras que não possuem lastro, servindo apenas para fins didáticos.

Nas próximas páginas, verificaremos quais as diferenças entre uma criptomoeda e outras formas de dinheiro, além de estudarmos a fundo o processo de geração e funcionamento das criptomoedas.

3 O FUNCIONAMENTO DAS CRIPTOMOEDAS

3.1 CRITPOMOEDAS E DINHEIRO REAL

Antes de abordarmos as criptomoedas, convido o leitor a fazer um rápido exercício mental. Imagine que você viva em uma pequena vila e produza trigo. Evidentemente, você não sobrevive apenas de trigo, já que precisa de outros produtos – por exemplo, sapatos.

Então, você vai até um produtor de sapatos e propõe trocar uma saca do trigo que produziu por alguns pares de sapatos. No entanto, o artesão já possui trigo de sobra, mas estaria disposto a trocar seus sapatos por whisky.

Para concretizar sua transação, você precisará encontrar alguém que produza whisky e queria trocá-lo por trigo, para em seguida voltar ao vendedor de sapatos e trocar novamente o whisky pelos sapatos. E ainda torcer para que ninguém seja mais rápido no processo.

Logo, uma economia em larga escala a base de trocas torna-se inviável, surgindo então a necessidade da existência de um material que seja aceito por todos. Naturalmente, algumas mercadorias passaram a ser aceita por todos, normalmente por possuir alguma utilidade prática comum.

Daí, podemos elencar a primeira condição para que um item possa ser utilizado amplamente como moeda de troca: **ser aceito por todos**.

Agora, suponha que sua comunidade decida realizar as trocas em pedras. Se uma saca de milho valesse um punhado de pedras, qualquer pessoa seria capaz de compra-la sem muito esforço, e você não veria razões para continuar produzindo trigo, já que é muito mais fácil coletar algumas pedras na rua e trocar pelos produtos que precisa. Dessa forma, ninguém mais produziria bens e o mercado não mais existiria.

Uma alternativa para o problema seria elevar o preço da saca de trigo para algumas toneladas de pedra. Obter manualmente uma dezena de toneladas de pedra para comprar os bens de que precisa seria muito mais difícil do que produzir trigo e vende-lo, então você o faria.

Porém, você seria obrigado a carregar suas toneladas de pedra pela vila toda vez que precisasse comprar algum item, o que seria extremamente complicado. A solução definitiva foi a adoção de itens mais raros.

Exemplos de mercadorias utilizadas como moedas de troca foram o gado bovino e o sal. Logo, você poderia trocar algumas sacas de trigo por punhados de sal e então utilizá-los para comprar um par de sapatos e garrafas de whisky, sem necessidade de rodar a cidade em busca de alguém disposto a aceitar seu produto.

Note, agora, outra característica necessária para que um item se torne uma moeda: **sua raridade**.

Entretanto, nem todas essas mercadorias apresentavam praticidade em sua circulação. O sal, por exemplo, poderia apresentar diversos níveis de pureza, além de ser facilmente dispersado e perdido.

Tão logo, surgiram os metais, como o ouro e a prata. Estes eram raros, facilmente moldáveis, apresentavam facilidade de transporte e fácil averiguação de pureza, além de poderem ser entesourados sem preocupações com a degradação das moedas.

Têm-se, então, outra característica importante: **a praticidade**.

Porém, ainda poderiam haver variações no momento de se averiguar seu grau de pureza. Surgem, então, a necessidade de certificar o metal de sua validade comercial, originando as primeiras cunhagens de moedas. Normalmente, o valor de uma moeda era avaliado pela quantidade de metal empregada em sua composição, na qual, por exemplo, uma moeda de 20 gramas de ouro seria trocada por uma mercadoria de mesmo valor.

Essa “certificação” reforça a primeira característica que estudamos neste capítulo, a sua aceitabilidade.

Na idade média, com o surgimento das rotas comerciais de longa distância, surgiu o costume de armazenar as moedas com um ourives, responsável por emitir um recibo que certificasse a posse do dinheiro. Por serem mais práticos do que as moedas de metal, eles passaram a ser usados também em transações, originando as primeiras células.

Com o tempo, da mesma forma ocorrida com as moedas, o governo passou também a emitir cédulas, controlando as falsificações e garantindo o poder de pagamento, além de garantir que cada cédula emitia corresponderia ao seu valor armazenado em ouro, denominado **lastro**.

Na maioria dos estados modernos, há uma instituição, denominada Banco Central, responsável por controlar a emissão de moeda.

Podemos, portanto, deduzir que para que qualquer item seja utilizado em larga escala como moeda na atualidade, ele precisa obrigatoriamente apresentar as características acima.

O mesmo vale para as Bitcoins, mas com correspondências diferentes – afinal, há uma grande discrepância entre o dinheiro físico e aquele controlado unicamente por um algoritmo de computador.

3.2 O QUE POSSIBILITA QUE AS CRIPTOMOEDAS SEJAM UTILIZADAS COMO DINHEIRO?

Como estudamos nas páginas anterior, um item precisa atender a algumas características para que possa ser utilizado como moeda de troca. O mesmo vale para o Bitcoin.

Para entendermos estes fatores, precisamos primeiro entender como uma criptomoeda funciona, desde seu lançamento na Internet até o processo de aquisição de unidades pelos usuários.

Uma das garantias pelas quais o dinheiro pode ser utilizado com segurança está em quem controla sua emissão. Um Estado centralizador é capaz de regulamentar a emissão da moeda, cabendo a ele a responsabilidade de garantir a autenticidade das cédulas e, principalmente, impedir que o mercado seja inundado repentinamente por uma emissão inapropriada de dinheiro – causando um processo de inflação.

Quando lidamos com uma moeda virtual, não há como deixa-las nas mãos de um Estado e, muito menos, de um indivíduo ou empresa, pois nenhum destes inspiraria credibilidade suficiente para tal. Pense: você trocaria todo seu dinheiro em uma moeda que eu criasse, cabendo a mim decidir quando emitir e para quem distribuir novas moedas? A resposta seria não, pois você não confiaria na minha capacidade de fazê-lo. E nem deveria.

Dessa forma, se a centralização não é possível, resta a segunda alternativa: deixar o controle da moeda nas mãos de uma estrutura descentralizada. No caso, de um algoritmo de computador que opera na forma peer-to-peer, ou P2P. peer (ou P2P).

Nessas redes, cada computador (agora chamado de node), através de seu respectivo provedor de Interna, se conecta com outros computadores integrantes da rede, de forma que a transmissão de pacotes é feita diretamente de node para node.

Através desse tipo de organização, têm-se um sistema no qual todos os computadores desfrutam do mesmo tipo de acesso à rede, o qual continuará funcionando mesmo que algum dos nodes saia do ar.

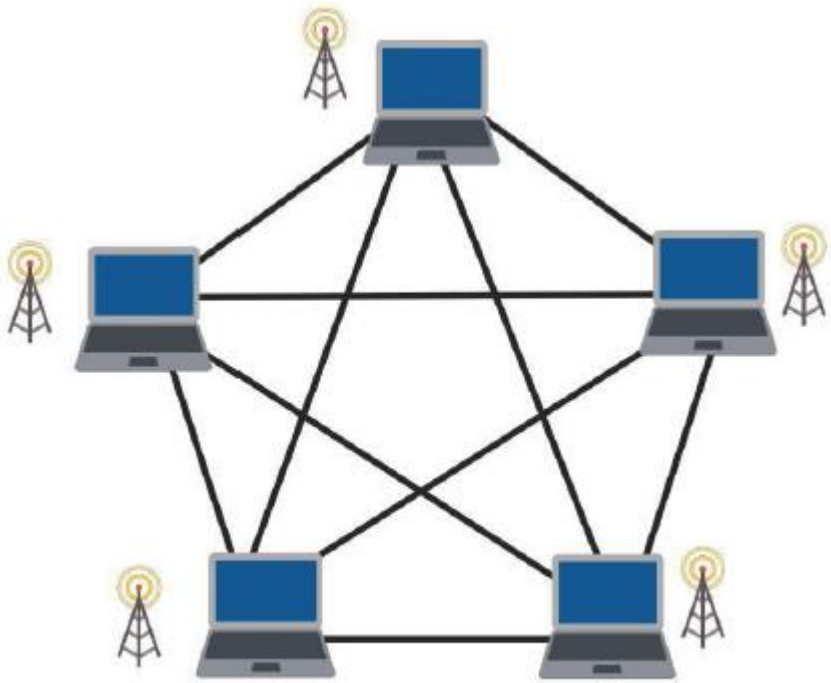


Figura 1: computadores arquitetados na forma de rede P2P.

Dessa forma, temos aqui as duas primeiras características do sistema de Bitcoins: **ele é descentralizado e impossível de ser retirado do ar**. Isso garante que o usuário possa ter segurança na moeda, já que ela não estará sujeita às vontades de algum indivíduo.

Essa é a razão pela qual as Bitcoins continuaram em vigor após o desaparecimento de Nakamoto: o sistema independia de seu criador para funcionar.

Entretanto, o que garante que Nakamoto, por exemplo, não tenha inserido uma linha de código no programa que faça com que a cada x Bitcoins transferidas, uma fração não seja transferida para sua conta pessoal?

É neste momento em que a ideologia do código aberto entra em cena. O algoritmo das Bitcoins – e das demais criptomoedas – foi disponibilizado sobre a chamada Licença MIT, que confere a qualquer usuário o direito de modificar, distribuir e, sobretudo, ler o código-fonte.

Logo, qualquer instrução maliciosa inserida no programa seria rapidamente identificada pelos demais usuários, e a moeda não obteria nenhum tipo de credibilidade sendo, portanto, ignorada.

Observe outra característica fundamental de uma criptomoeda: **o usuário não depende da fé para confiar no seu funcionamento**, já que pode, com alguma experiência, compreendê-lo e procurar falhas. Essa ação também garante que a moeda não será falsificada ou burlada, **eliminando a necessidade de um poder centralizador**.

Ainda assim, resta um último detalhe: o que controla a emissão de novas Bitcoins, e o que garante que o mercado não será subitamente inundado por Bitcoins, causando um processo de inflação e fazendo-o perder milhares de reais investidos?

Evidentemente, essa responsabilidade cabe ao algoritmo que administra a rede. Entretanto, como isso é possível?

O correto funcionamento do sistema de criptomoedas depende, sobretudo, e duas coisas: a emissão de moedas – garantindo sua raridade – e a constante vistoria da rede, garantindo que todas as transações realizadas sejam registradas e impedindo que um mesmo Bitcoin seja utilizado duas vezes.

Por se tratar de um software P2P, é necessário que esta operação seja feita de forma descentralizada, delegando a tarefa aos usuários do sistema. Por consequência, o processo consome capacidade de processamento, armazenamento em disco, banda de Internet e energia.

A solução encontrada por Nakamoto foi simples e engenhosa: associar a emissão de novas moedas com a garantia da segurança.

Dessa forma, os usuários que dedicassem recursos para a operação do sistema seriam recompensados com novas moedas. Ao associar o processo de manutenção da rede com a obtenção de dinheiro, pessoas se veriam motivadas a colaborar com este.

Evidentemente, aqueles que dedicassem mais recursos para o funcionamento do sistema deveriam ser recompensados com mais dinheiro, estimulando-os a oferecer cada vez mais recursos.

Mas ainda havia um problema: como evitar que alguém construa uma máquina potente, capaz de receber uma quantia imensa de Bitcoins, e causar um processo de inflação?

A solução foi fazer com que os computadores participantes, além de se encarregar da manutenção da rede, tivessem que realizar operações matemáticas para receber suas recompensas, cuja dificuldade seria determinada por um sistema que associa a quantidade de pessoas participando da empreitada com o poder de suas máquinas.

Esse sistema, denominado mineração, é o que garante a raridade das criptomoedas. A seguir, estudaremos, em detalhes, como ele ocorre.

3.3 A MINERAÇÃO

Agora que você já entendeu que o sistema de uma criptomoeda descentralizada necessita de uma força tarefa também descentralizada para funcionar e que os mineradores, remunerados na própria criptomoeda, representam essa força tarefa, é o momento de entender como o processo de mineração é realizado.

Milhares de pessoas enviam Bitcoins diariamente, umas para as outras. Mas a não ser que alguém mantenha um registro de todas essas transações, ninguém seria capaz de determinar quem pagou o quê.

A rede Bitcoin lida com isso registrando todas as transações realizadas em determinado período em uma lista, denominada **bloco**. Cada bloco é armazenado em uma cadeia de blocos, denominada **blockchain**. A blockchain pode ser usada para explorar cada transação já realizada na história de uma criptomoeda, em qualquer ponto da rede.

Entretanto, um registro precisa ser confiável, e sua autenticidade deve ser comprovada de forma digital. Como podemos ter certeza que a blockchain permanece intacta, e jamais é adulterada? É aí que entram os mineradores.

Quando um bloco de transações é criado, os mineradores devem processá-lo, transformando-o em uma cadeia numérica denominada hash, que é armazenada no bloco. A hash tem algumas propriedades interessantes: ela é única, e apenas dois blocos idênticos possuiriam a mesma hash, o que não acontece. Além disso, qualquer ínfima alteração em um bloco causa uma imensa modificação na hash.

Logo, é possível verificar a autenticidade de um bloco através da comparação de sua hash. Além disso, cada bloco é identificado com os códigos dos blocos que o sucedem e o antecedem, garantindo sua posição dentro da blockchain.

Dessa forma, os mineradores são capazes de “selar” um bloco, afirmando sua veracidade. Porém, todos eles competem entre si nesta tarefa, utilizando um

software específico para a mineração. Cada vez que uma hash é apresentada, seu respectivo minerador é recompensado com uma quantia em criptomoedas.

Porém, é extremamente fácil criar uma hash a partir de um conjunto de dados. Dessa forma a rede Bitcoin se encarrega de tornar a mineração mais difícil, através de um processo denominado proof of work, evitando que todos minerem centenas de blocos a cada segundo e inundem o mercado de Bitcoins.

Assim, o sistema exige que uma hash, para ser válida e incorporada na blockchain, deve obrigatoriamente aparentar de uma determinada maneira. Ou seja, deve conter uma determinada quantidade de zeros no início, que é determinada por um número de 32 bits denominado **nonce**.

É impossível predizer qual combinação de bits resultará no hash correto. Por essa razão, o hash é recalculado até que a sequência adequada seja encontrada. A número de bits necessário é variável, e cabe ao protocolo determiná-lo. Essa variação é denominada **dificuldade**. Dessa forma, o sistema é capaz de alterar a dificuldade de cada bloco conforme a capacidade dos mineradores, garantindo a raridade da moeda.

Ao encontrar uma hash válida, o minerador vencedor anuncia sua descoberta à rede, e ela é enviada e registrada permanentemente na blockchain. Em compensação, o ganhador recebe uma recompensa na criptomoeda corrente.

No caso da rede Bitcoin, um novo bloco é emitido a cada 10 minutos, e a dificuldade de mineração dos blocos é alterada a cada 2016 blocos. Em uma situação ideal, a dificuldade vale 1.

Portanto, em uma situação no qual cada bloco seja minerado a cada 10 minutos, seriam necessárias 2 semanas para que cada cadeia de 2016 blocos fosse concluída e, portanto, a dificuldade fosse alterada.

Entretanto, esse valor pode variar em função da capacidade dos mineradores envolvidos no processo, denominada **hashrate**, que denota quantas hashes o conjunto de mineradores é capaz de processar por segundo.

Dessa forma, quando a cadeia de 2016 blocos é concluída, o sistema ajusta a nova dificuldade de forma que a cadeia seguinte leve aproximadamente 2 semanas para ser finalizada. Se a cadeia anterior foi finalizada em menos de 2 semanas, a dificuldade aumenta. Se foi realizada em mais de 2 semanas, a dificuldade deve ser reduzida.

Assim, pode-se afirmar que a dificuldade de uma cadeia de blocos representa o tamanho da cadeia de bits cuja hash de cada bloco da cadeia possui.

Podemos converter dificuldade em bits a partir da seguinte fórmula, na qual B representa a quantidade de bits e D corresponde a dificuldade.

$$B = \log_2 D + 32$$

Por exemplo, a dificuldade atual da Bitcoin é de $678{,}760{,}110{,}083$. Aplicando a fórmula, temos que a cadeia de bits esperada para o bloco atual é de $\log_2 678{,}760{,}110{,}083 + 32 = 71{,}3$ bits.

Podemos, então, estimar o maior número de tentativas necessário para que um bloco seja resolvido, através da fórmula abaixo, na qual B representa a quantidade de bits e n a quantidade de tentativas.

$$n = 2^B$$

No nosso caso, esse valor corresponde a $2^{71{,}3} = 2{,}91525 * 10^{21}$ tentativas. Como o sistema tenta fazer com que cada bloco seja processado em 10 minutos, podemos dividir o total de tentativas pela quantidade de segundos presentes em 10 minutos, obtendo a hashrate total do bloco (H). Dessa forma:

$$H = \frac{n}{600}$$

No nosso exemplo, a hashrate corresponde a $485875 * 10^{18}$ hashes. Sabendo que $1G$ vale 10^9, podemos dizer que a hashrate total é de $4.858.754.124{,}39\ {}^{GH}/_{S}$.

Existem sites que permitem verificar todos esses valores, em primeira mão, para cada criptomoeda, como o CoinWarz (https://www.coinwarz.com/cryptocurrency).

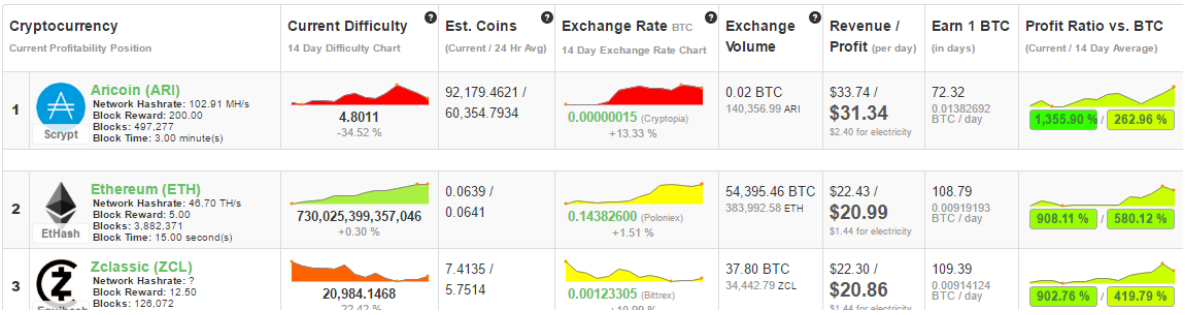
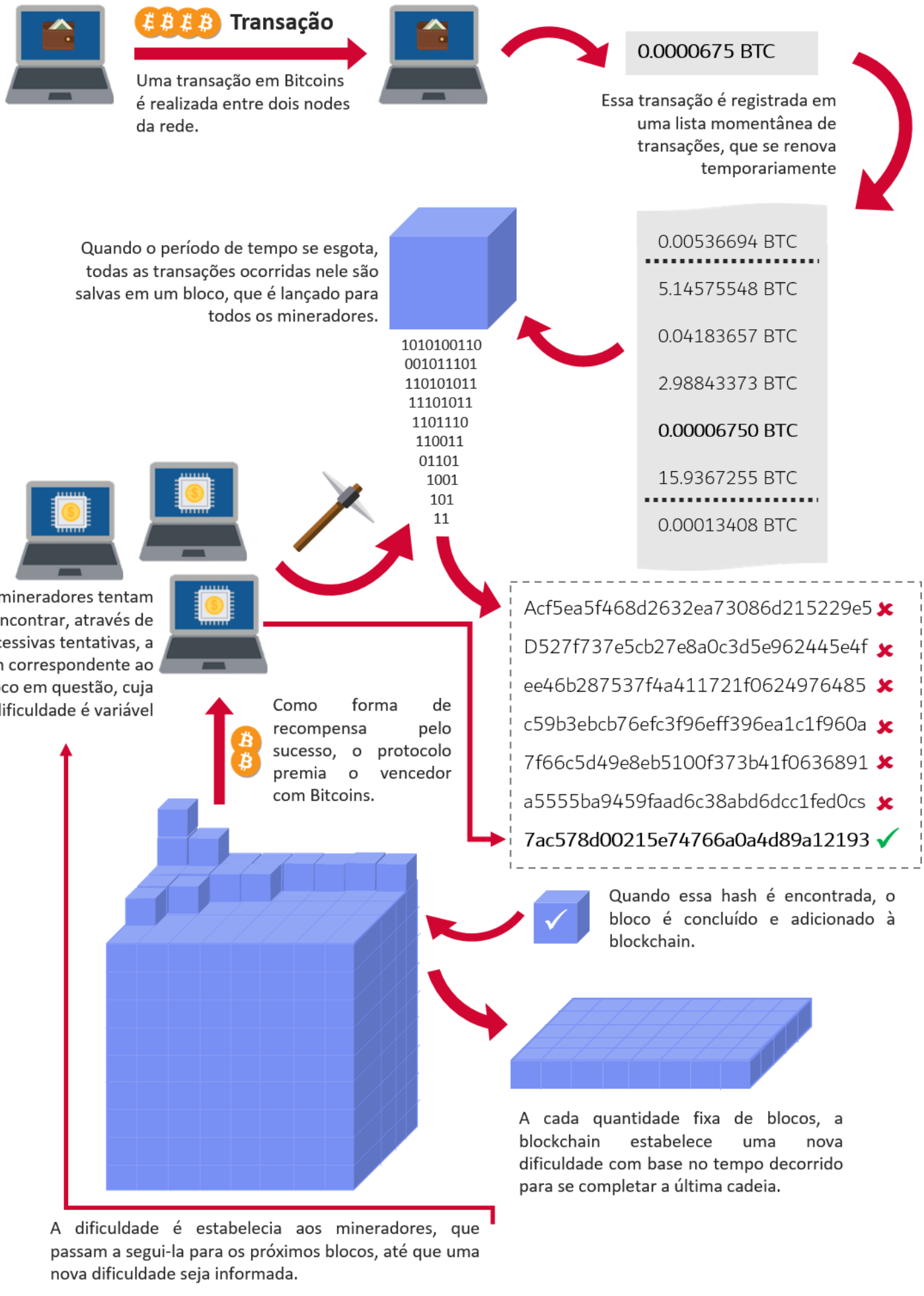


Figura 2: valores relativos à mineração de algumas critpomoedas.

Na próxima página, há um infográfico que ilustra todo o processo explicado nesta seção.


Transação
Uma transação em Bitcoins é realizada entre dois nodes da rede.
0.0000675 BTC
Essa transação é registrada em uma lista momentânea de transações, que se renova temporariamente
0.00536694 BTC
5.14575548 BTC
0.04183657 BTC
2.98843373 BTC
0.00006750 BTC
15.9367255 BTC
0.00013408 BTC
Quando o período de tempo se esgota, todas as transações ocorridas nele são salvas em um bloco, que é lançado para todos os mineradores.
1010100110
001011101
110101011
11101011
1101110
110011
01101
1001
101
11
Os mineradores tentam encontrar, através de sucessivas tentativas, a hash correspondente ao bloco em questão, cuja dificuldade é variável
Acf5ea5f468d2632ea73086d215229e5
D527f737e5cb27e8a0c3d5e962445e4f
ee46b287537f4a411721f0624976485
c59b3ebcb76efc3f96eff396ea1c1f960a
7f66c5d49e8eb5100f373b41f0636891
a5555ba9459faad6c38abd6dcc1fed0cs
7ac578d00215e74766a0a4d89a12193
Como forma de recompensa pelo sucesso, o protocolo premia o vencedor com Bitcoins.
Quando essa hash é encontrada, o bloco é concluído e adicionado à blockchain.
A cada quantidade fixa de blocos, a blockchain estabelece uma nova dificuldade com base no tempo decorrido para se completar a última cadeia.
A dificuldade é estabelecia aos mineradores, que passam a segui-la para os próximos blocos, até que uma nova dificuldade seja informada.

3.4 COMPRA, VENDA E NEGOCIAÇÕES

Uma vez que aprendemos como as Bitcoins são produzidas, resta agora estudarmos o processo de negociação das Bitcoins. Para tanto, é preciso que você veja os conteúdos estudados na seção anterior como um processo contínuo.

Aqui, abordaremos como as Bitcoins são negociadas por investidores – responsáveis por determinar sua cotação – e não por usuários comuns, já que estes serão estudados no capítulo seguinte.

O preço da Bitcoin é determinado da mesma forma que o preço de qualquer outro produto, como um carro, ou uma dúzia de bananas, é determinado: através de leis de mercado.

Comerciantes que possuam quantias significativas em Bitcoins podem vende-las e compra-las em serviços online, trocando-as por dinheiro oficial ou outras criptomoedas. Nessas situações, não é o serviço que determina o preço, mas sim os próprios comerciantes, que determinam um preço para cada negociação.

Simplificando, é a interação contínua entre vendedores e compradores que determina o preço das criptomoedas. Entretanto, é importante considerar que este preço não é determinado arbitrariamente.

Da mesma forma que um vendedor, ao estipular o preço, ele deve levar em consideração a quantidade de pessoas dispostas a pagar pelo seu produto, o mesmo vale paras criptomoedas.

Um negociador sempre irá definir o preço de suas criptomoedas considerando a oferta e demanda momentânea. Caso ele estipule um preço muito abaixo da média, suas Bitcoins irão se esgotar rapidamente e ele terá prejuízo. Caso estipule um preço muito acima, ninguém as comprará.

É assim, portanto, que o preço da Bitcoin é estipulado: a partir da última transação efetuada no momento. Evidentemente, uma casa de câmbio não será capaz de alterar o preço a todo instante, razão pela qual é adotado uma média das transações realizadas.

Além disso, as criptomoedas tendem a ser voláteis, isto é, apresentar alta variação de preço em um curto período de tempo, o que não é uma característica exclusiva das criptomoedas: petróleo, ações e vários outros produtos também sofrem tais variações.

Isso ocorre por que o mercado de criptomoedas ainda é relativamente pequeno se comparado ao de outros ramos, fazendo com que quantidades não tão

significativas de dinheiro sejam capazes de afetá-lo. Entretanto, a tendência é que o Bitcoin – e demais criptomoedas – tendam a estabilizar.

Figura 3: preço do Bicoin de 2010 até 2017.

4 MANUSEANDO CRIPTOMOEDAS

4.1 CONHECENDO O PROJETO

Antes de se iniciar na utilização de uma criptomoeda em específico, é interessante que você tire um tempo para se familiarizar com seu projeto, seus softwares e seu funcionamento.

Para isso, vá ao Google e pesquise pelo site oficial (ou de referência) da moeda. Moedas como o Bitcoin e o Litecoin possuem vastos artigos explicando seu funcionamento, inclusive versões em português.

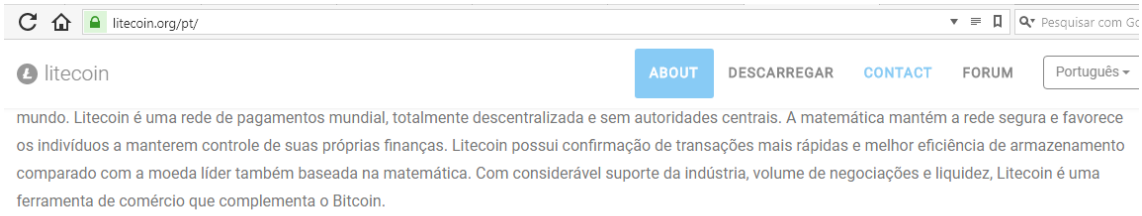
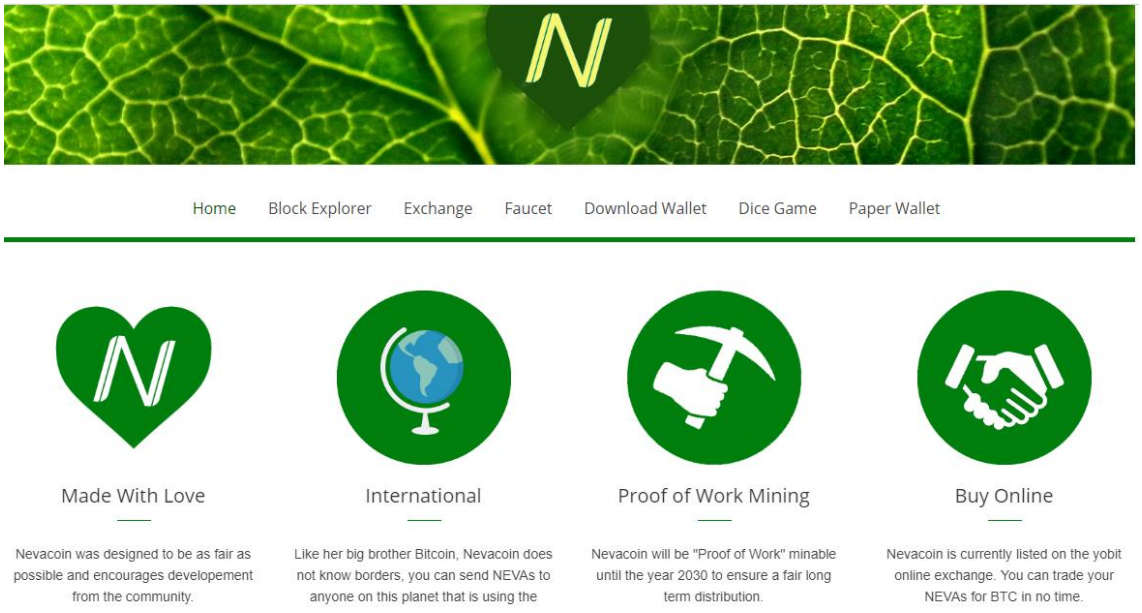


Figura 4: site do projeto Litecoin.

Já outros, principalmente de moedas menores, como a Nevacoin, possuem apenas sites em inglês, mas suficientemente intuitivos para um usuário iniciante.



Por fim, existem ainda aquelas criptomoedas que são lançadas de forma quase experimental, e cujos criadores não possuem recursos para manter um site amigável funcionando.

Nesse caso, sempre haverá uma postagem no BitcoinTalk (https://bitcointalk.org), fórum dedicado a discussão geral sobre criptomoedas, a respeito da moeda em questão.

Figura 5: anúncio de nova criptomoeda no BitcoinTalk.

Em todas as situações, é importante que você navegue pelos tópicos da moeda e se familiarize com a terminologia já conhecida. Normalmente, valores como a dificuldade atual de mineração ou o tempo de emissão de cada bloco serão exibidos.

O BitcoinTalk também é uma importante ferramenta para que você encontre locais que negociam a criptomoeda em questão, além de endereços para mineração e doações.

5 CARTEIRAS

O primeiro passo para trabalhar com criptomoedas é saber armazená-las. Ao contrário do dinheiro oficial, criptomoedas não são armazenadas em instituições bancárias, mas sim com o próprio usuário.

Este, por sua vez, é responsável por garantir a segurança de suas Bitcoins, pois ninguém mais o fará. Por essa razão, recomendo que você atente-se aos detalhes apresentados neste capítulo.

O local onde as criptomoedas são armazenadas é denominado **wallet**, e consiste de um programa simples – quase sempre todos possuem aparência semelhante – que permite enviar e receber moedas, além de exibir um breve histórico de suas transações.

5.1 TIPOS DE CARTEIRAS

Vale lembrar, também, que uma carteira só funcionará adequadamente se ela estiver de alguma forma conectada com a blockchain, uma vez que isto é necessário para que as transações possam ter valor. É justamente o método de conexão com a blockchain que diferencia os diversos tipos de wallet.

5.1.1 Wallet-core

Quando uma criptomoeda é lançada, o desenvolvedor fornece também uma wallet padrão, também conhecida como **core**. Para que ela possa funcionar, é necessário que toda a blockchain seja baixada para o computador do usuário, em um processo denominado **sincronização**.

Figura 6: funcionamento de uma wallet-core

A wallet dispensa instalação, sendo seu início simultâneo com sua primeira execução.

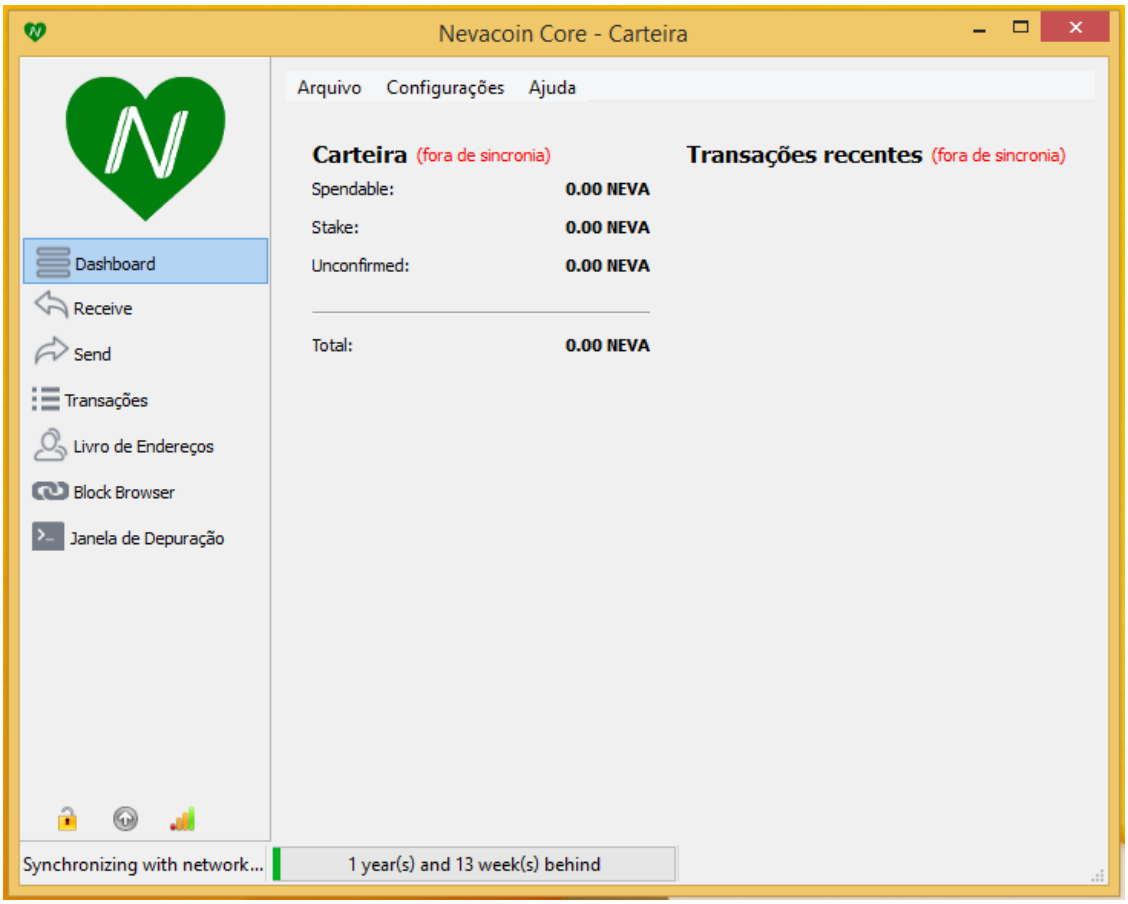
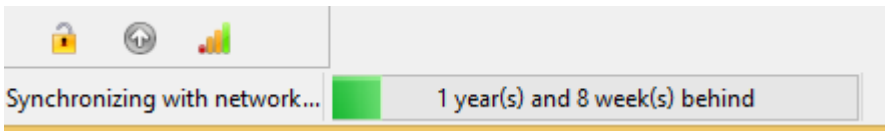


Figura 7: wallet padrão de Nevacoins.

Entretanto, será necessário aguardar o período de sincronização até que você possa utiliza-la. Ele é indicado no canto inferior da tela. Não se assuste se encontrar algo como “2 anos e 4 meses restantes”, pois isso não é uma estimativa de tempo decorrido – apenas o período correspondente ao histórico de transações que precisa ser baixado.



Dependendo da moeda, esse tempo pode variar de algumas horas para dias, já que depende da quantidade de nodes disponíveis para conexão no momento da instalação e da quantidade de transações existentes no histórico.

5.1.2 Wallets leves

Evidentemente, nem todos possuem o espaço em disco necessário para que a plena sincronização ocorra, além do incômodo que aguardar o processo pode representar. Por essa razão, terceiros podem desenvolver wallets que operam com apenas frações da blockchain, não necessitando realizar o download de toda a cadeia.

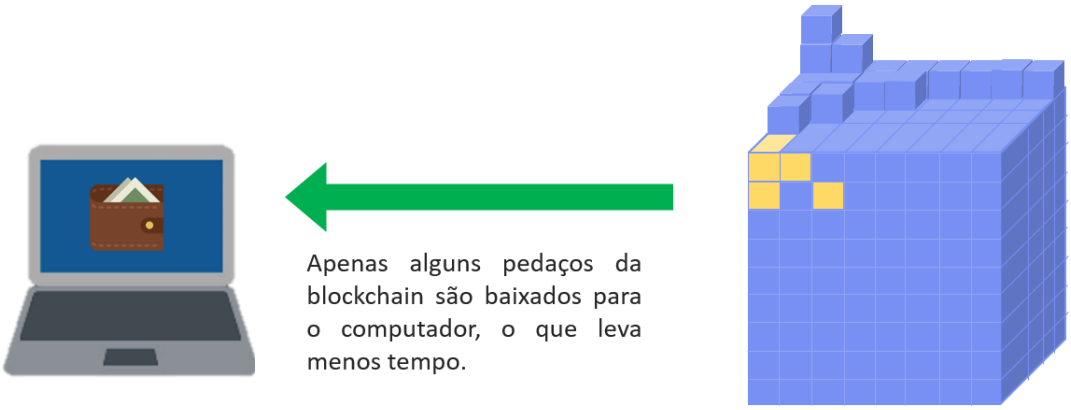


Figura 8: funcionamento de uma wallet leve.

Em uma carteira leve, o usuário ainda deve possuir todo o controle de suas criptomoedas, cabendo única e exclusivamente a ele o dever de garantir a segurança do dinheiro armazenado.

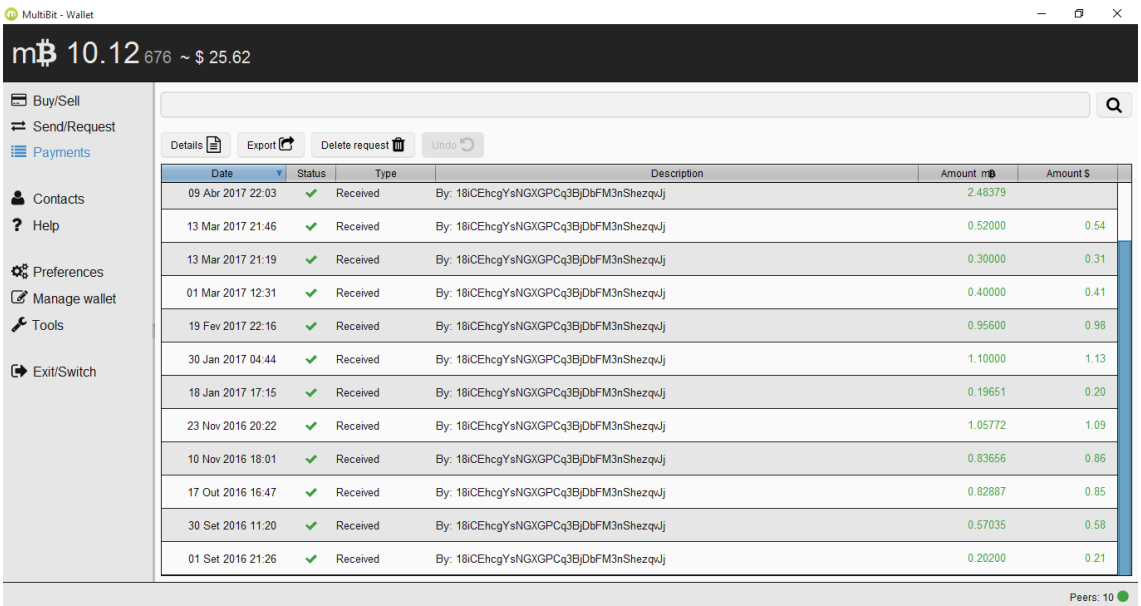


Figura 9: carteira leve de Bitcoins.

Em função destas características, esse tipo de carteira é o de utilização mais comum. Entretanto, não é recomendado para o armazenamento de grandes quantias – apenas para o uso diário, como uma carteira de dinheiro.

Além disso, nem todas as criptomoedas contam com carteiras desse gênero, pois elas quase sempre são programadas por terceiro. Se você pretende trabalhar com alguma moeda menos popular, provavelmente terá de se acostumar com a primeira alternativa.

5.1.3 Wallets online

Aqui, abordamos outro tipo de wallets: aquelas nas quais as criptomoedas são armazenadas nas mãos de terceiros, como em uma conta bancária. Apesar de serem mais rápidas que as convencionais, podem apresentar riscos.

Tais riscos situam-se, principalmente, no fato de que o usuário não detém controle direto sobre seus fundos. Toda a movimentação é feita através de um aplicativo ou de uma interface online.

Figura 10: funcionameno de uma wallet online.

Nessa situação, o provedor do serviço tem totais condições de desativá-lo e tomar para si as moedas de todos os usuários, tornando a escolha de um serviço desse gênero uma questão de fé. Por isso, recomendo utilizar este tipo de wallet apenas para valores ínfimos ou por um tempo curto.

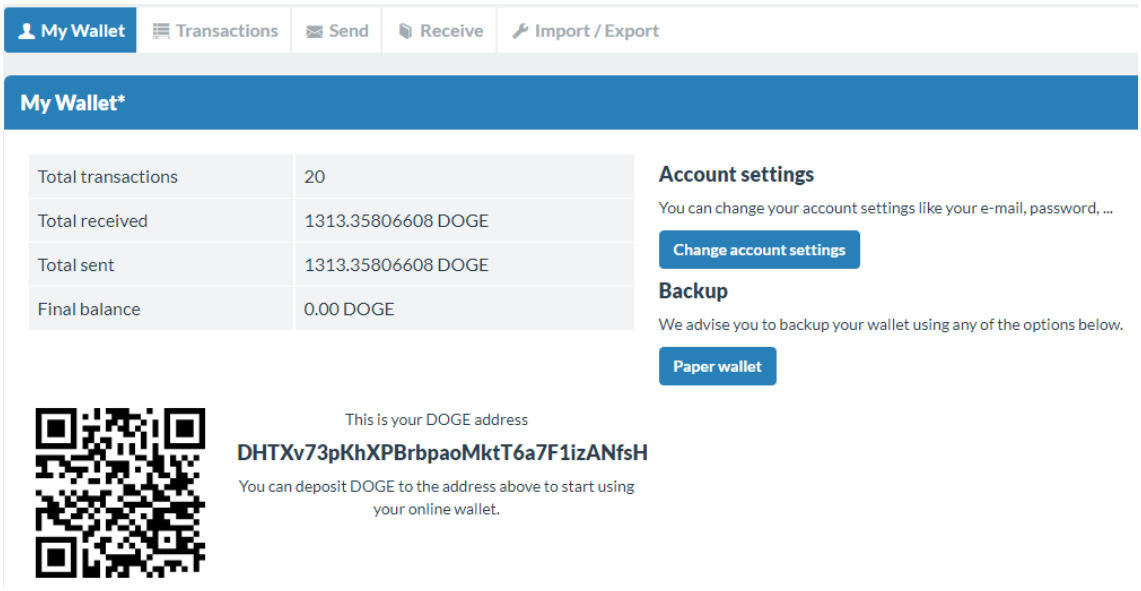


Figura 11: wallet online de Dogecoins.

5.1.4 Wallets de papel

Apesar deste termo causar estranhamento, wallets de papel são a melhor opção para armazenamento de grandes quantias de criptomoedas, ou durante um longo prazo.

Sua lógica de funcionamento é bastante simples: uma chave numérica é gerada, na forma de um código QR, que é impresso e mantido em um local seguro. Essa chave é associada com um node e um endereço para transações na rede de criptomoedas, e servirá para garantir o acesso posterior do usuário ao seu node.

Quando este desejar movimentar seus fundos, basta utilizar uma wallet convencional (qualquer uma das apresentadas acima) e operá-los como faria normalmente.

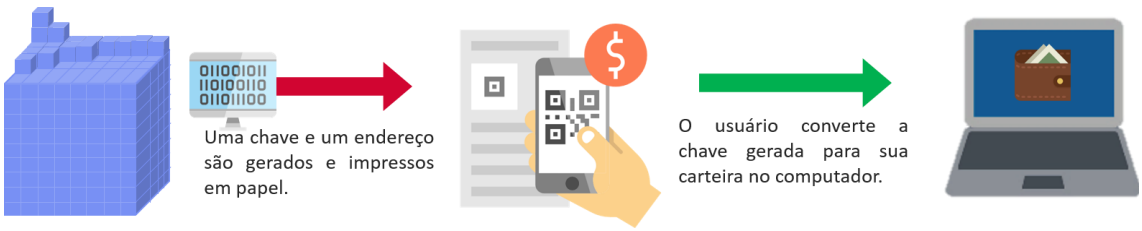


Figura 12: funcionamento de uma wallet de papel

O processo de criação de uma wallet de papel é extremamente simples: existem diversos serviços que permitem gerar uma carteira de papel para praticamente qualquer criptomoeda.

Um deles é o WalletGenerator.net (https://walletgenerator.net), que permite gerar carteiras de papel para mais de 120 criptomoedas diferentes. Para utilizá-lo, basta clicar na moeda em questão.

O programa irá solicitar que você passe o cursor do mouse pela tela arbitrariamente, a fim de coletar o máximo possível de dados aleatórios para geração de sua chave.

Em seguida, ele retornará dois códigos QR: um corresponde a sua chave privada, que deve ser impressa e mantida em um lugar seguro. O outro, corresponde ao endereço de depósito, que pode ser público e será utilizado para transferir fundos para sua wallet de papel.

O serviço ainda recomenda que o processo seja realizado através da versão em código do website – presente no GitHub – com a Internet desconectada e em um sistema operacional livre de spywares. Se você realmente precisa de uma wallet segura, pode ser interessante seguir esses passos.

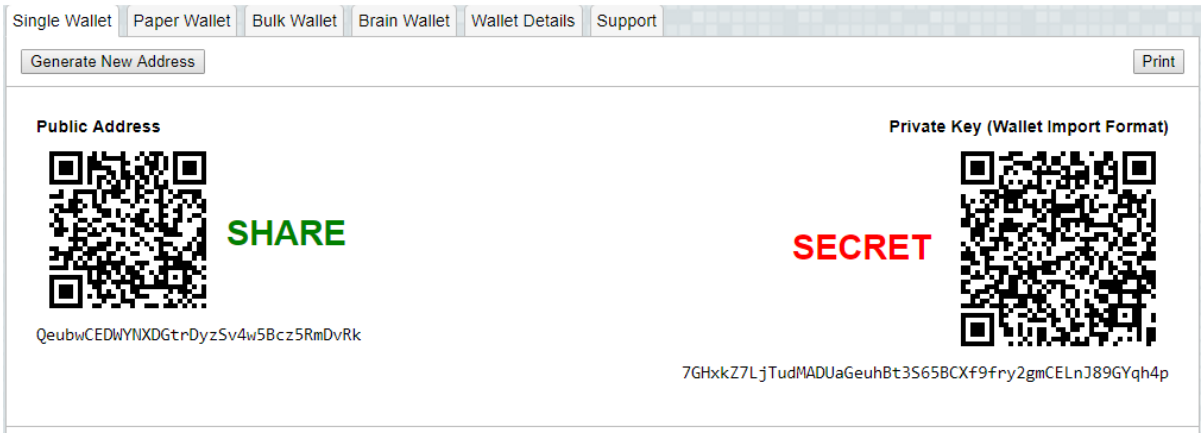


Figura 13: geração de endereços em uma wallet de papel.

Para utilizá-lo, basta imprimir ambos os códigos e guardar o código secreto em segurança. Mais adiante, explicaremos como recuperar uma carteira através de uma chave privada.

Se preferir, existem ainda serviços que geram e imprimem uma wallet personalizada, além de outros que vendem wallets mais duráveis e a prova d'água.

Figura 14: wallet de papel de Nevacoins impressa.

5.2 MANUSEANDO UMA CARTEIRA

Uma vez que você tenha escolhido sua carteira, é o momento de aprender a utilizá-la. As informações abaixo devem ser aplicáveis em quase todas as wallets core, e na maioria das wallets leves ou online. No entanto, podem haver pequenas diferenças dependendo do programa utilizado.

5.2.1 Operações básicas

A maioria das carteiras possui um menu lateral, que permite realizar as operações básicas com a criptomoeda em questão. Na primeira opção, denominada Dashboard, pode-se ver o total de moedas existentes na carteira, além de um registro das transações ocorridas recentemente. Normalmente, é também exibido um ícone especial para transação de débito, crédito ou transação ainda não confirmada pela rede.

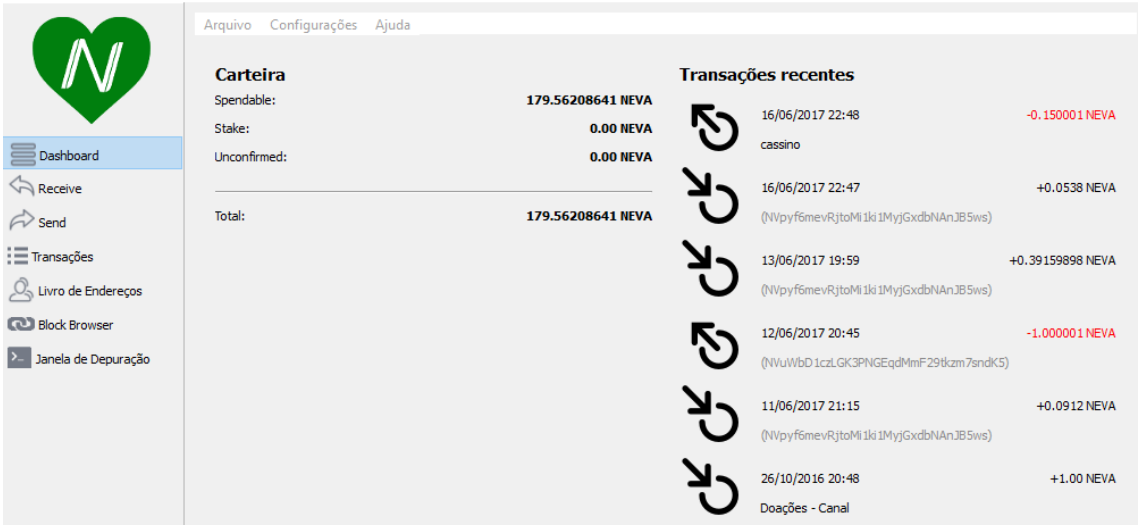


Figura 15: aba Dashboard de uma carteira de criptomoedas.

A seguir, na aba denominada Receive, permite – como o nome indica – receber criptomoedas. Isso é feito através da geração de um endereço, que pode ser convertido também em QR code e possibilita que outro usuário envia moedas para você. Além disso, pode-se gerar quantos endereços desejar, todos indicando para a mesma carteira.

A função acima citada poder ser útil caso você receba muitas transações de pessoas diferentes e queria manter um controle a respeito de quem te envia o quê.

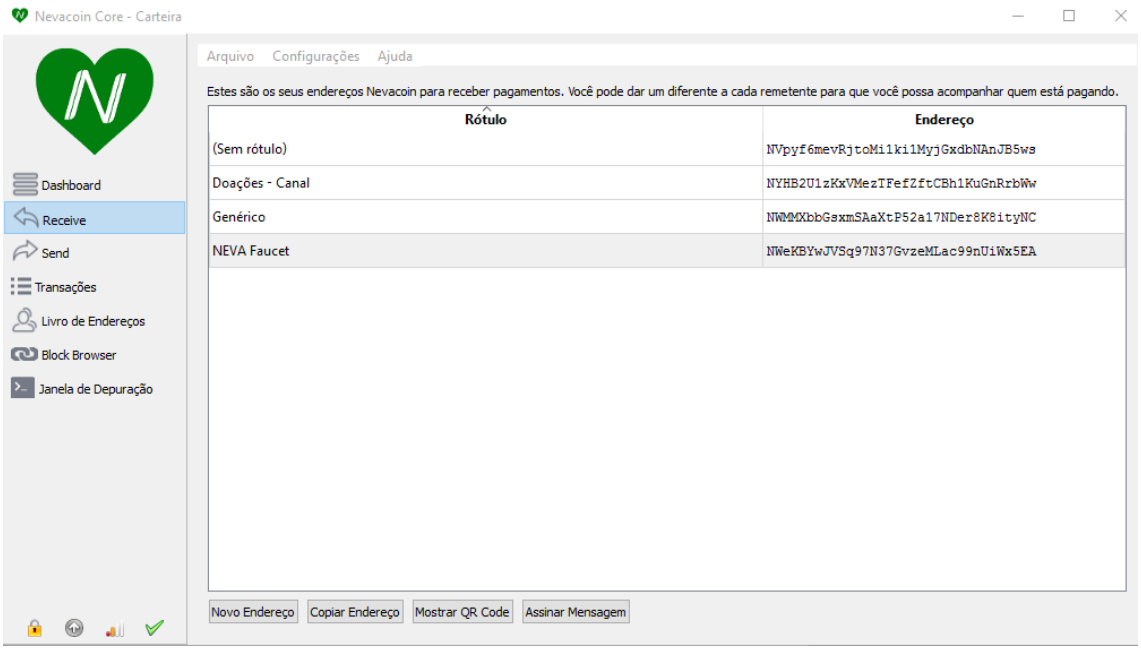


Figura 16: aba Receive de uma carteira de criptomoedas.

Existe também a aba Send, que permite ao usuário enviar moedas para qualquer endereço dentro da rede. Aqui, você pode inserir o endereço de

pagamento, adicionar uma etiqueta caso queira salvar o endereço em questão e determinar a quantidade de moedas a serem enviadas.

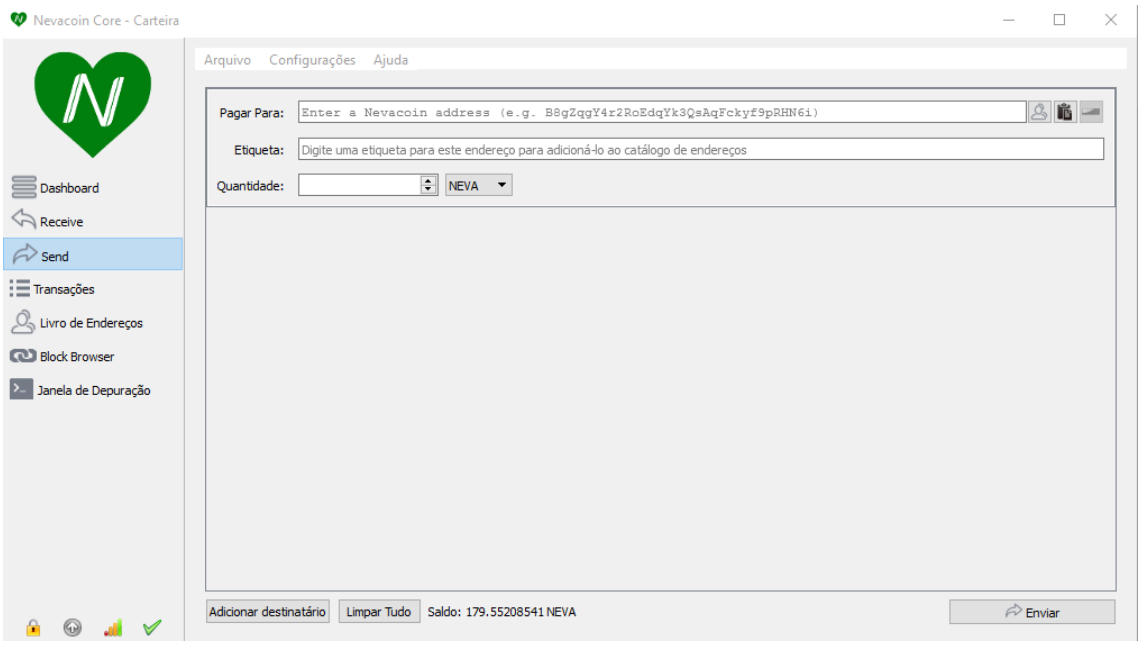


Figura 17: aba Send de uma carteira de criptomoedas.

Também é possível que você se depare com as seguintes notações, que identificam unidades menores ou maiores que a unidade padrão do sistema – ou seja, que 1 unidade da moeda. Neste caso, fique atento ao valor solicitado pela transação e ao valor que você irá inserir.

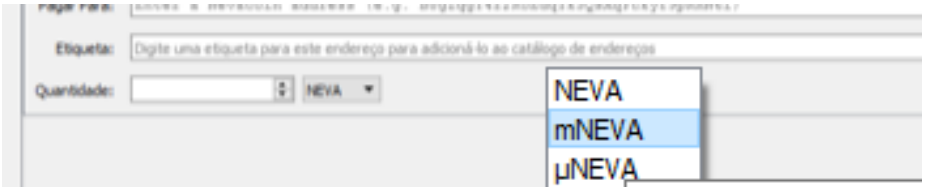


Figura 18: múltiplos de uma mesma unidade de criptomoeda.

Para tanto, siga a tabela abaixo, na qual estão explicitados os múltiplos e submúltiplos, de acordo com o Sistema Internacional.

yotta	Y	10^{24}	1 000 000 000 000 000 000 000 000
zetta	Z	10^{21}	1 000 000 000 000 000 000 000
exa	E	10^{18}	1 000 000 000 000 000 000
peta	P	10^{15}	1 000 000 000 000 000
tera	T	10^{12}	1 000 000 000 000
giga	G	10^{9}	1 000 000 000
mega	M	10^{6}	1 000 000
kilo	k	10^{3}	1 000
hecto	h	10^{2}	100
deca	da	10^{1}	10
-	-	10^{0}	1
deci	d	10^{-1}	0,1
centi	c	10^{-2}	0,01
mili	m	10^{-3}	0,001
micro	μ	10^{-6}	0,000 001
nano	n	10^{-9}	0,000 000 001
pico	p	10^{-12}	0,000 000 000 001
femto	f	10^{-15}	0,000 000 000 000 001
atto	a	10^{-18}	0,000 000 000 000 000 001
zepto	z	10^{-21}	0,000 000 000 000 000 000 001
yokto	y	10^{-24}	0,000 000 000 000 000 000 000 001

Figura 19: potências de 10 e suas denominações.

Há também a aba Transactions, na qual você pode obter o registro de todas as transações que já foram realizadas envolvendo a sua carteira. Note também que as transações, após realizadas, demoram alguns minutos para serem confirmadas e, no caso das de crédito, para você poder efetivamente utilizar o valor recebido.

Isso acontece por que, ao se tratar de uma rede descentralizada, é necessário que outros nodes da rede vejam a transação ocorrida e verifiquem se ela é válida ou não.

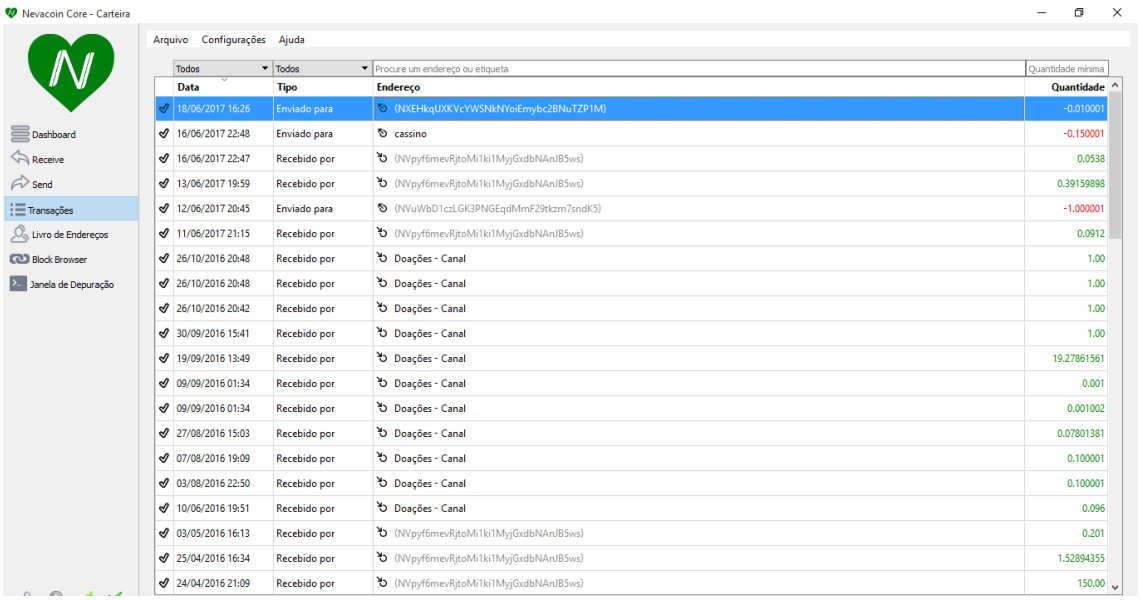


Figura 20: histórico de transações.

Clicando em uma transação específica, você pode visualizar informações como o número de identificação, o valor e a quantidade de confirmações que ela já possuiu dentro da rede.

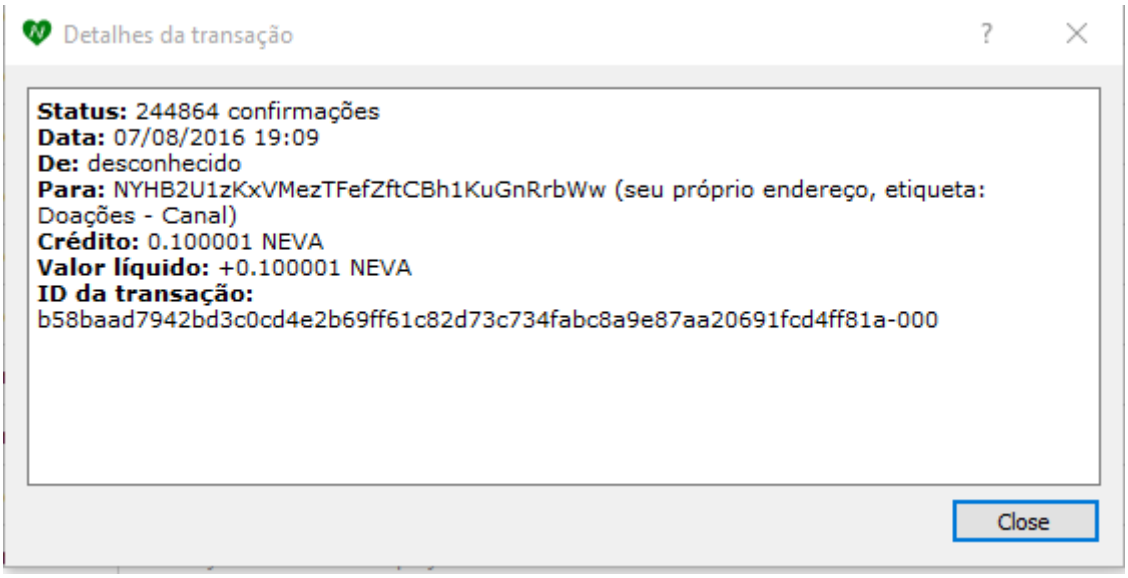


Figura 21: detalhes de uma transação.

Na aba Adress Book, é possível adicionar endereços com os quais você realiza transações com frequência.

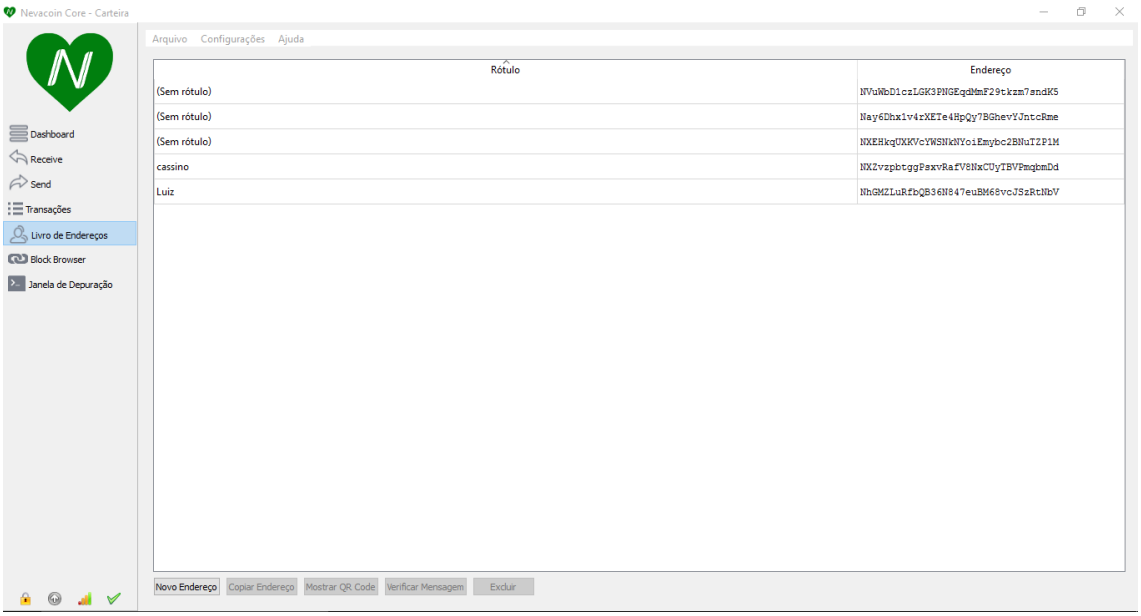


Figura 22: livro de endereços.

Além disso, toda wallet possui um explorador de blocos, que permite que você visualize dados a respeito de cada bloco já emitido pelo sistema (dificuldade, hashrate na qual foi minerado, recompensa, entre outros). Também é possível visualizar detalhes de uma transação qualquer, adicionando seu ID.

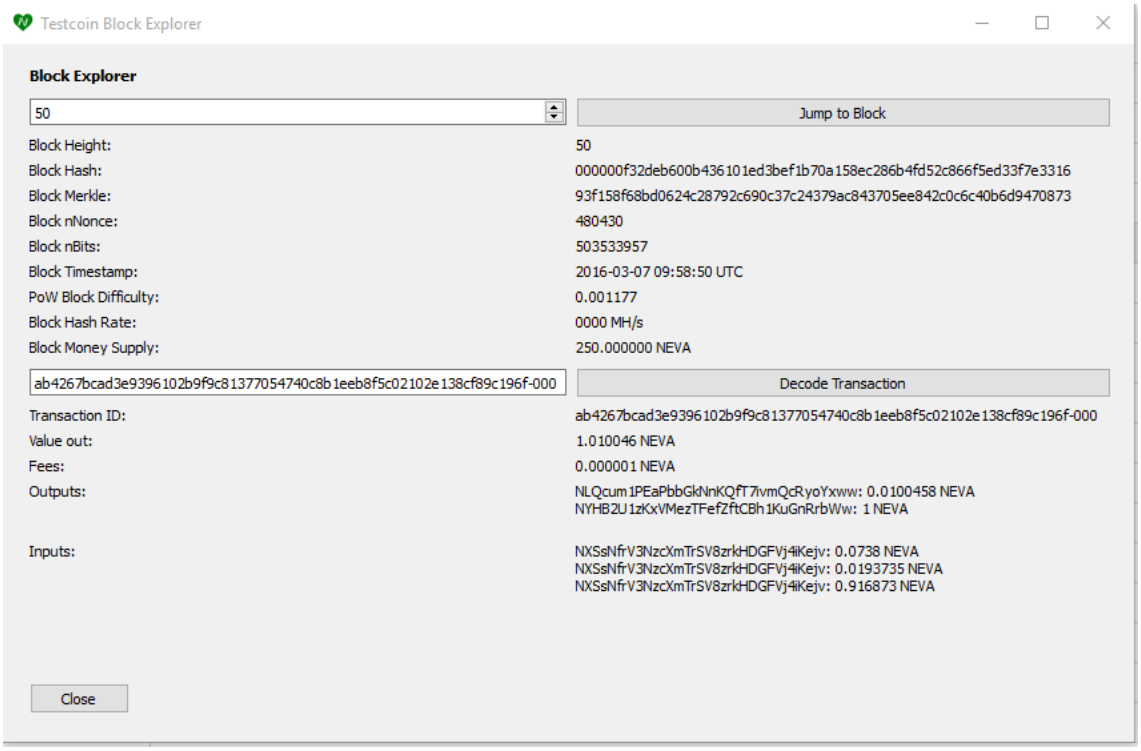


Figura 23: explorador de blocos.

Por fim, existe uma janela de depuração, que exibe informações a respeito do software em questão, além de uma linha de comando (a qual estudaremos adiante) e dados sobre as taxas de download e upload do sistema.

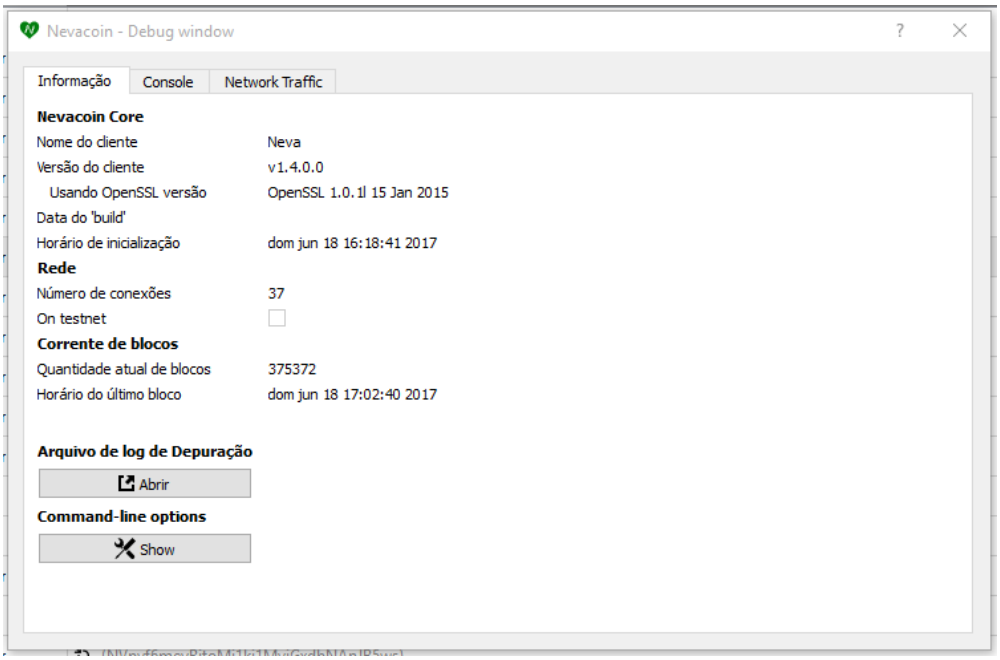


Figura 24: janela de depuração.

5.2.2 Encriptando sua wallet

Como já mencionado anteriormente, você é o responsável pela segurança de suas moedas. Caso utilize sua carteira sem nenhuma configuração adicional, ela poderá ser facilmente roubada por um atacante que consiga acesso a ela.

Sendo assim, é possível colocar uma senha na carteira através da aba *Configurações*, selecionando em *Criptografar Carteira*.

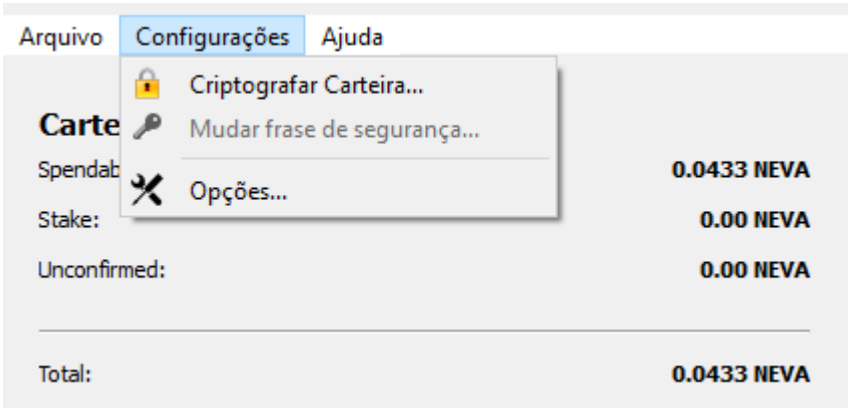


Figura 25: criptografando carteira.

Em seguida, defina uma senha para a carteira. É interessante que você utilize uma senha forte, pois será ela que definirá o aceso à sua wallet. Caso um atacante roube uma carteira protegida, na maioria das vezes ele conseguirá apenas visualizar seu saldo.

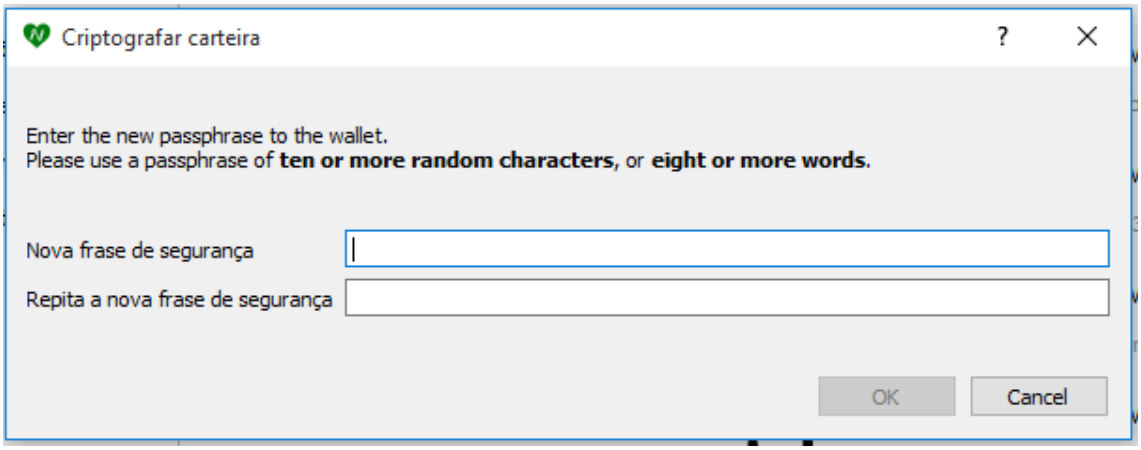


Figura 26: processo de criptografia da wallet.

Após a definição da senha, a seguinte mensagem será exibida. Em seguida, abra novamente a carteira para poder utilizá-la.

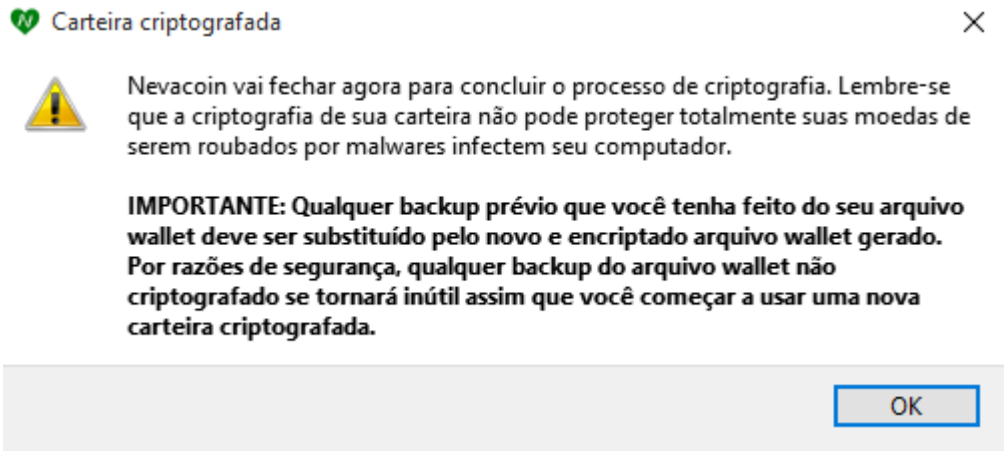


Figura 27: mensagem pré processo de criptografia.

Deste momento em diante, qualquer transação que você realize utilizando a carteira irá solicitar uma chave de segurança.

Vale lembrar também que outras wallets, em especial as wallets leves, podem apresentar formas diferentes de manter sua carteira segura. Por exemplo, o sistema pode solicitar que você insira uma senha toda vez que acesse a carteira.

5.2.3 Exportando um backup

Suponha que você decida trocar de computador, formata-lo, ou mesmo migrar de sistema operacional. Evidentemente, esse processo deverá ser feito de forma a manter o backup de suas moedas e evitando, portanto, que elas se percam.

Carteiras de terceiros costumam possuir outros métodos para recuperação de backups, tais como chaves geradas por uma sequência de palavras. Por essa razão, mostraremos apenas o processo para wallets comuns.

Na guia Arquivo, de sua carteira, selecione a opção Backup Carteira.

Figura 28: proceso de realização do backup.

Lhe será solicitado que escolha um diretório do computador, no qual um arquivo de extensão .dat será salvo. Ele é o arquivo de backup da carteira, e deverá ser mantido em local seguro.

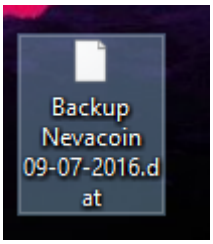


Figura 29: arquivo de backup.

Ao contrário do que é de se imaginar, não é necessário realizar backups regulares de suas carteiras, já que função do backup é apenas guardar a chave secreta da carteira. Entretanto, certifique-se de mantê-los em um ou mais locais acessíveis.

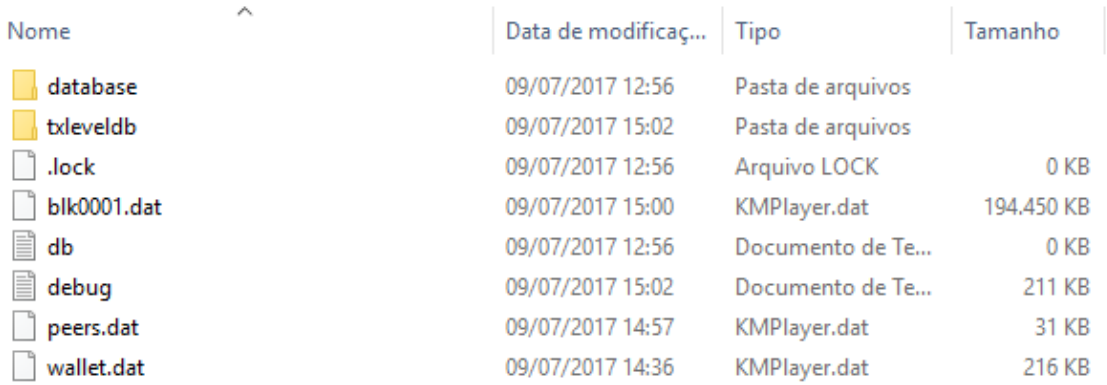
5.2.4 Restaurando um backup

Suponha, agora, que você formatou seu computador e perdeu todos os dados da carteira, mas manteve alguns backups em um disco externo. É, então, o momento de restaurá-los para voltar a utilizar suas moedas normalmente.

Após reinstar a wallet e aguardar sua sincronização, será preciso adicionar manualmente o arquivo de backup à pasta da wallet, já que a maioria destas não contam com uma opção mais intuitiva aos usuários.

Para isso, pesquise, na barra de busca do Windows: %appdata%. Da mesma forma que você já deve ter visto em um tutorial de Minecraft.

Na pasta C:\Users\Natanael\AppData\Roaming, procure a pasta da wallet cujo backup deve ser restaurado. Normalmente, ela é identificada pelo nome da moeda. Ao encontra-la, acesse-a. Você verá os seguintes arquivos:



Nome	Data de modificaç...	Tipo	Tamanho
database	09/07/2017 12:56	Pasta de arquivos	
txleveldb	09/07/2017 15:02	Pasta de arquivos	
.lock	09/07/2017 12:56	Arquivo LOCK	0 KB
blk0001.dat	09/07/2017 15:00	KMPlayer.dat	194.450 KB
db	09/07/2017 12:56	Documento de Te...	0 KB
debug	09/07/2017 15:02	Documento de Te...	211 KB
peers.dat	09/07/2017 14:57	KMPlayer.dat	31 KB
wallet.dat	09/07/2017 14:36	KMPlayer.dat	216 KB

Delete o arquivo *wallet.dat*. Mas atenção: fazer isso removerá a wallet original, fato que você não precisará se preocupar caso estiver lidando com uma wallet recém-instalada.

Entretanto, se julgar necessário, copie o arquivo para um lugar seguro antes de deletá-lo. Em seguida, renomeie o nome do arquivo de backup para *wallet.dat*, e coloque-o nesta pasta.

Reinicie a carteira, e você deverá ter acesso à conta presente no backup. Entretanto, caso esta esteja encriptada, você ficará restrito a visualizar o saldo e o histórico de transações, não podendo movimentar as moedas. Isso só será possível após inserir a senha, definida anteriormente.

5.3 COMO MANTER SUA CARTEIRA SEGURA?

Algumas dicas de segurança básicas são suficientes para evitar que a segurança de suas moedas seja comprometida. Em suma, deve-se encontrar medidas que impeçam potenciais atacantes de terem acesso aos arquivos da sua carteira e, principalmente, às suas senhas.

A primeira delas, e mais evidente, é a definição de uma senha forte o bastante em todas as suas carteiras. Sempre utilize senhas extensas, compostas por

números, letras maiúsculas e minúsculas e caracteres especiais, pois isso dificulta ataques de força bruta.

Se encontrar dificuldades na memorização destas senhas, utilize um software de gerenciamento de senhas de código aberto, como o KeePass (http://keepass.info).

Além disso, deve-se ter cuidado redobrado com o armazenamento dos backups. Não os deixe em dispositivos externos que podem ser facilmente perdidos ou acessados por terceiros. Preferencialmente, mantenha-os em pastas criptografadas e discretas.

Evite, também, utilizar wallets online ou de terceiros para o armazenamento de grandes quantias. Sempre dê preferência para aquelas de código aberto, e nunca abra mão de uma wallet de papel quando necessário.

Existem ainda as medidas que todo usuário deveria tomar, independente de possuir criptomoedas, já que são de importância vital para a proteção de suas informações pessoais. Você pode aprender estas técnicas de navegação segura em https://youtu.be/8zVsR495F-M.

6 SUAS PRIMEIRAS MOEDAS

Neste ponto, você já sabe como as criptomoedas funcionam. Já sabe, também, como configurar e manusear corretamente uma carteira. Chegou o momento de obter suas primeiras moedas, passo importante para que você, utilizando pequenas quantias aprenda quais as melhores formas de manuseá-las.

Muitos usuários tendem a achar que a melhor forma de obter criptomoedas é através da mineração. No entanto, existem meios mais fáceis de conseguir seus primeiros valores sem a necessidade de se adentrar em um campo tão complexo.

6.1 FAUCETS

Faucet, do inglês, significa “torneira”. Em criptomoedas, eles possuem um funcionamento análogo: “gotejam” quantias ínfimas de criptomoedas, normalmente equivalentes a frações de centavo, para usuários iniciantes.

Neste momento, você provavelmente pensou: o que me impede de enriquecer utilizando faucets? Dois fatores. Primeiro, a quantia que eles fornecem é mínima, e seria necessário um número absurdo de sessões para se obter algum valor significativo. Segundo, todos os faucets possuem recursos que impedem um mesmo usuário de sacar repetidas vezes seguidas, sendo normalmente imposto um intervalo de algumas horas entre cada saque.

Entretanto, faucets podem ser uma boa alternativa para obter suas primeiras criptomoedas e realizar alguns testes e até mesmo testar a confiabilidade daquele serviço que promete armazenar suas moedas.

Um faucet pode funcionar de diversas formas. Aqui, citarei algumas delas, e indicarei quais são as mais funcionais, aquelas que, nem tanto, e quais são absolutamente improdutivas – ou sequer funcionam.

O primeiro e melhor tipo – e infelizmente, o mais raro também – é aquele que cumpre sumariamente sua função: a de fornecer moedas. Normalmente, são criados pelo próprio desenvolvedor da criptomoeda como forma de incentivar os usuários a utilizá-la.

Um exemplo é o faucet de Nevacoins (https://nevacoin.net/faucet), que entrega ao usuário uma quantia entre 0.01 e 0.1 NEVA. É um valor ínfimo, mas interessante.

Neste faucet, o funcionamento é simples: basta inserir o endereço de recebimento, verificar que você não é um robô e aguardar o pedido.

Figura 30: faucet de Nevacoins.

Em alguns projetos menores, principalmente naqueles em que o programador não é capaz de projetar um sistema um pouco mais eficiente, e recorrer para métodos manuais.

Nestes, como no faucet de Quarkcoins (http://www.quarkcoins.com/free-quarkcoins.html), as moedas só são entregues sob alguma condição, como compartilhar o projeto como público em alguma rede social. Além disso, é preciso informar, nos comentários, o que você fez para merecê-las.

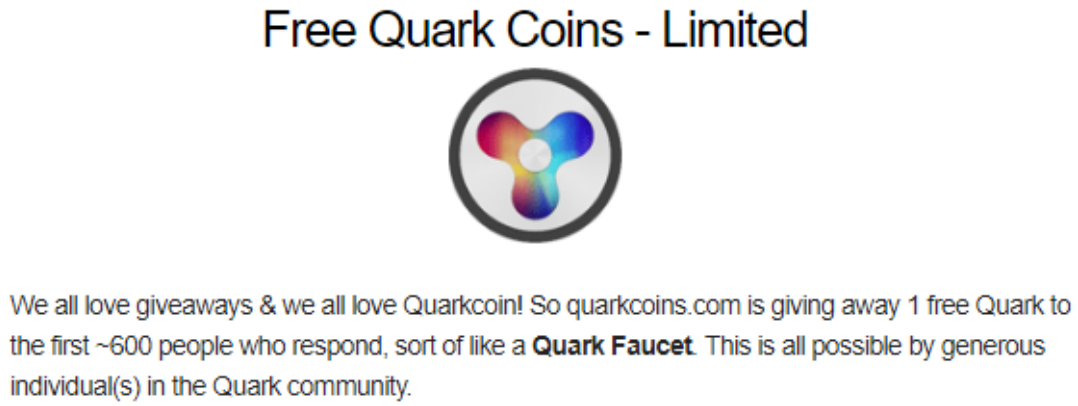


Figura 31: faucet de Quark Coins

Existem, ainda, alguns faucets que possuem um limite mínimo para saque, a fim de garantir que você realize um mínimo de cliques no site e, por consequência, gere receita para seus criadores através de anúncios. Outros, ainda, fazem isso através de um endereço temporário e terceirizado, ou através de pagamentos semanais.

Estes são o caso da maioria dos faucets das principais criptomoedas, tais como Bitcoins, Litecoins ou Dogecoins, e todos eles possuem fins lucrativos, já que ganham através dos anúncios, ao contrário dos anteriores, que operavam através de doações.

Por fim, existem os faucets falsos. Estes tem a aparência de um faucet real, e inclusive exibem um saldo de criptomoedas que aumenta descomunalmente rápido, instigando o usuário a continuar obtendo-as.

Entretanto, no momento do saque, é solicitado que o usuário realize algum tipo de ação para obter suas moedas, tais como clicar em uma propaganda, contratar um serviço de SMS ou se cadastrar – as vezes com seu cartão de crédito – em algum site duvidoso.

Na maioria das vezes, esses faucets, além de tomar seu tempo e dinheiro, não funcionam. Procure ficar longe deles.

Pronto para um pouco de conhecimento proibido? Uma quantidade considerável de faucets apresentam métodos de autenticação, tais como endereço de IP ou endereço da carteira que podem ser facilmente burlados através de ferramentas como o Tor (https://www.torproject.org/projects/torbrowser.html.en) ou do simples uso de múltiplos endereços. Se você tiver força de vontade suficiente, pode conseguir drenar um faucet em algumas horas através dessa ferramenta. Não necessariamente será lucrativo, mas é possível.

6.2 COMPRANDO CRIPTOMOEDAS

Se você procurou se aprofundar neste mundo com o único e exclusivo objetivo de realizar uma transação em alguma criptomoeda, ou precisa de uma quantia mais volumosa, pode comprar criptomoedas em casas de câmbio especializadas.

Infelizmente, a maioria dessas casas cambiam apenas nas principais moedas, cabendo ao usuário que deseja outra mais específica a negociação em lugares específicos, que serão estudados mais adiante.

No Brasil, pode-se comprar e vender Bitcoins e Litcoins através do Mercado Bitcoin (https://www.mercadobitcoin.com.br), serviço já conceituado pela mídia por sua credibilidade.

Para tanto, o primeiro passo será realizar o depósito (em reais) no serviço, para depois convertê-los em Bitcoins, as quais podem, então, ser transferidas para uma carteira. Isso é feito através de depósito bancário, a ser realizado em uma agência do Banco do Brasil, Santander ou Caixa Econômica Federal em um caixa automático ou no caixa da agência.

Ao criar uma conta no Mercado Bitcoin, alguns dados, como CPF e nome completo serão solicitados. Caso queria aumentar seu limite de depósito diário, pode optar por enviar foto de documento original com foto.

Após a criação da conta, você verá, no canto esquerdo, um menu semelhante a esse, no qual existem todas as possibilidades de negociações.

Figura 32: menu do Mercado Bitcoin.

Para comprar, selecione a criptomoeda desejada e clique em *Depósito*. Ali, você deverá informar o método de pagamento, o banco no qual deseja pagar e o valor requisitado, cujo mínimo é de 50 reais. Além disso, há uma tarifa obrigatória que fica retida no Mercado Bitcoin.

Figura 33: aviso de depósito no Mercado Bitcoin

Após enviar o aviso de depósito, você receberá, em seu e-mail, detalhes a respeito de como a transação deve ser realizada. Resumidamente, você deverá efetuar o depósito no valor escolhido para a razão social apresentada.

Quando tiver com o comprovante em mãos, deverá escrever, nele, seu número de CPF e a frase “Depósito para comprar Bitcoin”, tirar uma fotografia dele (ou digitaliza-lo) e enviar, como anexo, na guia de depósitos presente no site.

Vale lembrar que nenhum aviso de depósito é obrigatório, e pode ser cancelado a qualquer momento.

Uma vez que a compra foi realizada, seu saldo em reais será depositado na sua conta no site. Para comprar Bitcoins, clique em *Comprar*, na aba da criptomoeda. Selecione o valor desejado e proceda com a compra;

Figura 34: convertendo reais em Bitcoins.

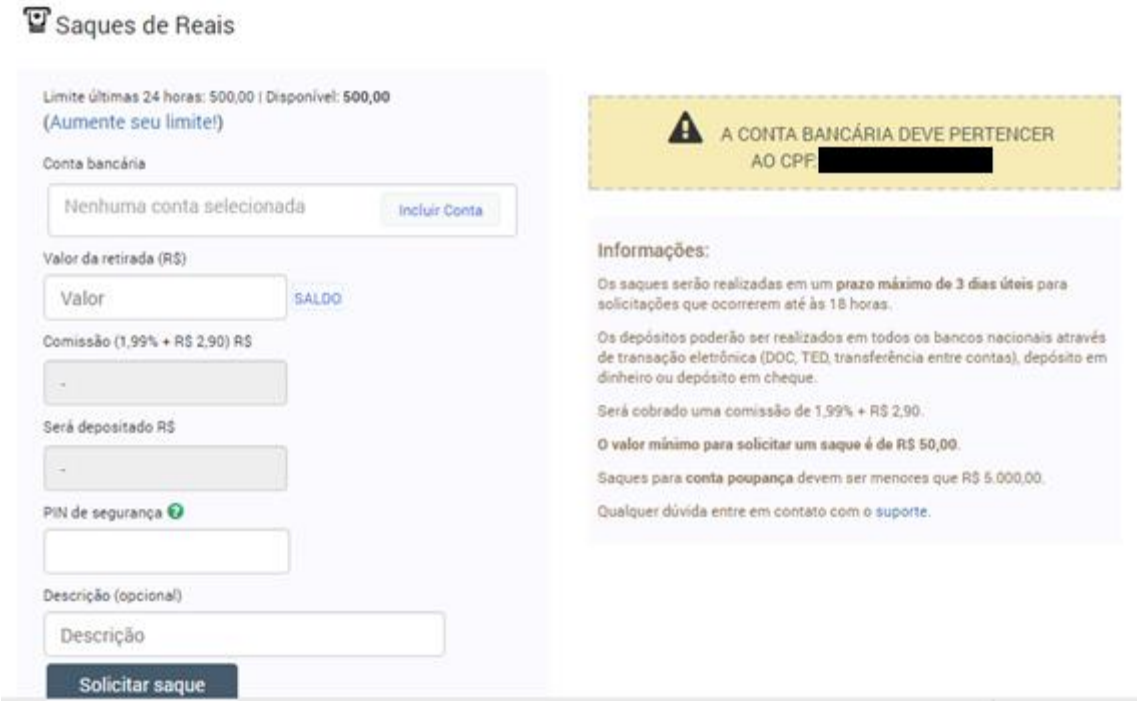
Em seguida, você pode transferir suas Bitcoins para sua carteira através da opção *Transferir Bitcoins*, disponível no mesmo menu.

Figura 35: transferindo Bitcoins para seu endereço.

Caso você deseje receber Bitcoins diretamente em sua conta do Mercado Bitcoin, pode fazê-lo através da opção *Receber Bitcoins*, que gera um código QR contendo um endereço para depósito.

É ainda possível converter Bitcoins em reais através de um menu semelhante, na opção *Vender*. Esse é o único passo de proceder para o saque de dinheiro.

Por fim, o saque é possível apenas através de depósito bancário, necessitando de uma conta corrente em uma instituição financeira qualquer. Obrigatoriamente, a conta bancária deverá pertencer ao CPF do comprador,



7 MINERAÇÃO

7.1 TIPOS DE MINERAÇÃO

Sendo um minerador, você – ou melhor, o seu computador – será responsável por realizar os cálculos necessários para adivinhar a hash do bloco atual. Logo, é evidente que uma considerável capacidade de processamento será necessária na empreitada.

Seu computador possui, basicamente, duas fontes de processamento: seu processador, também denominado CPU, e sua placa de vídeo, também denominada GPU. Ambos podem ser utilizados para mineração, mas o uso de GPU costuma ser mais comum, já que esta costuma ser pouco requerida em atividades que não envolvem jogos, vídeos ou modelagem 3D – ficando disponível para uso na mineração.

Figura 36: processador, placa de vídeo e hardware próprio para mineração.

Existem também hardwares vendidos especificamente para serem utilizados na mineração. Eles combinam, de forma eficiente, alta durabilidade, grande capacidade de procedimento e reduzido consumo de energia, mas são caros e não devem ser adquiridos sem planejamento prévio.

Figura 37: centro de mineração de Bitcoins.

Além disso, para cada um desses equipamentos, existem duas principais formas de minerar: sozinho ou em grupo.

Na mineração solo, cada usuário deve, por si só, tentar resolver os blocos que são enviados para toda a rede, devendo competir com todos os demais usuários, incluindo aqueles que estão trabalhando em grupo. Caso tenha sucesso, o minerador receberá a recompensa de forma integral, mas em caso contrário, nada receberá.

Por essa razão, a mineração solo torna-se inviável, dado que uma única máquina dificilmente será capaz de competir em poder de mineração com o resto da rede.

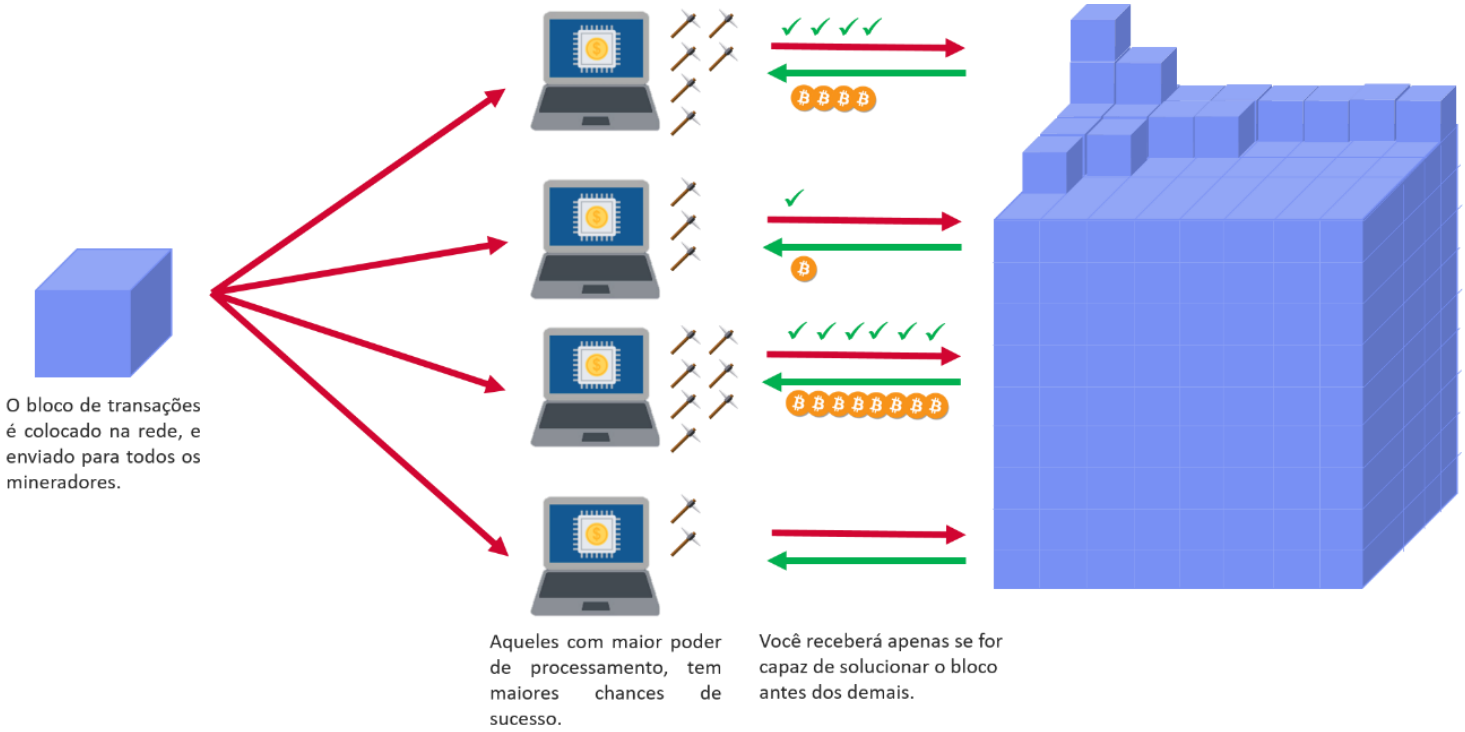


Figura 38: mineração solo.

Já na mineração em grupo, também chamada de pool, vários usuários combinam seus respectivos poderes de mineração em um objetivo comum. No caso, encontrar a hash do bloco em questão.

Se vários usuários participam da tarefa e compartilham as informações obtidas entre eles, isso faz com que a eficiência de trabalho seja aumentada e existam mais chances de se obter sucesso na procura da hash.

Em caso de sucesso, a recompensa integral será destinada para a pool, que é então responsável por dividi-la entre os mineradores de forma proporcional ao poder de mineração que cada um compartilhou. Considerando que, caso cada

minerador trabalhasse de forma individual os ganhos seriam mais altos, mas esporádicos e não compensariam os gastos com energia, a mineração em grupo torna-se uma excelente alternativa, em especial para moedas com maior dificuldade.

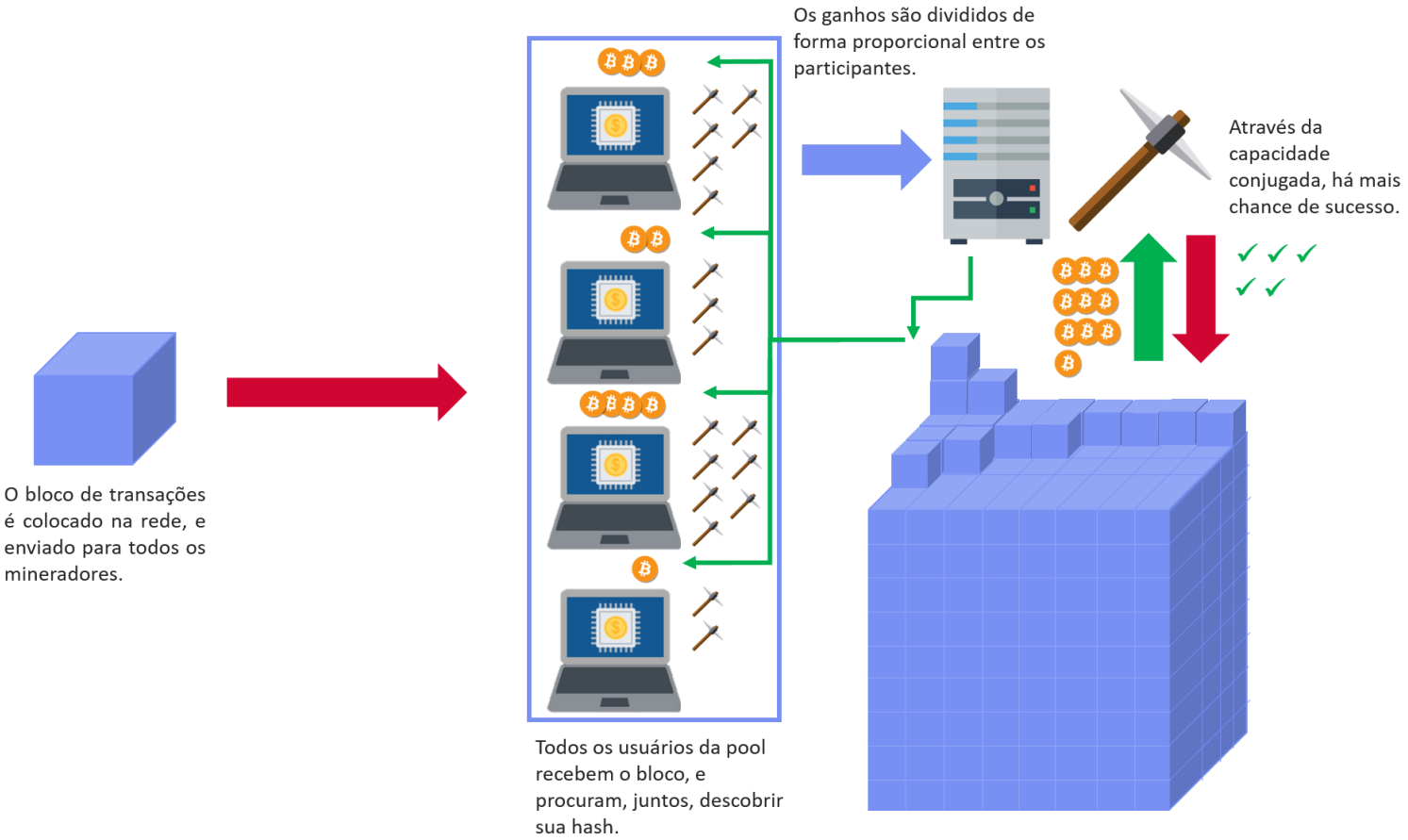


Figura 39: mineração em grupo, também chamada de pool.

Existem, ainda, alguns serviços que permitem que você, dentro da pool, compre ou venda capacidade de mineração para outros usuários. Para o minerador, isso pode potencializar seus ganhos e, para quem vende o poder de mineração, pode ser compensador.

7.2 MINERADORES

Independentemente do tipo de mineração que desejarmos realizar, será preciso um software específico para a tarefa, denominado minerador. Existem mineradores específicos para mineração em CPU e em GPU e, neste último caso, eles ainda podem variar conforme a marca da placa de vídeo especificada.

Eles ainda variam conforme o algoritmo da moeda em questão. Normalmente, um minerador é programado de forma a ser capaz de operar com

determinados algoritmos, não sendo funcional para algoritmos excluídos de sua lista.

Neste material, citarei os principais mineradores tanto para CPU quando para GPU, e mostrarei exemplos práticos para dois deles, compatíveis com o meu hardware (um processador Intel e uma placa gráfica NVIDIA). Entretanto, o funcionamento destes é semelhante e facilmente intuitivo para quem já é familiarizado com sua terminologia.

Para mineração através da CPU, indico o cpuminer (https://sourceforge.net/projects/cpuminer/).

Já para mineração através da GPU, recomendo, para placas de vídeo da NVIDIA, o ccminer (http://ccminer.org). O programa funciona para uma vasta gama de algoritmos e é, provavelmente, tudo que você precisa para mineração.

Existem, ainda, mineradores produzidos objetivando um algoritmo em específico. Você também pode usá-los, se achar necessário.

Para dar prosseguimento ao curso, faça download de ambos os mineradores e extrai-os para uma pasta de sua preferência. Nas próximas páginas, lhe mostrarei como colocá-los em funcionamento. Mas antes, é interessante aprender alguns conceitos para utilizar os programas.

Você pode obter a lista de algoritmos de operação de um minerador através do arquivo *readme.txt* – ou de nome semelhante. Lá, além de encontrar todas as especificações técnicas do software, você verá se ele é ou não apto para minerar a moeda que deseja.

```
This code is based on the pooler cpuminer and inherits
its command line interface and options.

  -a, --algo=ALGO       specify the algorithm to use
                          bastion     use to mine Joincoin
                          bitcore     use to mine Bitcore's Timetravel10
                          blake       use to mine Saffroncoin (Blake256)
                          blakecoin   use to mine Old Blake 256
                          blake2s     use to mine Nevacoin (Blake2-S 256)
                          bmw         use to mine Midnight
                          cryptolight use to mine AEON cryptonight (MEM/2)
                          cryptonight use to mine XMR cryptonight
                          c11/flax    use to mine Chaincoin and Flax
                          decred      use to mine Decred 180 bytes Blake256-14
                          deep        use to mine Deepcoin
                          dmd-gr      use to mine Diamond-Groestl
                          fresh       use to mine Freshcoin
                          fugue256    use to mine Fuguecoin
```

Figura 40: especificações do minerador.

Caso queira obter ajuda geral a respeito do minerador, inicie uma janela de comando (MS-DOS ou terminal Unix – ou a janela do PowerShell que, por alguma razão, o Windows 10 insiste em substituí-la) em seu diretório e utilize, juntamente com o nome do arquivo executável do minerador, a sintaxe *-h*.

```
PS E:\Hacking\Criptomoedas\Mineradores\ccminer-2.0-release-x64-cuda-8.0> .\ccminer-x64.exe -h
*** ccminer 2.0 for nVidia GPUs by tpruvot@github ***
    Built with VC++ 2013 and nVidia CUDA SDK 8.0 64-bits

  Originally based on Christian Buchner and Christian H. project
  Include some algos from alexis78, djm34, sp, tsiv and klausT.

BTC donation address: 1AJdfCpLWPNoAMDfHF1wD5y8VgKSSTHxPo (tpruvot)

Usage: ccminer [OPTIONS]
Options:
  -a, --algo=ALGO       specify the hash algorithm to use
                        bastion     Hefty bastion
                        bitcore     Timetravel-10
                        blake       Blake 256 (SFR)
                        blake2s     Blake2-S 256 (NEVA)
```

Figura 41: comando de ajuda para o ccminer.

7.3 MINERAÇÃO EM POOL

Finalmente, eis o momento de botar a mão na massa. Mostrarei, neste tópico, os procedimentos para mineração em grupo. Em função da mineração solo ser inviável para a maioria das moedas e de complexidade que foge do caráter desse material, não iremos abordá-la em detalhes.

Para que você possa realizar a mineração em pool é necessário – obviamente – uma pool. Recomendo, tratando de iniciantes, começar minerando uma moeda de baixa dificuldade, pois essa lhe trará rápidos resultados.

A pool que utilizaremos para nossos estudos é a Aikapool (https://aikapool.com), que oferece uma vasta gama de moedas alternativas disponíveis para mineração.

Available pools

Logo	Pool name	Symbol	Algo	Workers	Pool Hashrate	Net Hashrate	Difficulty	Current Block	Round progress	Nodes	Stratum Port
	Signatum NEW! Profit!	SIGT	skunkhash	110	4243.86 MH/s	932.98 GH/s	9992.4	10773	238.51 %	7	7939
	OliTwistCoin NEW!	OLIT	x11	4	664.23 MH/s	677.93 MH/s	4.74	58339	105.11 %	4	7983
	Octanox NEW!	OTX	x11	4	421.89 MH/s	988.73 MH/s	120.17	15291	73.81 %	4	7982
	QuarkCoin	QRK	quark	5	1103.78 MH/s	6459.22 MH/s	9249.3	4530579	259.19 %	8	7966
	EquiTrader NEW!	EQT	scrypt	0	0 MH/s	5.69 GH/s	3884.49	18313	173.69 %	7	7919

Figura 42: moedas disponíveis na Aikapool.

Observe que a tabela apresenta diversas informações, tais como a quantidade de mineradores, o poder de mineração de pool, a dificuldade da moeda, o bloco atual, o algoritmo, entre outros. A escolha da moeda a ser minerada dependerá de todos esses fatores.

Por exemplo, iremos optar por minerar Quarkcoins por meio de GPU utilizando o ccminer. O primeiro passo é verificar, na documentação do programa, se ele comporta o algoritmo *quark*, utilizado na moeda.

```
penta       use to mine Joincoin / Pentablake
quark       use to mine Quarkcoin
qubit       use to mine Qubit
scrypt      use to mine Scrypt coins
```

Figura 43: Sim! É possível minerar moedas com o algoritmo quark através do ccminer.

Dada a confirmação, devemos selecionara moeda nos cadastrar na Pool. No caso da Aikapool, um único cadastro pode ser utilizado para todas as criptomoedas. Preencha o formulário de cadastro, não se esquecendo de inserir um PIN, um código de 4 dígitos que será utilizado para realizar qualquer alteração na conta. Você não pode esquecê-lo em hipótese alguma.

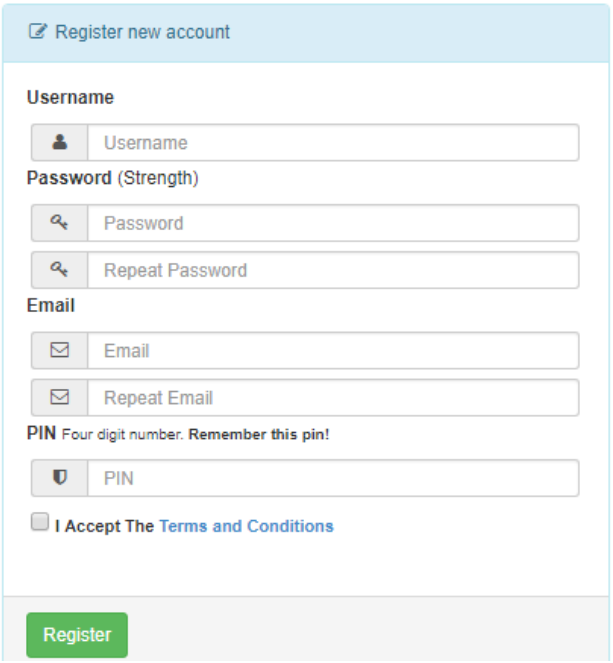
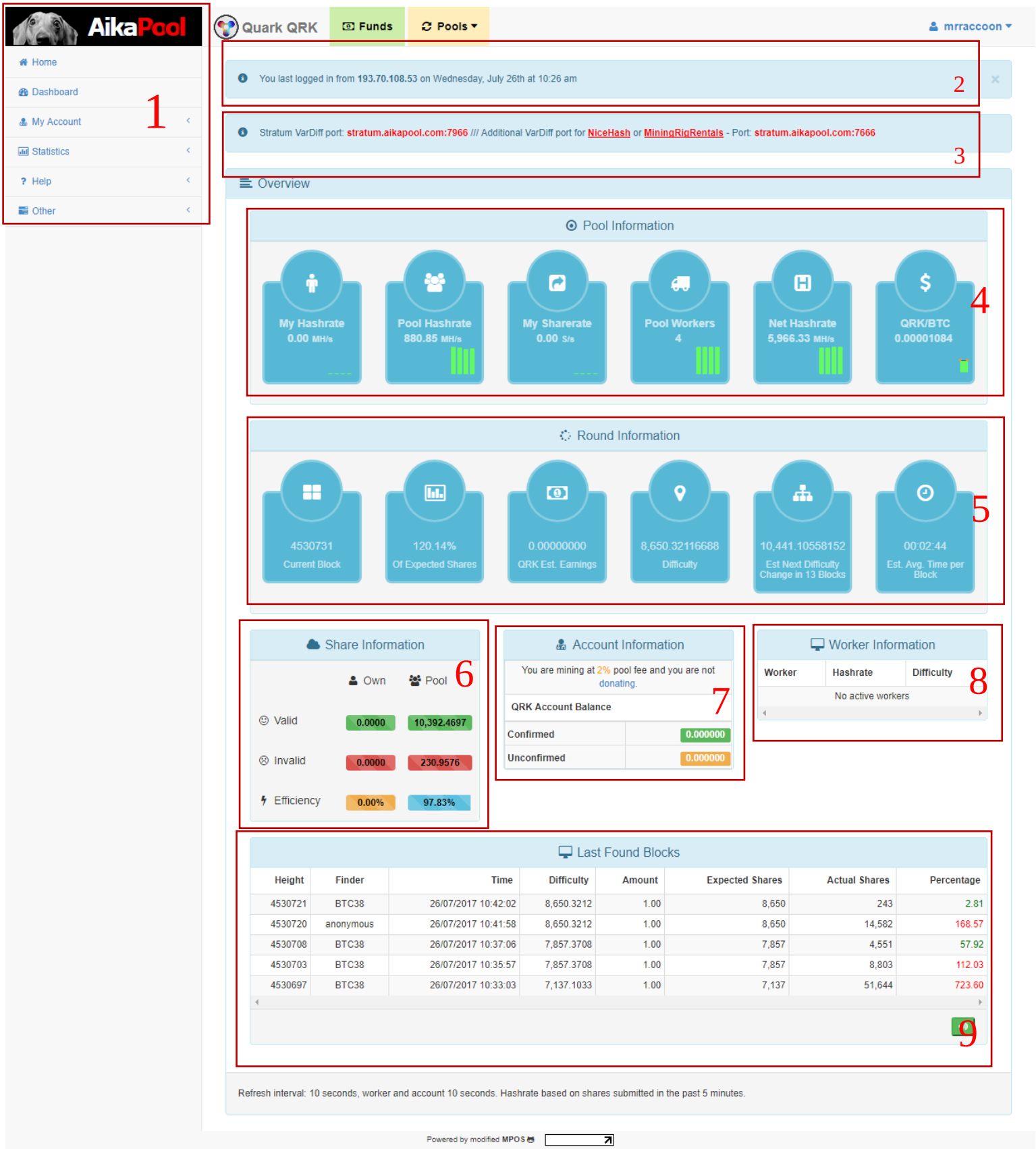


Figura 44: formulário para cadastro na Aikapool.

Após o cadastro, você terá acesso a seguinte interface. É importante que saiba a função de c ada um dos elementos da página. Observe, nas próximas páginas, o significado de cada um de seus elementos.



1. Menu básico da pool. Nele, você pode realizar diversos tipos de operações, que serão explicados a seguir.
2. Último login realizado no serviço. Pode ser útil para verificação de intrusos em sua conta.
3. Endereço da pool. Essa informação será utilizada para configurar seu minerador.
4. Informações a respeito dos mineradores que trabalham na pool, naquele momento, além de detalhes a respeito de seus trabalhadores.
5. Informações a respeito do bloco atual, que está em mineração. Exibe dificuldade, tempo e próxima dificuldade estimada
6. Permite você comparar os valores de seus mineradores com os valores de toda a pool.
7. Exibe o saldo que você já possui, diferenciando-o em confirmado e não confirmado.
8. Informações a respeito de cada trabalhador seu ativo.
9. Informações a respeito dos últimos blocos encontrados.

O próximo passo para administrar a pool é adicionar um trabalhador – ou seja, um usuário fictício capaz de minerar. Isso é feito através do menu principal em *My Account* > *My Workers*. Defina, na opção da esquerda, um nome de usuário e uma senha e adicione um novo minerador. Não se preocupe, pois essas duas informações não são confidencias.

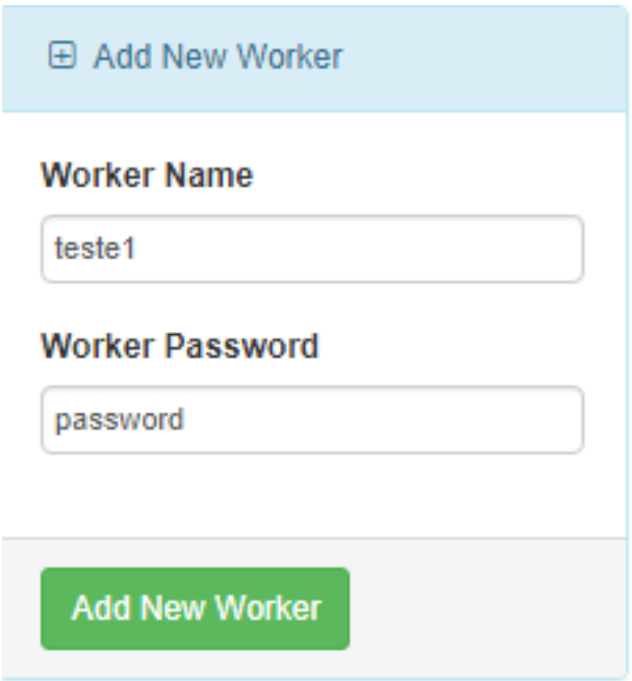


Figura 45: criando um novo trabalhador.

Uma vez adicionado, você irá visualizá-lo na aba de trabalhadores. Lá, é exibido o login de seu trabalhador, juntamente com a senha que definiu. Observe, também, na informação exibida logo acima: ela contém o endereço que será utilizado para seu minerador.

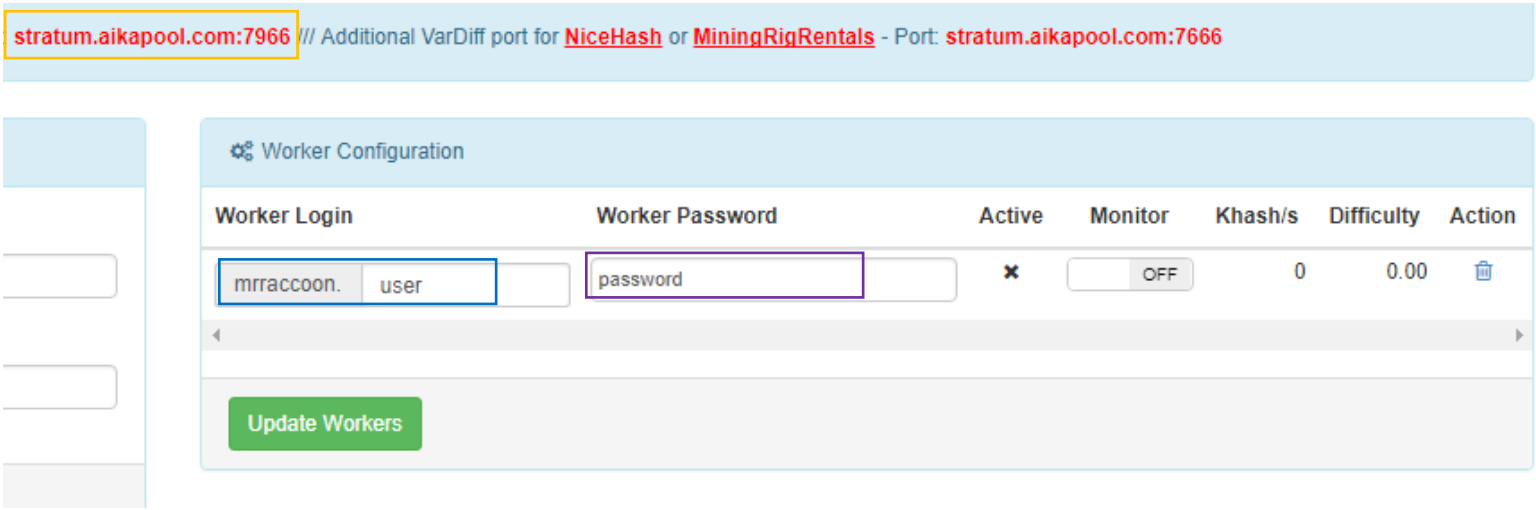


Figura 46: informações necessárias para mineração em pool.

Chegou, então, o momento de configurar o minerador. Para isso, abra o bloco de notas, e insira a seguinte sintaxe:

ccminer-x64.exe -a [algoritmo] -o stratum+tcp://[endereço] -u [usuário] -p [senha] -i [intensidade]

Veja, abaixo, o que colocar em cada campo:

- Algoritmo: a sintaxe do algoritmo da moeda que você deseja minerar. O código para cada uma consta no *readme.txt* do minerador.
- Endereço: o endereço do servidor da pool. Ele está na área acima dos trabalhadores, aqui marcado em amarelo.
- Usuário: login do trabalhador que será utilizado para aquele minerador. Deve ser inserido utilizando o ponto que separa o nome de usuário da conta do nome do trabalhador. Marcado em azul.
- Senha: senha do trabalhador que será utilizado para aquele minerador. Marcada em roxo.
- Intensidade: intensidade do trabalho de mineração. Para uma primeira tentativa, escolha um valor entre 9 e 15. A seguir, irei explicar como definir o valor correto para a instensidade.

Aqui, utilizando intensidade 15, nosso código ficará assim:

ccminer-x64.exe -a quark -o stratum+tcp://stratum.aikapool.com:7966 -u mrraccoon.user -p password -i 15

Após inserir a linha de comando no arquivo de texto, salve-o, na pasta do minerador, com a extensão *.bat* e qualquer nome que desejar – de preferência identificando o que será realizado. Por exemplo:

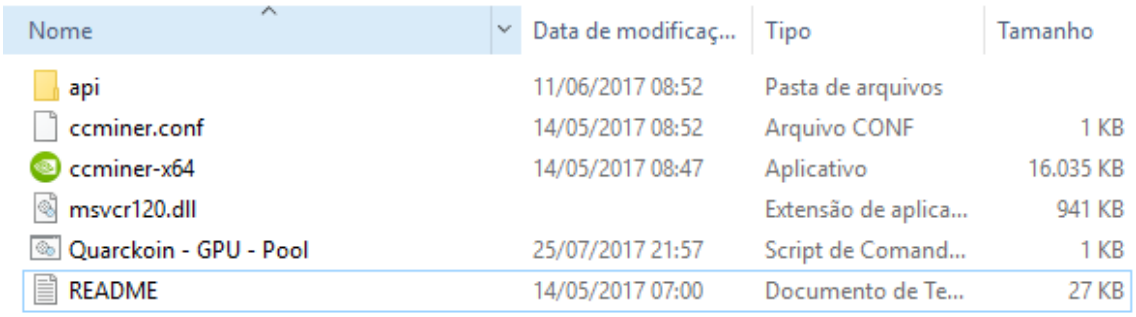


Figura 47: arquivo *.bat* criado na pasta do minerador.

Inicie o arquivo criado. Se tudo estiver sido configurado corretamente, você verá mensagens em verde na tela do prompt de comando que irá se abrir. Deixe-o aberto durante todo o processo de mineração, pois fechá-lo irá interromper.

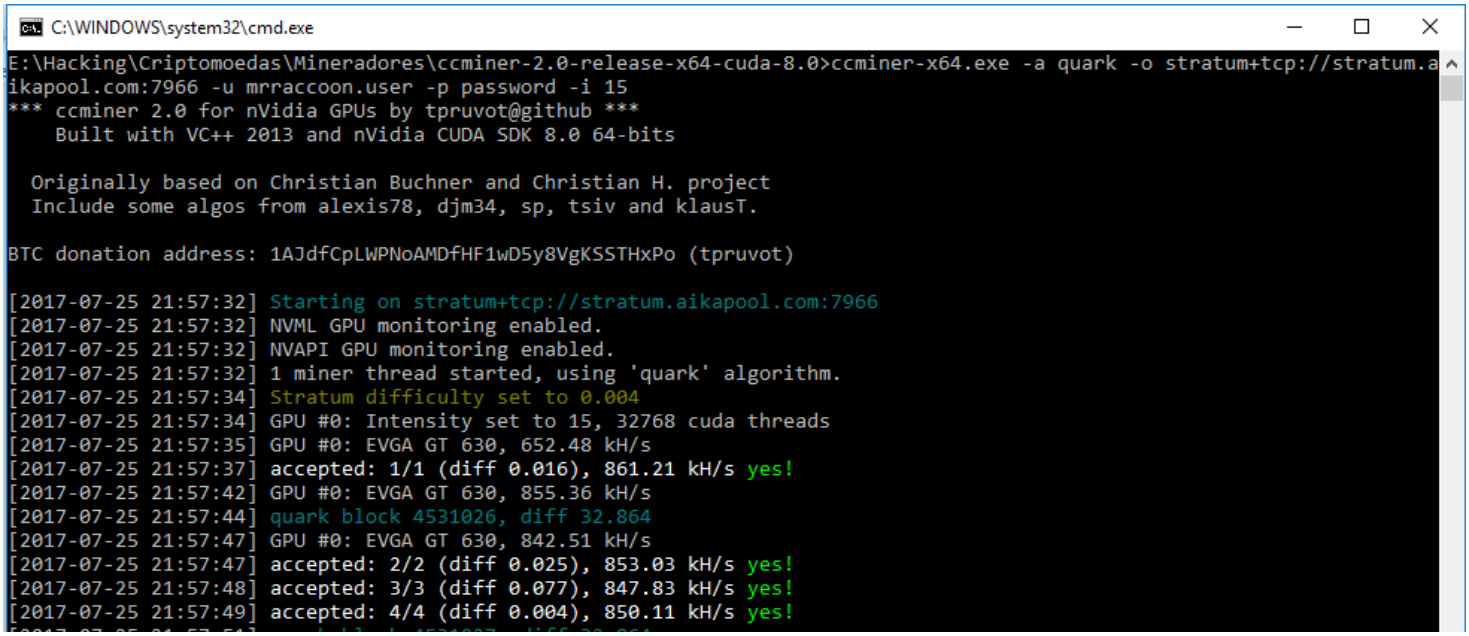


Figura 48: minerador em execução. Note as mensagens de sucesso.

Neste momento, você já deverá verificar que o trabalhador vinculado com o minerador em execução está ativo na pool. Depois de algo tempo notará, também, que suas primeiras moedas – ainda não confirmadas – começarão a aparecer em seu balanço.

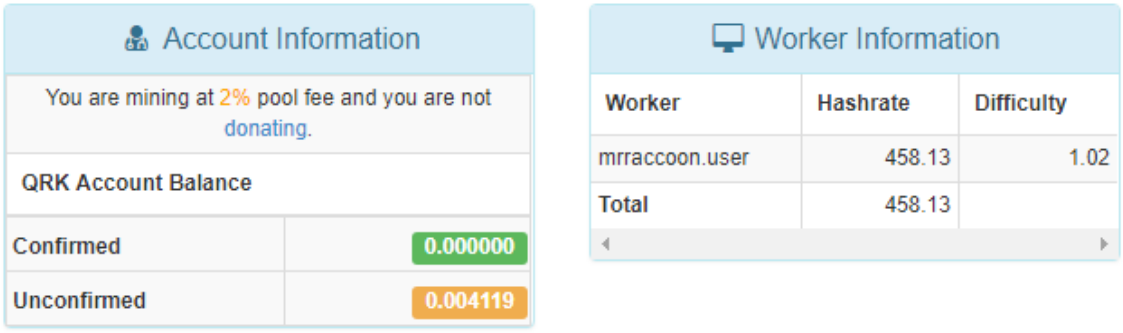


Figura 49: indicativos de que a mineração está ocorrendo conforme esperado.

Após esse processo, aguarde o tempo necessário para que a mineração ocorra. Quando desejar, você poderá enviar a quantia minerada – após a inserção do PIN - para uma wallet qualquer no menu *My Workers* > *Edit Account*.

Para isso, primeiro determine um endereço de pagamento na caixa *Account Details* e faça a transferência para o mesmo endereço na janela *Cash Out*. Uma pequena taxa será cobrada pela pool.

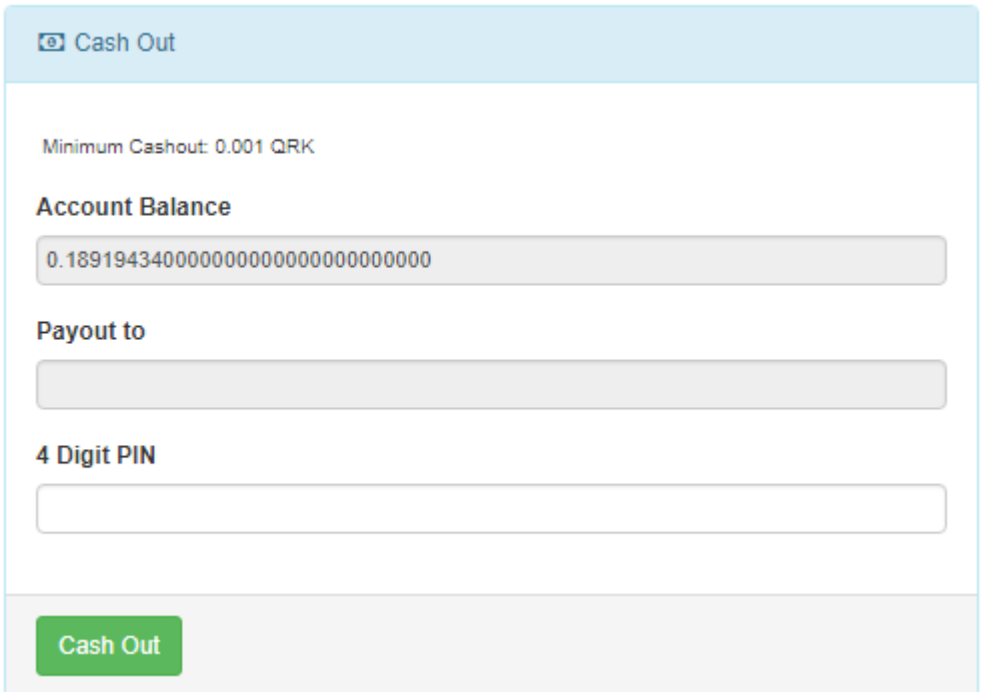


Figura 50: menu para saque da quantia obtida.

7.4 CUIDADOS DURANTE A MINERAÇÃO

Por mais que a mineração possa parecer um processo empolgante, você deverá se atentar a algumas coisas durante sua execução – principalmente no que se diz respeito a temperatura dos componentes utilizados.

Em decorrência de exigir alto desempenho da placa gráfica ou do processador, é incrivelmente fácil que estes equipamentos ultrapassem a temperatura máxima estabelecida pelo fabricante, causando danos muitas vezes irreverAsíveis.

Sendo assim, o monitoramento da temperatura é fundamental. Nunca se esqueça de instalar um programa do gênero, de preferência o Speecy (https://www.piriform.com/speccy), já que este exibe a temperatura graficamente também.

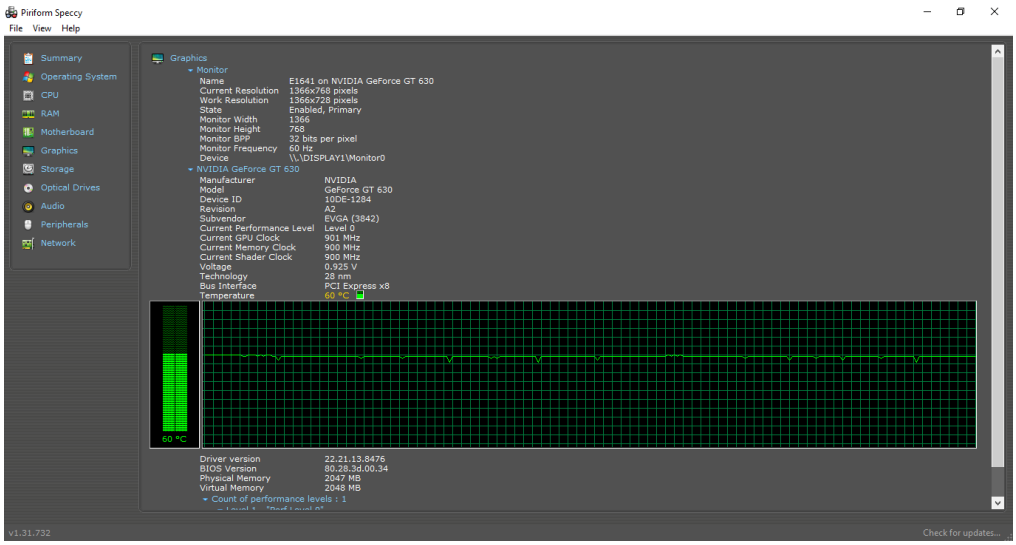


Figura 51: interface do Speecy.

Aproveite, também, para se informar a respeito da temperatura máxima de seu equipamento, conforme especificado pelo fabricante, e evite ao máximo utilizá-lo em temperaturas acima ou da mesma dezena desse valor, especialmente se pretende fazer da mineração uma atividade contínua.

Lembre-se: a placa de vídeo tem como função principal a renderização de jogos, e jogatinas não costumam durar dias inteiros sem interrupções. Logo, se pretende mantê-la funcionando, faça-o em uma temperatura aceitável.

Segue, abaixo, uma tabela – um tanto lúdica – indicando temperaturas de operação genéricas, que se encaixam na maioria dos modelos. Não a considere como verdade absoluta. Apenas a use como forma de orientação.

0°C - 29°C	Você deveria, primeiro, ligar seu computador	
30° C - 49°C	Ocioso, sem tarefas em execução. Tem certeza que seu minerador está ligado?	
50°C - 59°C	A GPU ainda está em marcha lenta. Você pode colocar mais um pouco de energia	
60°C - 69°C	Tem ação acontecendo. Sua GPU está funcionando em uma taxa bastante aceitável!	
70°C - 75°C	Está ficando quente, com mineração otimizada. Não deveríamos aumentar a temperatura.	
75°C - 79°	Área questionável. Algumas GPUs podem lidar com essa temperatura sem maiores problemas, mas é recomendado reduzi-la.	
80°C - 89°C	Como brincar com fogo. Pode parecer que a GPU está bem, mas danos de longo prazo estão sendo causados. Apenas mantenha essa temperatura se você não pretende utilizá-la por mais de um ou dois anos.	
90°C - 99°C	Definitivamente, algum dano ocorreu. Não respire no cheiro de queimado, isso provavelmente lhe fará mal.	
100°C - 109°C	Talvez você ainda possa usar sua GPU depois disso. Mas trate-a bem, como trataria um filhote maltratado.	
110°C+	Parabéns! Sua GPU é um peso de papel. Espere-a esfriar antes de pendurá-la na parede.	

Figura 52: faixas de temperatura para mineração emGPU.

Ao minerar pela primeira vez, fique atendo aos indicadores de temperatura e evite atingir as faixas vermelhas indicadas na tabela. Caso isso ocorra, faça ajustes na intensidade do minerador até que a temperatura se estabilize em uma faixa aceitável – quanto maior a intensidade, mais esforço é necessário e, portanto, maior a temperatura.

Uma vantagem do Speecy é o gráfico de temperatura conforme o tempo. Ele será útil para que você possa saber se a temperatura indicada é estável, ou se ainda está amumetando. Veja abaixo:

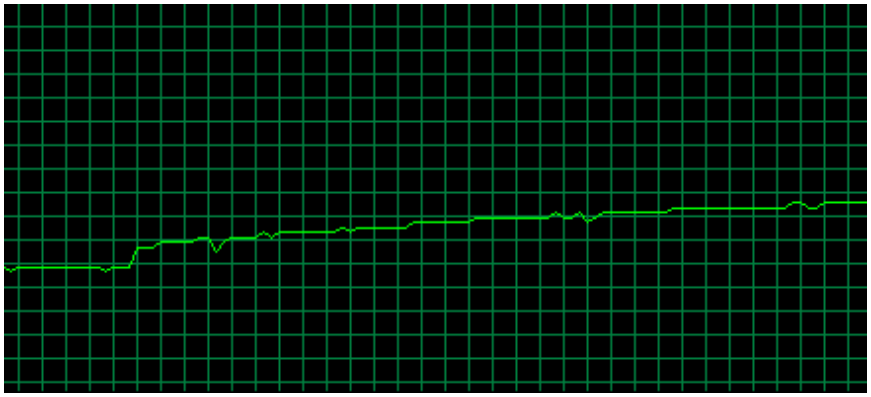


Figura 53: situação na qual a temperatura é crescente.

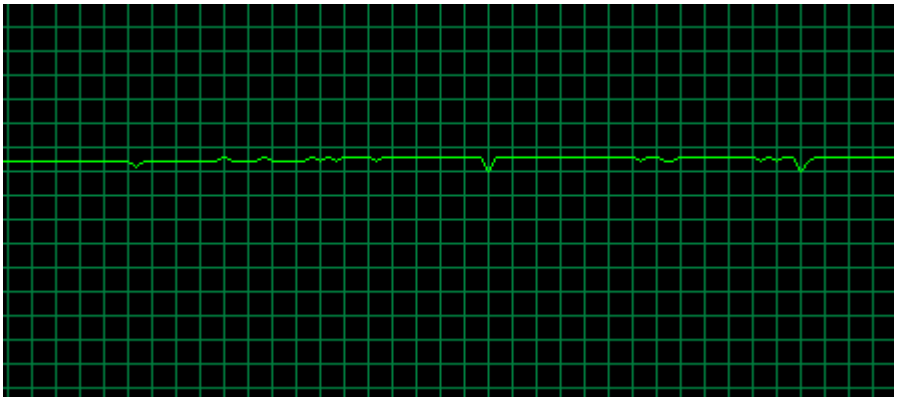


Figura 54: situação na qual a temperatura está estabilizada.

Apenas pare o monitoramento quando perceber que não há mais aumento de temperatura, e que essa se estabilizou em uma faixa segura. Caso contrário, continue acompanhando as variações.

7.5 TÉCNICAS DE ARREFECIMENTO

Caso perceba que a mineração dentro da temperatura aceitável é improdutiva e sinta necessidade de aumentar a intensidade, é recomendado que você procure por formas de reduzir a temperatura de seus equipamentos e permitir a mineração em uma intensidade maior.

Em tese, não há um limite mínimo de temperatura a ser obedecido. Quanto mais frio o ambiente estiver, melhor, salvo casos em que ocorra a condensação (passagem da água em estado gasoso da atmosfera para o estado líquido), já que isso danifica os componentes.

Dessa forma, lhe apresentarei, primeiro, algumas formas de reduzir a temperatura de seu equipamento de mineração. Vale lembrar que todas elas envolvem um custo, que deve ser computado antes de pôr em prática um empreendimento maior.

7.5.1 Dissipadores de calor

O dissipador de calor é um objeto metálico, com grande área superficial, cujo objetivo é promover a troca de calor entre sua origem e o ambiente, através da rápida condução térmica. A grande área superficial permite o maior contato da peça com o ar externo.

São soluções baratas, de fácil instalação e que não consomem energia elétrica para funcionar. Entretanto, podem não ser tão eficientes e costumam já vir inclusos na maioria dos equipamentos em que há risco de aquecimento.

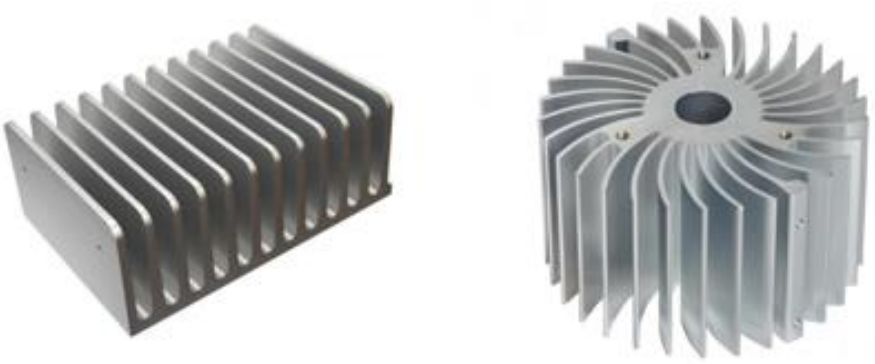


Figura 55: dissipadores de calor.

7.5.2 Ventoinhas

Já as ventoinhas são dispositivos que tem por promover o fluxo de ar nas imediações do componente, conforme sua instalação.

Quando sua função é lançar ar frio para o equipamento, ele é denominado ventilador, e costuma ser instalado de forma lateral à superfície terrestre. Já quando sua função é retirar o ar quente das imediações do equipamento, ele costuma ser instalado com o fluxo de saída apontado para cima, pois a tendência do ar quente é subir na atmosfera.

Figura 56: ventoinha.

A maioria das ventoinhas disponíveis no mercado possuem, em sua lateral, uma seta horizontal e vertical que indicam o sentido de rotação do motor e a orientação do fluxo de ar, respectivamente.

Figura 57: indicativo de setas em uma ventoinha.

Ventoinhas possuem, por padrão, a saída XHP-3 ou XHP-4, que se diferenciam pela quantidade de fios. Os fios vermelho e preto têm a função de conduzir corrente elétrica para o motor, enquanto que os de outras cores (azuis, brancos, amarelos ou vermelhos) enviam sinais a respeito do funcionamento da ventoinha (como o número de rotações por minuto) e permitem a sua regulagem.

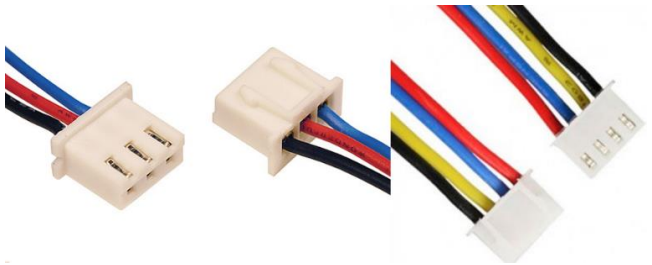


Figura 58: conectores XPH-3 e XPH-4.

Esses conectores devem ser plugados na saída destinadas a eles, presente na placa mãe. Entretanto, é possível adaptá-los através da soldagem dos fios vermelho e preto em pontos específicos, ou convertê-los em USB conectado estes fios aos fios de respectivas cores presentes no cabo USB.

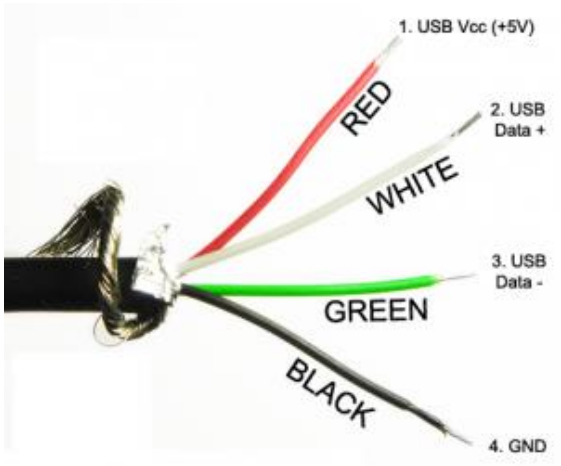


Figura 59: interior de cabo USB.

Vale lembrar, no entanto, que esse tipo de adaptação deve ser feito apenas em caráter provisório pois, o cabo USB não é capaz de fornecer a corrente máxima para a rotação especificada do motor da ventoinha.

Uma adaptação caseira, mas interessante, que já realizei foi a seguinte: converti uma ventoinha para USB e, a afim de evitar parafusa-la no dissipador de calor da placa gráfica (o que poderia danificar o equipamento), utilizei um tripé para celular e o mantive dentro do gabinete.

7.5.3 Cooolers

Muitos costumam confundir cooler com ventoinha. Entretanto, há um pequeno detalhe: o cooler é, na verdade, o resultado da associação entre uma ventoinha e um dissipador de calor.

Figura 60: cooler.

Ao contrário das ventoinhas, que podem ser instaladas em qualquer ponto do gabinete, os coolers devem ser instalados de forma que o dissipador de calor faça contato com o componente que sofre aquecimento.

7.5.4 Refrigeração com água

Existem também a possibilidade de refrigeração do equipamento com água. Nessa situação, a água fria é transportada por entre os componentes através de tubulações – absorvendo calor – e, ao retornar, é resfriada por um conjunto de ventoinhas.

Entretanto, sistemas como esse são caros e muitas vezes desnecessários. Apenas os utilize após um rigoroso planejamento.

Figura 61: sistema de arrefecimento com água.

8 NEGOCIANDO CRIPTOMOEDAS

Em nosso capítulo final, chegou a hora de estudarmos como a compra e venda de criptomoedas – oriundas ou não da mineração – deve ser feita. Vale lembrar que aqui lhe ensinarei a utilizar um mercado de criptomoedas e algumas técnicas de compra e venda. Esse material não irá ensiná-lo a enriquecer, apenas a ser capaz de procurar seus próprios métodos para fazê-lo.

Estudamos, em capítulos anteriores, como casas de câmbio funcionam: elas permitem que qualquer usuário compre e venda criptomoedas com base em um preço fixo, definido pela própria casa e não havendo, portanto, a possibilidade de negociações. Em mercados, o funcionamento é diferente: todo usuário pode escolher o valor que está disposto a cobrar ou pagar por suas moedas.

Evidentemente, isso indica que toda a qualquer negociação em serviços do tipo é regida única e exclusivamente pelas leis de mercado, razão pela qual você deverá dominá-las para compreender seu funcionamento.

8.1 DEPOSITANDO SUAS PRIMEIRAS MOEDAS

Existem diversos serviços de compra e venda de moedas, os quais mencionarei a seguir. Para fins didáticos, utilizaremos o Cryptopia (https://www.cryptopia.co.nz), cujo funcionamento é praticamente o mesmo dos demais mercados.

Cabe a você criar uma conta no Cryptopia. Ao cria-la, o próximo passo será depositar suas primeiras moedas, que podem ser oriundas de qualquer fonte. Isso pode ser feito através do menu superior, na aba *Deposit*.

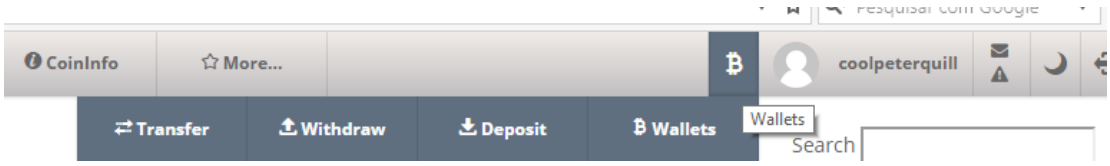


Figura 62: menu para depósito de suas moedas.

Em seguida você deverá escolher, dentre todas as moedas negociadas no mercado, pela moeda que deseja depositar.

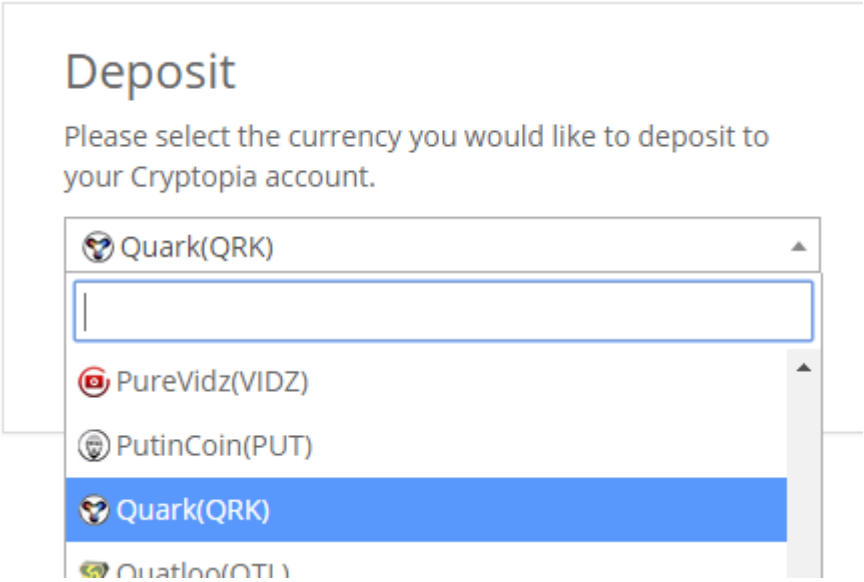


Figura 63: criando seu endereço.

Após a escolha, lhe será exibido o endereço para envio das moedas.

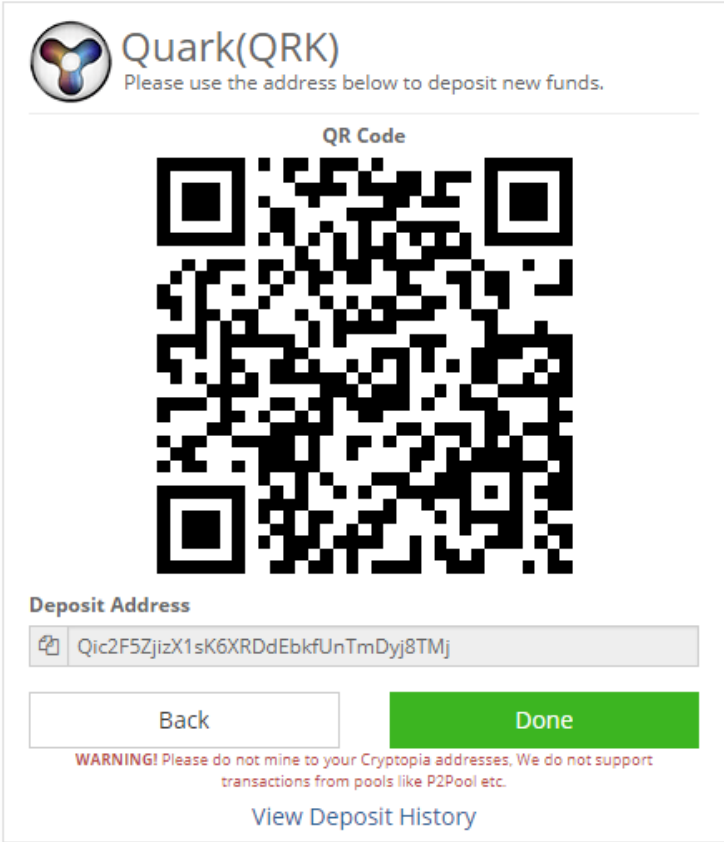


Figura 64: endereço criado.

A partir de agora, você já pode enviá-las. Uma vez criado, seu endereço será adicionado ao menu *Ballances*, no qual é possível ter acesso à todas as moedas existentes em sua conta, além de realizar o saque, transferir saldo para outros

serviços e, principalmente, depositar novas moedas. Há também a opção de "limpar" seu balanço, o que pode ser útil para restos de transações que representam uma quantia irrisória.

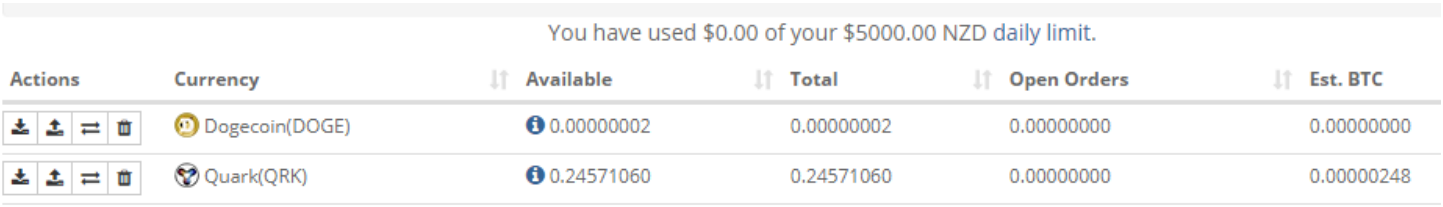


Figura 65: balanço.

Ao enviar uma quantia, pode demorar algum tempo para que você as receba no seu balanço. Nunca deixe grandes quantias acumularem em um mercado: armazená-las nesse tipo de serviço é o mesmo que armazená-las em uma wallet online.

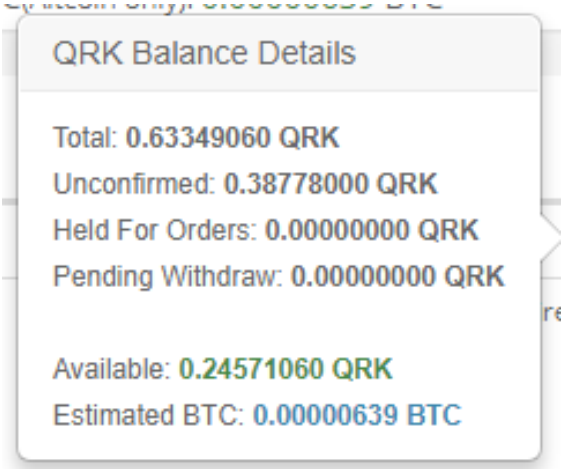


Figura 66: saldo enviado, mas ainda não disponível para uso.

8.2 COMPREENDENDO AS NEGOCIAÇÕES

Em uma negociação, troca-se uma quantia em determinada criptomoeda por outra quantia em outra criptomoeda. Os sistemas de negociações online costumam lidar com cada par de moedas separadamente, dividindo os negociadores em dois grupos: aqueles que querem trocar X por Y, e aqueles que querem trocar Y por X.

Normalmente, X é uma moeda alternativa, como a Quarkcoin, ao passo que Y é uma moeda conhecida, como a Dogecoin. Dessa forma, costuma-se dizer que aqueles que procuram trocar X por Y estão vendendo X, e aqueles que procuram trocar Y por X estão comprando X.

Suponha que você chega em um mercado e deseja vender Quarkcoins. Se você possui pressa em vende-las rapidamente, irá comprar daquele que lhe oferecer mais dinheiro.

Entretanto, os potenciais compradores podem desejar comprar apenas determinada quantidade de moedas. Caso essa quantidade seja menor que aquela que você deseja vender, será preciso negociar com o segundo melhor comprador, e assim por diante.

Logo, fica evidente que, para melhor organização, seria muito mais interessante se houvesse uma lista de todos os que desejam comprar Quarkcoins, quantas Quarkcoins cada um deseja comprar e qual preço cada um deseja pagar. Por conveniência, essa lista é organizada de na ordem de quem paga o maior preço.

Abaixo, há uma tabela fictícia que exemplifica a situação apresentada. Aqui, cada proposta de vendedor ou comprador é chamada de ordem.

Ordens de compra	
Para mim, quanto vale uma Quarkcoin em Dogecoins?	Quantas Quarkcoins estou disposto a comprar?
7 DOGE	17 QRK
6,8 DOGE	5 QRK
5 DOGE	200 QRK
4 DOGE	1 QRK
2,3 DOGE	66 QRK
1 DOGE	20 QRK
0,5 DOGE	10 QRK
0,000000001 DOGE	500000 QRK

Figura 67: exemplo de ordens de compra.

Supondo que você queira vender 15 QRK, evidentemente você as venderá pelo preço de 7 DOGE. Entretanto, se você quiser vender 20 QKR, deverá vender 17 QRK para o primeiro comprador, e 3 QRK para o segundo comprador.

Sendo assim, para um comprador, quanto mais ele pagar por cada Quakcoin, maior a chance de realizar o negócio rapidamente, mas seu gasto em Dogecoins será maior.

Caso o comprador deseje pagar um valor inferior para cada Quarkcoin, sua chance de realizar negócio será menor, pois todas as ordens de compra posicionadas acima dele terão prioridade. Ele apenas terá sucesso caso todas essas ordens se esgotarem e nenhuma outra surgir.

Suponha, agora, que você não está contente com o preço de 7 DOGE por cada QRK. O procedimento a se fazer é, então, anunciar quanto você quer por cada QRK. Sua proposta é também registrada na forma de ordem, de forma que os menores valores têm prioridade em relação aos maiores.

Ordens de venda	
Para mim, quanto vale uma Quarkcoin em Dogecoins?	Quantas Quarkcoins estou disposto a vender?
7,2 DOGE	6 QRK
7,3 DOGE	20 QRK
8 DOGE	300 QRK
8,5 DOGE	666 QRK
8,7 DOGE	3 QRK
9 DOGE	50 QRK
80 DOGE	60 QRK
100000000 DOGE	200 QRK

Figura 68: ordens de venda.

Logo, se você oferece um preço próximo a maior ordem de compra por cada QRK, é provável que não tardará até encontrar um comprador disposto à cobrir sua proposta e aceita-la. E é isso que ele precisará fazer caso estiver com urgência na negociação.

Por outro lado, propor valores absurdos fará que com sua negociação só obtenha sucesso caso todas as demais acima obtiverem – o que dificilmente irá acontecer.

O resultado da associação entre essas duas tabelas é chamado boleta, e contém todos os valores propostos para compra e venda.

Ordens de venda	
Para mim, quanto vale uma Quarkcoin em Dogecoins?	Quantas Quarkcoins estou disposto a vender?
7,2 DOGE	6 QRK
7,3 DOGE	20 QRK
8 DOGE	300 QRK
8,5 DOGE	666 QRK
8,7 DOGE	3 QRK
9 DOGE	50 QRK
80 DOGE	60 QRK
100000000 DOGE	200 QRK

Ordens de compra	
Para mim, quanto vale uma Quarkcoin em Dogecoins?	Quantas Quarkcoins estou disposto a comprar?
7 DOGE	17 QRK
6,8 DOGE	5 QRK
5 DOGE	200 QRK
4 DOGE	1 QRK
2,3 DOGE	66 QRK
1 DOGE	20 QRK
0,5 DOGE	10 QRK
0,000000001 DOGE	500000 QRK

Figura 69: boleta.

Ao participar de uma negociação, cabe a você decidir se a melhor opção é cobrir a primeira ordem (de compra ou de venda) ou propor uma nova, com base na sua urgência e situação do mercado. Tome apenas a cautela de não vender suas moedas por um preço menor que a primeira ordem de compra, pois isso – salvo determinadas circunstâncias – é absolutamente irracional.

Evidentemente, em uma situação real, você terá a sua disposição uma boleta um pouco mais complexa, contendo valores como a soma de todas as moedas propostas, a taxa de conversão, o produto da negociação caso o valor integral seja coberto, entre outros.

Sell Orders 9599.75323510 QRK

Price (DOGE)	Amount (QRK)	Total (DOGE)	Sum (DOGE)
23.99999990	6.00000000	143.99999940	143.99999940
23.99999999	0.29039750	6.96954000	150.96953940
24.00000000	135.00788246	3240.18917904	3391.15871844
25.00000000	10.16699000	254.17475000	3645.33346844
26.00000000	322.70171941	8390.24470466	12035.57817310
26.78000000	14.85317369	397.76799142	12433.34616452
29.91000000	4.00013334	119.64398820	12552.99015272
29.99899900	10.00000000	299.98999000	12852.98014272
29.99900000	399.33794710	11979.73907505	24832.71921777

Buy Orders 192432.51210324 DOGE

Price (DOGE)	Amount (QRK)	Total (DOGE)	Sum (DOGE)
16.00000000	17.33758350	277.40133600	277.40133600
15.10000003	8.66879175	130.89875569	408.30009169
15.10000000	7.00000000	105.70000000	514.00009169
15.00000130	363.26251308	5448.93816844	5962.93826013
15.00000128	4.15497678	62.32465702	6025.26291714
15.00000000	7732.94777126	115994.21656890	122019.47948604
14.89724529	0.07048283	1.05000001	122020.52948605
14.00000004	3.43749999	48.12500000	122068.65448605
13.00000004	3.43749999	44.68750001	122113.34198606

Figura 70: boleta do Cryptopia.

8.3 A PRIMEIRA NEGOCIAÇÃO

A partir de agora, você já é capaz de realizar sua primeira negociação. Para tanto, você deverá acessar o menu Exchange > Markets e nele pesquisar a moeda que deseja negociar. Lhe serão exibidas algumas opções.

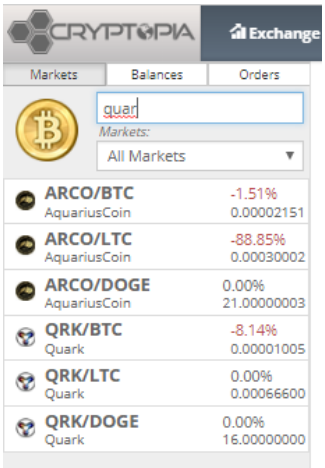


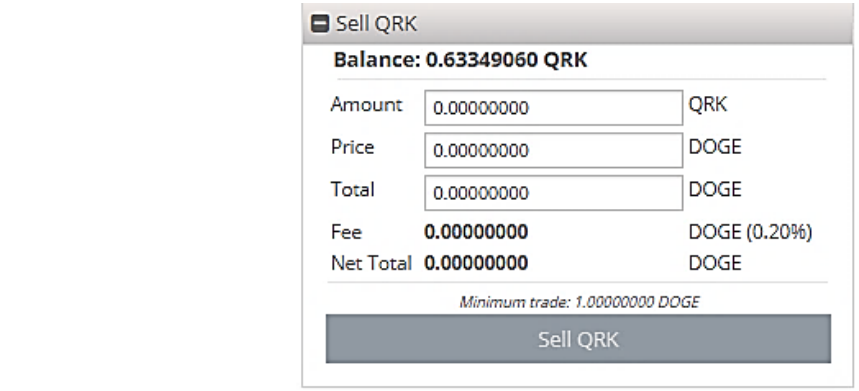
Figura 71: menu de mercado.

Neste exemplo, iremos vender uma quantia de 0.63 QRK em Dogecoins. O primeiro passo para realiza-la é observar a boleta, na parte de ordens de compra – que é o que nos interessa.

Na caixa superior, observamos o nosso balanço associado aos campos no qual escolhemos o total de moedas a serem vendidas, e por qual preço.

Esse campo pode ser preenchido manualmente, ou automaticamente clicando-se no seu saldo (para vende-lo por inteiro) ou em uma ordem (para cobri-la).

Cobrir uma ordem fará com que a negociação seja realizada imediatamente, ao passo que inserir um valor no campo *Price* maior que o da maior ordem fará com que sua ordem seja inserida na boleta.



Buy Orders — 192432.51210324 DOGE

Price (DOGE)	Amount (QRK)	Total (DOGE)	Sum (DOGE)
16.00000000	17.33758350	277.40133600	277.40133600
15.10000003	8.66879175	130.89875569	408.30009169
15.10000000	7.00000000	105.70000000	514.00009169
15.00000130	363.26251308	5448.93816844	5962.93826013
15.00000128	4.15497678	62.32465702	6025.26291714
15.00000000	7732.94777126	115994.21656890	122019.47948604
14.89724529	0.07048283	1.05000001	122020.52948605
14.00000004	3.43749999	48.12500000	122068.65448605

Figura 72: menu para venda e ordens de compra.

Neste exercício, iremos vender aproximadamente metade de nosso saldo (portanto 0,31 QRK) de forma a cobrir toda a oferta, e vender o restante pelo preço de 17 DOGE – que, por estar abaixo da maior ordem, irá para a boleta.

Para a primeira negociação, basta clicar no valor da primeira ordem, definir o total a ser vendido e realizar a venda.

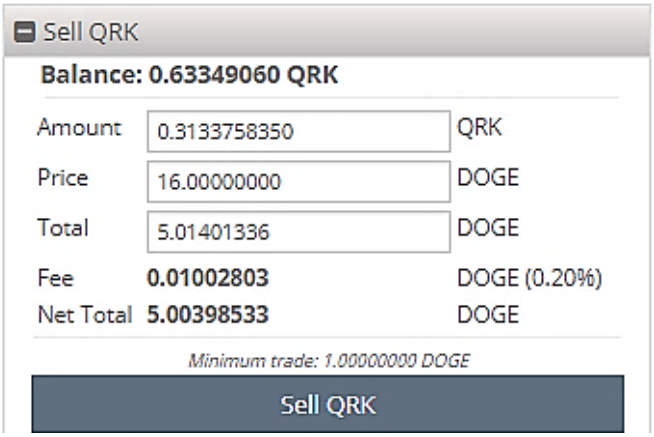


Figura 73: efetuando venda de Quarkcoins.

Imediatamente, você irá receber uma notificação de venda concluída. Ela foi imediata, pois cobriu a ordem apresentada.

Figura 74: ordem concluída.

Agora, vamos realizar a segunda operação. Para selecionar todo o saldo restante, basta clicar em seu balanço e definir o preço.

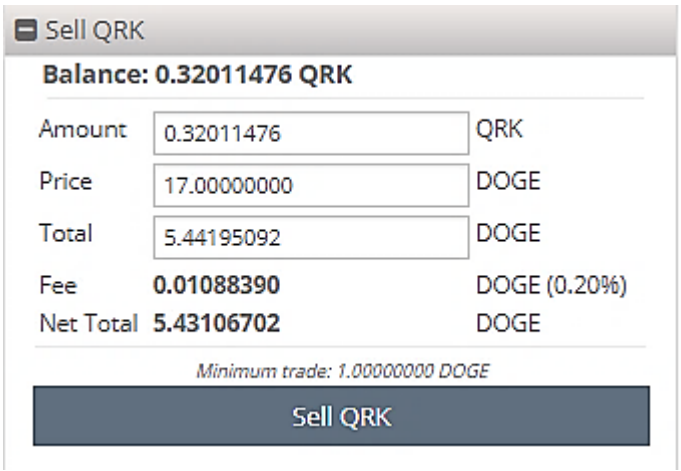


Figura 75: efetuando a venda de Quarkcoins sem cobrir a ordem.

Imediatamente, receberemos uma notificação informando que nossa ordem foi fixada, e poderemos vê-la na tabela de vendas da boleta. Note que, por termos escolhido um valor inferior ao menor valor, nossa ordem agora tem prioridade.

Sell Orders 9600.07334986 QRK

Price (DOGE)	Amount (QRK)	Total (DOGE)	Sum (DOGE)
17.00000000	0.32011476	5.44195092	5.44195092
23.99999990	6.00000000	143.99999940	149.44195032
23.99999999	0.29039750	6.96954000	156.41149032
24.00000000	135.00788246	3240.18917904	3396.60066936
25.00000000	10.16699000	254.17475000	3650.77541936
26.00000000	322.70171941	8390.24470466	12041.02012402

Figura 76: ordem fixada.

Devemos, então, aguardar até que algum comprador cubra a nossa ordem. Durante esse período, o balanço fica retido, mas pode ser liberado a qualquer momento por meio do cancelamento da ordem.

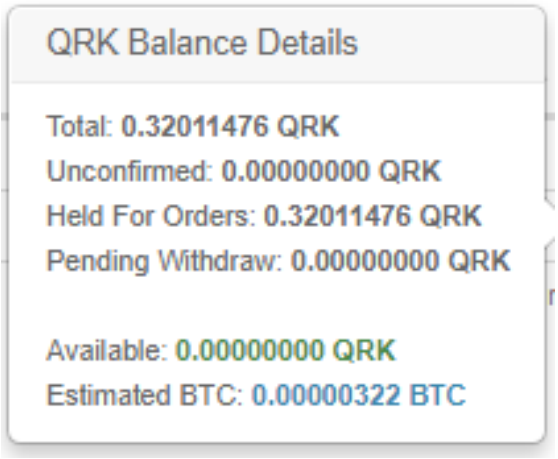


Figura 77: saldo retido para a ordem.

8.4 DICAS PARA NEGOCIAÇÃO

Agora que você já sabe como uma operação de compra e venda deve ser realizada, resta saber quando você deve e quando não deve realiza-las. Evidentemente, esses conhecimentos serão aprimorados ao longo de sua própria experiência, mas ter algum domínio a respeito deles pode lhe ajudar como principiante.

8.4.1 Gráficos em candlestick

Para tanto, precisarei lhe introduzir algumas noções de economia. Você deve ter percebido que o mercado de criptomoedas é algo contínuo, no qual são

realizadas negociações ao longo do dia, envolvendo diversos preços de venda e compra.

Existem diversas formas de monitorar a variação destes preços ao longo do tempo. Uma dessas formas é através de um tipo de gráfico denominado candlestick,

Ele está presente na maioria dos mercados de criptomoedas, e possui barras flutuantes que se assemelham a velas, podendo assumir duas cores diferentes e ainda apresentar sombra – uma barra mais fina pendendo para o lado inferior ou superior da barra.

Veja um exemplo abaixo, retirado da página de negociações de Quarkcoins por Bicoins, de um período de 2 dias, sendo o eixo X destinado à contagem de tempo e o eixo Y utilizado para os valores atingidos – sempre para compra e venda da moeda indicada no canto superior esquerdo.

Figura 78: gráfico candlestick.

Cada uma das barras coloridas (grandes ou pequenas) representa uma medição realizada. O primeiro passo para interpretar um gráfico do tipo é verificar qual o intervalo de tempo cada barra representa.

Para isso, escolha um trecho qualquer do gráfico, como abaixo. Observe o período de tempo presente entre duas marcações no eixo X e conte quantas barras há dentro dele. Divida o período pela contagem de barras, e obterá o intervalo. Nesse caso, o período é de 4 horas, e possui 4 barras. Logo, cada barra representa um intervalo de 1 hora.

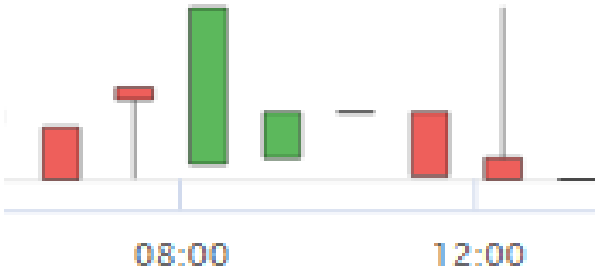


Figura 79: aferindo o intervalo de cada candle do gráfico.

Agora que sabemos a quanto tempo cada candle diz respeito, resta interpretar o que ocorreu dentro deste intervalo. Mas, antes, é importante definir dois conceitos: preço de abertura e preço de fechamento.

Eles correspondem à média dos valores envolvidos em cada negociação no começo e no final do período, respetivamente. Por exemplo, um candle de 1h de duração que começa às 16h, possui como preço de abertura a média de todas as transações realizadas às 16h, e possui como preço de fechamento a média de todas as transações realizadas às 16:59h.

Conhecendo esses conceitos, o primeiro detalhe a ser observado é a cor do candle. Um candle verde indica que o preço de abertura foi menor que o preço de fechamento, e um candle vermelho indica que o preço de abertura foi maior que o preço de fechamento.

Logo, ao ver um candle, você deve ser capaz de identificar, com base em sua cor, quais valores indicam os preços de fechamento e de abertura. Para candles verdes (denominados de alta), o preço de fechamento está na parte superior do gráfico e, para candles vermelhos (denominados de baixa), o preço de fechamento está na parte inferior.

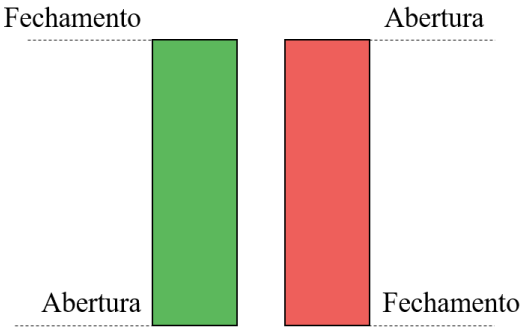


Figura 80: cores de candles e seus significados.

Independentemente de sua cor, candles também podem apresentar linhas finas situadas exatamente em seus centros (denominadas pavios). Seus pontos mais

altos e mais baixos indicam, respectivamente, os valores mais altos e mais baixos envolvidos em negociações ao longo daquele período.

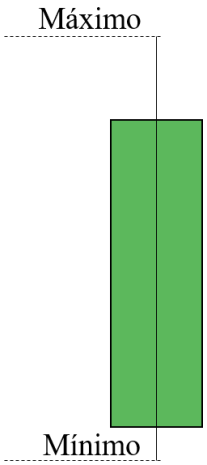


Figura 81: linhas em candles.

Por fim, gráficos do gênero podem ainda contar com informações adicionais. É o caso do gráfico utilizado no Cryptoopia, que ainda apresenta alguns detalhes a respeito do mercado nas últimas 24 horas, além de dados a respeito do candle selecionado.

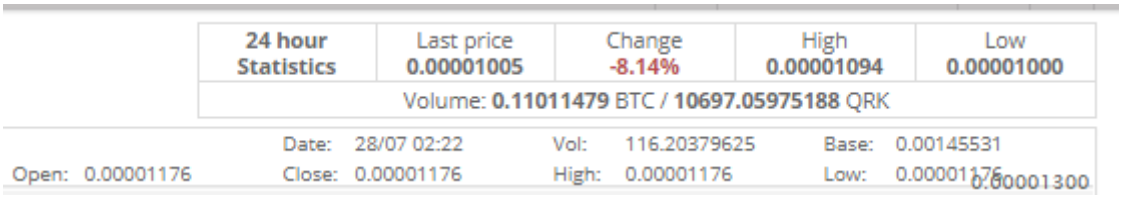


Figura 82: informações adicionais.

O Cryptoopia conta, também, com um gráfico de barras (em cinza) imediatamente abaixo dos candles que indica o volume total de moedas negociado em cada horário.

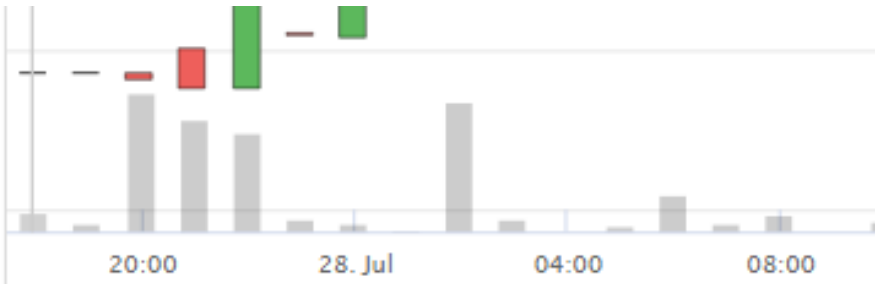


Figura 83: indicador de volume negociado.

8.4.2 Padrões em candles

Agora que você já sabe como interpretar um gráfico de candlestick, resta saber de que forma seus indicadores podem influenciar nas suas decisões. Mas, antes, é interessante que você memorize um lema a ser seguido: **compre baixo, venda alto**.

Isso significa que o melhor momento para comprar criptomoedas é quando seu preço está baixo, e o que o melhor momento para vende-las é justamente quando seu preço está em alta.

Dessa forma, irei mostrar alguns candles que podem lhe indicar padrões interessantes em suas movimentações, baseado no artigo do Infomoney.

O candle abaixo, chamado de **Piercing Lane**, é composto por, após sucessivas quedas, um novo candle de queda seguido por um candle de alta que penetra em mais da metade no candle anterior. Sua aparição pode ser um forte indicativo de que o mercado tende a sofrer reversão, ou seja, que o preço tenderá a subir após uma sequência de quedas.

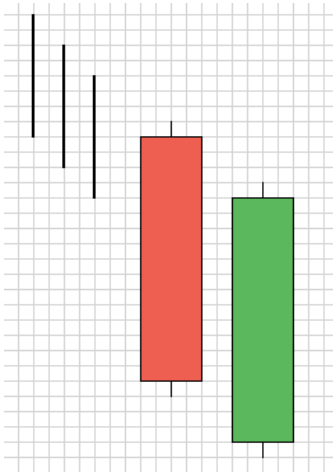


Figura 84: Piercing Lane.

Já o próximo candle, denominado **Kicking**, é composto por um candle de baixa seguido por um candle de alta, ambos sem pavios (também chamado de **Marobozu**), ou com pavios pequenos. É um sinal muito forte de que, independentemente do comportamento anterior, o mercado seguirá em alta, pois a força compradora é muito grande.

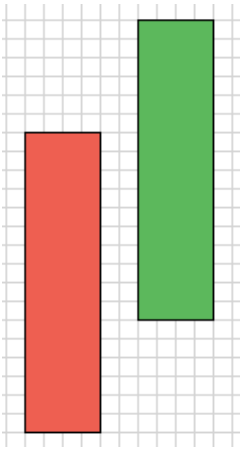


Figura 85: Kicking.

Candles que não possuem corpos ou cores (ou seja, aqueles nos quais o preço de abertura foi igual ao preço de fechamento) podem ser indicadores interessantes. Estes costumam ser chamados de **Doji**.

Quando um Doji é encontrado entre um candle de alta e um candle de baixa, é um sinal eminente de que houve uma reversão e de que a tendência do mercado é manter-se na forma do candle mais a direita. Ele é chamado de **Bebê Abandonado** (não me pergunte quem inventa esses nomes).

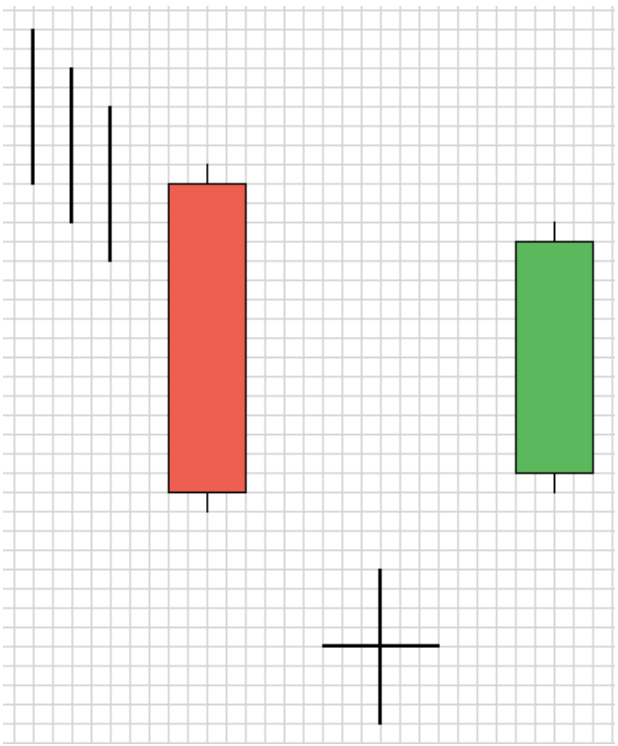


Figura 86: Bebê Abandonado indicando alta.

Quando a situação é oposta, dizemos que o Bebê Abandonado pode indicar uma futura baixa, como no exemplo:

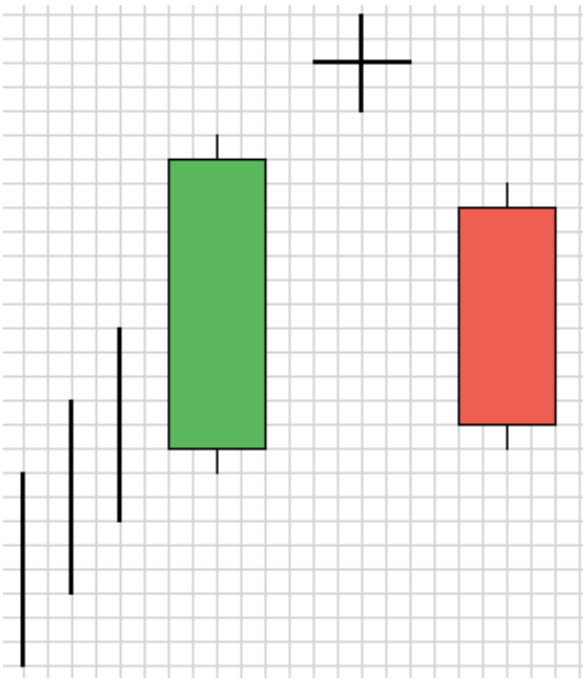


Figura 87: Bebê abandonado de alta.

Caso, no lugar do Doji tenhamos um candle de corpo pequeno (seja ele de alta ou baixa), observamos uma indicação também de uma mudança, mas não tão abrupta quanto na situação anterior. Podem haver também mais de um candle de corpo pequeno no fundo da reversão. Essa formação é denominada **Estrela da Manhã** e, quando na forma contrária, é denominada **Estrela da Tarde**.

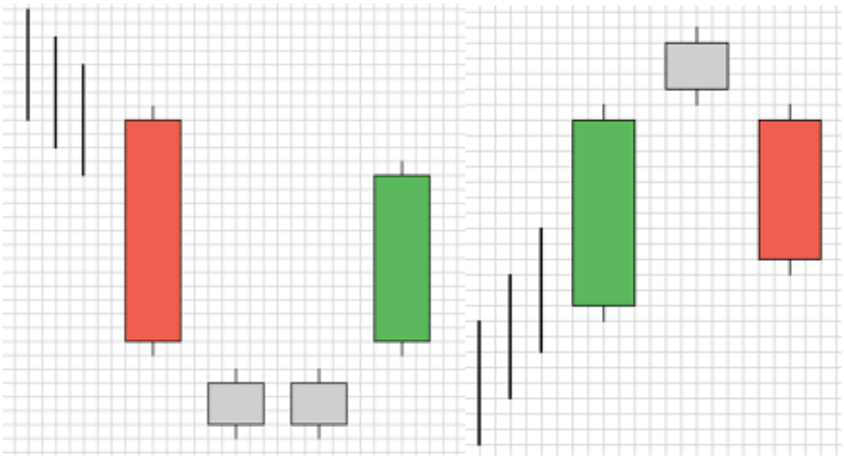


Figura 88: Estrela da Manhã (esquerda) e Estrela da Tarde (direita).

Outro sinal de alta é o chamado **Three Outside Up**, composto por um engolfo (quando o primeiro candle é menor que o segundo e fica dentro dos limites deste) seguido de um candle de alta, confirmando a reversão esperada.

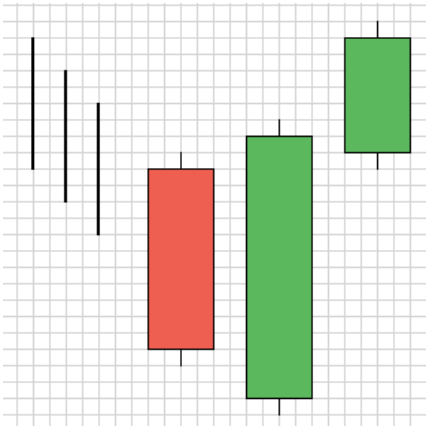


Figura 89: Three Outside Up

Quando observamos um Doji após uma série de quedas com sombra para baixo, temos um sinal de confiabilidade média que indica uma possível recuperação do mercado.

Nestes, o mercado abre e rapidamente leva os preços a novas mínimas, mas em algum momento o preço se torna atraente e os investidores voltam a comprar, levando o preço a subir. Ele é chamado de **Dragonfly Doji**.

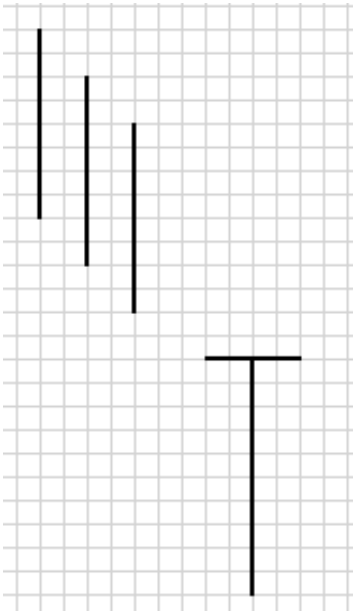


Figura 90: Dragonfly Doji.

Um indicativo de indecisão no mercado é um doji com grandes pavios em ambos os lados, denominado **Long Legged Doji**.

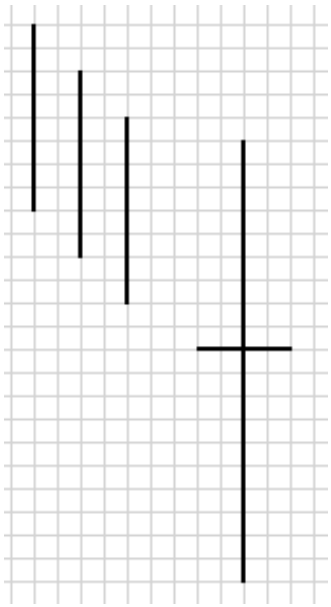


Figura 91: Long Legged Doji.

A **Gravestone de alta** também é um padrão interessante, no qual, após um movimento de queda, é observado um Doji com o pavio para cima. Ele indica uma possível reversão do movimento de baixa.

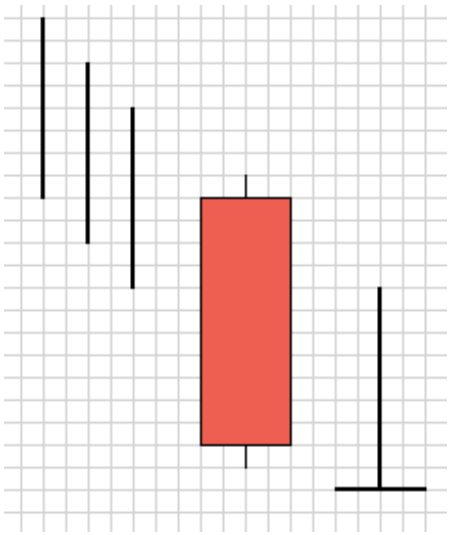


Figura 92: Gravestone de alta.

Já quando ocorre uma **Gravestone de baixa**, essa aparece na forma exatamente oposta: após uma sequência de altas, e indica uma possível queda do mercado.

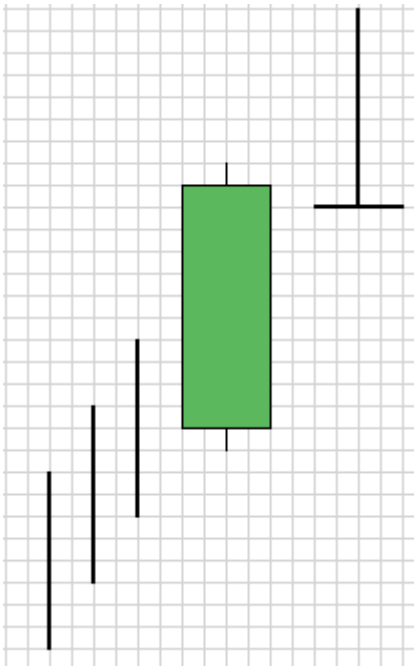


Figura 93: Gravestone de baixa.

Quando, após um candle sem pavios ou sombras, encontramos um Doji com pavios e sombras de mesmo tamanho, ele é denominado **Harami Cross** (de baixa ou de alta, dependendo do candle antecessor) e indica uma possível reversão do mercado.

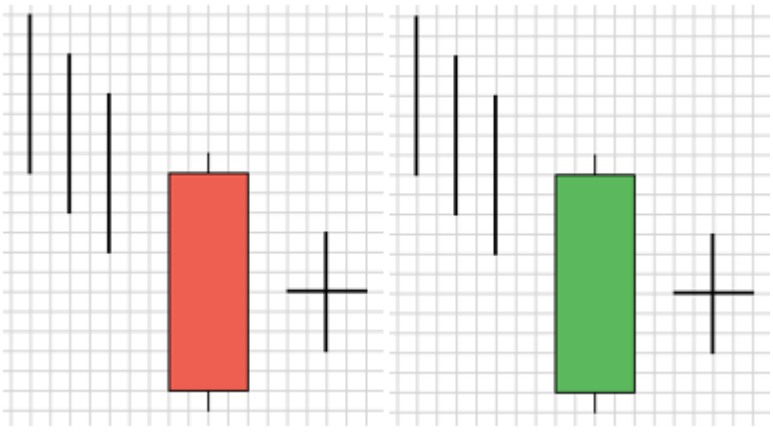


Figura 94: Harami Cross de alta (esquerda) e de baixa (direita).

Existe também o **Breakway**, caracterizado por um fundo arredondado, formado por vários candles (ao menos 5 deles). Indica que o mercado atingiu um ponto de sobrevenda e patamares de preços menores não mais predominam, rumando para um momento de alta.

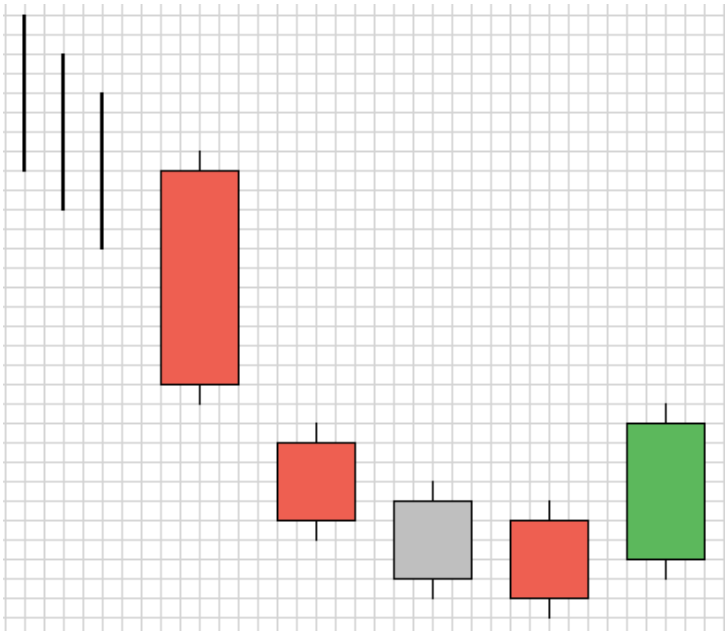


Figura 95: Breakway.

Chamamos de **Nuvem Negra** um padrão formado pois dois candles, um de alta e um de baixa, que caracteriza o final de uma tendência de alta, como fechamento próximo ao da mínima do dia, sendo este menor que o fechamento do dia anterior. Quanto maior o candle de baixa penetrar o candle de alta, maior será a probabilidade de reversão.

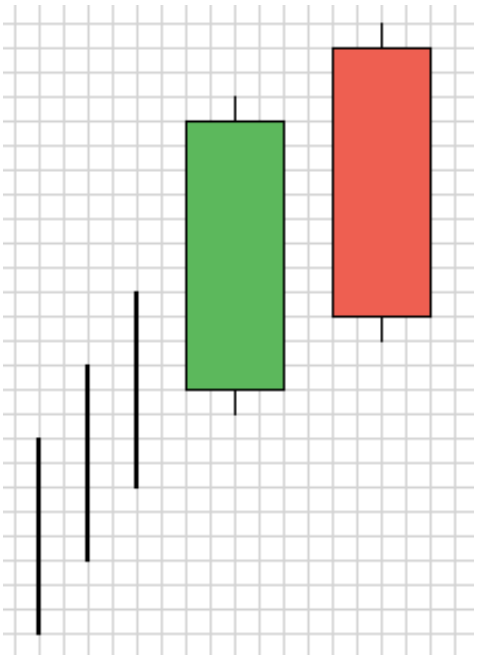


Figura 96: Nuvem Negra.

Uma formação denominada **Three Black Crows** indica um movimento de queda do mercado, e é composto de três candles de queda sucessivos.

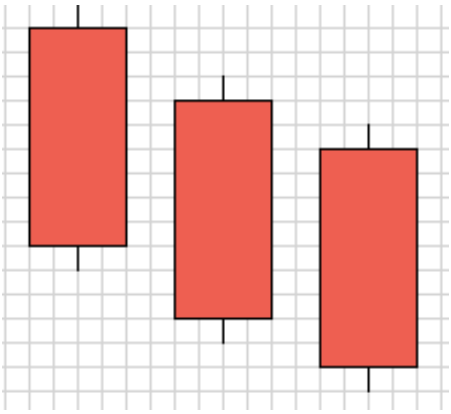


Figura 97: Three Black Crows.

Existem também o **Martelo** e o **Martelo Invertido** que indicam possibilidades de reversão: alta ou baixa, respectivamente.

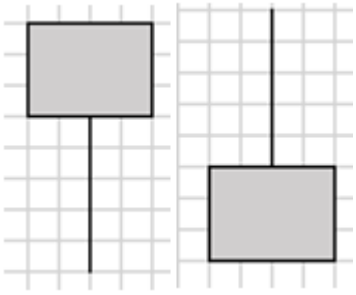


Figura 98: Martelo (esquerda) e Martelo Invertido (direita.

Concluíndo, caberá a você, durante as operações, procurar por cada candle e interpretar suas possívieis indicações. Uma ideia interessante para o usuário iniciante é observar em registros antigos e procurar por exemplos práticos do que foi estuado na teoria .