Trabalho de Conclusão do Curso de Bacharelado em Ciência da Computação

Ricardo Macedo <rick@pataca.io>

sob a orientação de
Prof. Flávio Soares (IME-USP)
Prof. Gilson Schwartz (ECA-USP)

2014

PATACA

um sistema para promoção da descentralização da moeda através de moedas criptográficas

MOEDA

Todos os dias, bilhões de pessoas utilizam moedas para movimentar valores. Hoje em dia, elas são emitidas por países e seu valor varia livremente, de acordo com o mercado.

Porém, antes de 1971, seu valor era dado de acordo com uma certa quantidade de ouro ou outro metal.

Pré-História até 600 a.C

Desde a antiga Suméria, em 2500 a.C., é possível encontrar tábuas cuneiformes que relatam depósitos e dívidas em trigo dos camponeses. Meios de troca em metais eram primariamente utilizados para o comércio, mas enfrentavam problemas com relação ao transporte e sua segurança.

600 a.C. até início do séc. XX

As primeiras moedas surgiram por volta de 600 a.C. na região da Anatólia, atual Turquia. Elas eram compostas de ouro e prata, portando uma ensígnia ou inscrição. Apesar de irregulares em seu formato, possuíam pesos padronizados, facilitando seu uso no comércio.

A utilização de metais ou ligas metálicas, tais como o ouro, a prata e o cobre, para o armazenamento de valor se difundiu, sendo base para o comércio mundial e sistemas econômicos nacionais até o início do século XX.

1944 até 1971: Sistema de Bretton Woods

Com muitos países abandonando o padrão-ouro devido à crise dos anos 1920 e ao endividamento decorrido da II Guerra Mundial, as 44 nações aliadas assinam um acordo que prevê que os Estados Unidos mantenham a conversibilidade de sua moeda em ouro a uma taxa fixa de US$ 35 por 1 onça (28,35 g) do metal. A partir disso, as outras moedas nacionais, tais como o marco e o franco, atrelam-se ao dólar.

1971 até hoje

Em 1971, o presidente norte-americano Richard Nixon suspende a garantia de conversão de dólares em ouro. Isto encerra a existência de um lastro metálico nas finanças internacionais, passando a adotar um regime de câmbio flutuante para as moedas.

DESCENTRALIZAÇÃO

A descentralização é um conceito que pode ser aplicado a diversas áreas. Relacionada a sistemas, sejam eles computacionais, políticos ou econômicos, ela democratiza o acesso, estabelecendo protocolos bem definidos de funcionamento.

ARPANET e troca de pacotes

Precursora da internet, a ARPANET foi uma das primeiras redes a implementar o protocolo TCP/IP, utilizado atualmente. Seu objetivo era interligar laboratórios de pesquisa e universidades dos Estados Unidos para facilitar a troca de informações.

O protocolo TCP/IP estabelece um conjunto de regras que possibilita interligar redes distintas, transportando dados entre elas.

Não há roteamento central: os pacotes de dados são repassados para o melhor candidato (*best-effort*) que, prossegue com a transmissão. Desta forma, a internet torna-se escalável e mais resistente a falhas.

BitTorrent

O BitTorrent consiste em um protocolo de troca de arquivos que também não prevê um servidor central. Os nós da rede que possuam um determinado arquivo, completo ou parcial, enviam os dados para os que querem obtê-lo.

Um arquivo, ou conjunto deles, pode ser encontrado através de uma chave de hash de seus dados. Isto é possível através da implementação de um banco de dados distribuído chamado Distributed Hash Table (DHT), compartilhado entre todos os nós da rede.

BITCOIN

Em 2008, um usuário, cujo pseudônimo é Satoshi Nakamoto, publica um artigo descrevendo um sistema eletrônico de pagamentos chamado Bitcoin.

Ele se baseia em um modelo chamado "proof-of-work", onde comprova-se que uma determinada quantidade de trabalho foi realizada através de um processo difícil de computar, porém fácil de verificar.

Afinal, o que é bitcoin?

Bitcoin é uma estrutura baseada em criptografia de chave pública e em hashes criptográficos, mais especificamente, o SHA-256. Este algoritmo mapeia uma informação qualquer de tamanho arbitrário para um número de 256 bits, cuja distribuição probabilística é uniforme, ou seja, para um certo dado de entrada, a saída está em todos os pontos do intervalo $[0, 2^{256}]$ com igual probabilidade.

De onde eles surgem?

O bitcoin é constituído por blocos, que são responsáveis pela emissão da moeda. Estes, ao invés de serem criados, são descobertos.

Blocos são estruturas de dados compostas, majoritariamente, por transações bitcoin. A primeira transação de um bloco é a recompensa por encontrá-lo, e seu destino é a carteira de quem realizou tal ação.

Para encontrar um bloco, é necessário que seu valor de hash seja menor que um dado valor informado pela rede. Isto é feito através da mineração, que itera o campo *nonce* do bloco, até satisfazer esta condição.

Atualmente, a recompensa é de 25 bitcoins por bloco. Ela cai pela metade a cada 210.000 blocos.

Blockchain (ou cadeia de blocos)

Uma vez encontrado o valor que satisfaça a condição, o bloco é propagado na rede e verificado pelos outros nós.

Além das transações, o bloco armazena o hash do bloco anterior. Uma vez que o bloco é encontrado e verificado pelos nós da rede bitcoin, e devido a sua estrutura, as informações ficam registradas de forma imutável em uma forma de lista ligada.

O blockchain armazena trabalho, pois algoritmos de hash criptográfico, como o SHA-256, não possuem bijeção com seus dados de entrada. Isto significa que não há alternativa para encontrar uma entrada cuja saída seja um valor específico, a não ser através de tentativa e erro.

Uma moeda sem bancos

Com estas características, o bitcoin apresenta-se como uma forma de moeda eletrônica que não necessita de intermediários para que pessoas em partes distantes do mundo possam transacionar valores.

Além disso, somente o portador da chave privada de um determinado saldo pode movimentá-lo. Isto significa que não há estornos ou transações realizadas por terceiros que não possuam as credenciais necessárias.

PROOF-OF-WORK NA MINERAÇÃO

O minerador prova que realizou trabalho mostrando um dado cujo valor de hash é menor do que um dado valor.

Vamos demonstrar como isso é feito supondo uma situação onde um dado, para ser aceito, deve possuir um valor de hash que comece com 24 bits zero, ou 3 dígitos hexadecimais "00".

DADO
`pataca:0`

`pataca` é o valor a ser aceito;
`0` é um inteiro, chamado *nonce*.

VALOR DE HASH SHA-256
`3195ca2e65fb47dd5c66f6ea57e9619e`
`1ae74a37e634a94686ff1ea230c27909`

Como observamos, o valor de hash não satisfaz a condição. Para isso, iteramos o campo *nonce* até encontrar um valor de hash que possua as características desejadas:

DADO
`pataca:27156202`

VALOR DE HASH SHA-256
`000000163856a42ed2c6216f14a71395`
`c542f69dd36c6e37dfee0a1299da1111`

Agora, o dado pode ser aceito, já que satisfaz as condições impostas. Como não existe outra maneira de encontrar o valor de *nonce* que resulte em um determinado valor de hash a não ser através do cálculo sucessivo do SHA-256 para cada iteração, o minerador prova que realizou trabalho ao informar o dado.

PATACA

Utilizar o bitcoin como lastro possibilita integrar diferentes economias locais, movimentando valores entre elas. O dinheiro de uma comunidade pode ter valor em outra, além de possibilitar a qualquer pessoa criar a sua própria moeda.

O Pataca fornece um sistema de contas e um protocolo de comunicação entre instâncias do sistema.

Conceito

Pequenas economias estão ao nosso redor e fazemos uso delas cotidianamente. Exemplos bastante próximos são os tickets do Restaurante Universitário e o empréstimo de livros nas bibliotecas, além de milhas em companhias aéreas, entre outros programas de fidelidade.

Pataca é um sistema para criação e administração de economias locais que permite atrelar um lastro em criptomoeda, integrando a comunidade a uma rede descentralizada de troca de valores.

Tecnologias

A implementação atual do Pataca foi escrita em Python, utilizando Twisted Matrix para gerenciar a comunicação com a internet e SQLAlchemy para o mapeamento objeto-relacional. É leve o suficiente para rodar em um Raspberry Pi.

Como funciona

Toda a interação com o Pataca é feita através de uma API baseada em REST, com comunicação em JSON trafegando em um canal seguro (SSL).

As chamadas são feitas para URIs do servidor, de acordo com a operação requisitada.

Módulos

O Pataca se estrutura em módulos, que podem ser adicionados ou removidos de uma instância. Esses seguem uma especificação simples, indicando a URI base e um dicionário de operações, onde cada uma aponta para uma função. Os módulos são encapsulados em pastas, o que permite que sejam redistribuídos individualmente ou em pacotes.

Módulos podem definir novos modelos no banco de dados, além de interagir com os já presentes, como usuário, conta e moeda.

Utilização

Como constitui-se de uma API, o Pataca possui como objetivo a simplificação de seu uso por parte de outras aplicações. Estas também podem ser interfaces gráficas, desenvolvidas para web ou dispositivos móveis.

Desta forma, Pataca é integrável com quaisquer sistemas que possuam ou queiram possuir um sistema de contas, com a emissão de tokens.

Lastro

O lastro é implementado como um módulo, que atrela um estoque em criptomoeda a um estoque de uma moeda presente no Pataca.

PROTOCOLO PATACA

O protocolo Pataca permite que instâncias do sistema troquem valores entre si de acordo com uma determinada taxa de conversão, dada pela razão entre o estoque de bitcoins e o estoque total de uma moeda do sistema.

PASSO-A-PASSO

SITUAÇÃO
Alberto prometeu repassar 500 botões, de sua conta nas Organizações Foo, para Bernardo, que possui uma conta, em estalecas, no Bar Bar, um popular ponto-de-encontro local.

1 Alberto pergunta a Bernardo qual seu endereço Pataca, que informa `bernardo@bar.net`

2 Alberto inicia a transferência de 500 botões da sua conta `alberto@foo.org` para a conta de Bernardo.

3 O servidor `foo.org` bloqueia o saldo correspondente e notifica o servidor `bar.net` sobre a transferência, pedindo um endereço de carteira bitcoin que represente a conta `bernardo@bar.net`

4 O servidor `bar.net` responde com o endereço e aguarda.

5 Com o endereço bitcoin de destino, foo.org verifica a taxa de câmbio, no caso, 0,0002 bitcoin por botão, envia a quantia de 0,1 bitcoin para a carteira, ou 500 botões, e notifica bar.net sobre a transação.

6 Ao receber a transação, após um certo número de confirmações da rede bitcoin, `bar.net` credita a conta de Bernardo com 125 estalecas, dado que a taxa de câmbio é de 0,0008 bitcoin por estaleca.

REFERÊNCIAS

[1] GRAEBER, David. **Debt: The First 5000 Years.** Nova Iorque: Melville House Publishing, 2011.
[2] BENKLER, Yochai. **The Wealth of Networks: How Social Production Transforms Markets and Freedom.** Yale University Press, 2006.
[3] NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** *http://bitcoin.org/bitcoin.pdf*, 2008.

Twisted Matrix
www.twistedmatrix.com

SQLAlchemy
www.sqlalchemy.org

apoio MERCADO BITCOIN.NET

website pataca.io

twitter @gopataca