PATACA

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

um trabalho de **Ricardo Macedo** sob a orientação do **Prof. Flávio Soares (IME-USP)** e **Prof. Gilson Schwartz (ECA-USP)**

Pataca possibilita
você criar sua
própria moeda.

Mas, o que isso
SIGNIFICA?

A MAIS BREVE HISTÓRIA DA MOEDA

A MAIS BREVE HISTÓRIA DA MOEDA

ANTES DA CUNHAGEM

600 A.C. ATÉ INÍCIO DO SÉC. XX

SISTEMA DE BRETTON WOODS

MOEDA FIDUCIÁRIA

DESCENTRALIZAÇÃO

DESCENTRALIZAÇÃO

ARPANET BITTORRENT WIKIPÉDIA OPEN SOURCE

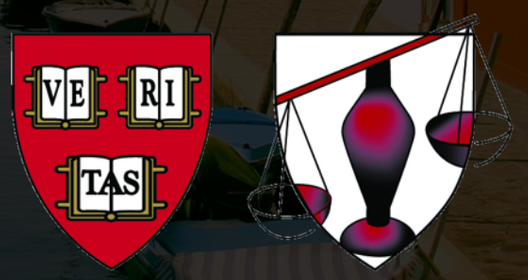
DESCENTRALIZAÇÃO

ARPANET BITTORRENT WIKIPÉDIA OPEN SOURCE

SABIR

Primavera De Filippi
Samer Hassan

http://sabir.cc/



Berkman

The Berkman Center for Internet & Society
at Harvard University


bitcoin

bitcoin

SATOSHI NAKAMOTO (PSEUDÔNIMO)

SISTEMA DE TRANSFERÊNCIA DE VALORES

SEM INTERMEDIÁRIOS

DESCENTRALIZADO

BASEADO EM CRIPTOGRAFIA

bitcoin

SATOSHI NAKAMOTO (PSEUDÔNIMO)

SISTEMA DE TRANSFERÊNCIA DE VALORES

SEM INTERMEDIÁRIOS

DESCENTRALIZADO

BASEADO EM CRIPTOGRAFIA

BLOCKCHAIN

(proof-of-work)

PROOF-OF-WORK

PROOF-OF-WORK

DWORK E NAOR, 1992

CONTRA SPAM

UTILIZA FUNÇÕES DE HASH CRIPTOGRÁFICO

SOLUÇÃO DE UM DESAFIO

PROOF-OF-WORK

DWORK E NAOR, 1992

CONTRA SPAM

UTILIZA FUNÇÕES DE HASH CRIPTOGRÁFICO

SOLUÇÃO DE UM DESAFIO

BITCOIN UTILIZA SHA-256

Vamos supor um sistema
que somente aceite
mensagens cujo hash
SHA-256 do cabeçalho
comece com 24 bits zero,
ou 6 zeros hexadecimais.

DADO

```
pataca:0
```

VALOR DE HASH SHA-256

```
3195ca2e65fb47dd5c66f6ea57e9619e
1ae74a37e634a94686ff1ea230c27909
```

DADO

```
pataca:0
```

VALOR DE HASH SHA-256

```
3195ca2e65fb47dd5c66f6ea57e9619e
1ae74a37e634a94686ff1ea230c27909
```

DADO

```
pataca:27156202
```

VALOR DE HASH SHA-256

```
000000163856a42ed2c6216f14a71395
c542f69dd36c6e37dfee0a1299da1111
```

BLOCKCHAIN

cadeia de blocos

CONTEÚDO DO BLOCO BITCOIN

Hash do bloco anterior
Transações
Nonce
etc.

BLOCKCHAIN

cadeia de blocos

ethereum

Blockchain programável

https://ethereum.org/

MOTIVAÇÃO

OBJETIVO

CRIAR UM SISTEMA
QUE GERENCIE E INTEGRE
ECONOMIAS LOCAIS,
POSSIBILITANDO TRANSACIONAR
VALORES ENTRE ELAS UTILIZANDO
UM MEIO DE TROCA COMUM.

PATACA

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

um trabalho de **Ricardo Macedo** sob a orientação do **Prof. Flávio Soares (IME-USP)** e **Prof. Gilson Schwartz (ECA-USP)**

Pataca é um sistema que gerencia moedas sociais, cujo valor pode estar atrelado a um lastro em bitcoin.

Escrito em Python.
Completamente modular.

Twisted Matrix Comunicação com a rede
SQLAlchemy Mapeamento objeto-relacional

CARACTERÍSTICAS

Uma API extensível que trafega JSON, com:

- ✓ Controle de perfis de usuário
- ✓ Criação e manipulação de contas-correntes
- ✓ Módulos
- ✓ Mapeamento automático de classes em tabelas no banco de dados
- ✓ Comunicação entre servidores Pataca

EXEMPLO DE USO:
POST /

```
Authorization: Token 4cc78bab-0ff0-42e9-a70d-4ceaaa0ab023
Content-Type: application/json

{
   “op”: “transferFunds”,
   “orig”: “bob”,
   “dest”: “alice”,
   “amount”: 300,
   “description”: “Payment
      for kitchen table”
}
```

RESPOSTA:

```
{ “success”: 1 }
```

COMO CRIAR UMA CHAMADA DE API

SETTINGS.PY

```
import requests

uri = ‘’

operations = [
              operation(‘transferFunds’,
                        requests.transfer_funds),
              operation(‘createUser’,
                        requests.create_user),
              …
             ]
```

PROTOCOLO PATACA

- ✓ Possibilita a transferência de valores entre instâncias do Pataca
- ✓ Federação (conta@hostdoservidor.com)
- ✓ Taxa de câmbio baseada no estoque de criptomoeda ou em um valor informado.

Vamos supor que Alberto possua uma conta, em botões, nas Organizações Foo e queira transferir 500 botões para Bernardo, que possui uma conta em estalecas no Bar Bar.

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*.

PRÓXIMOS PASSOS

- ✓ Interfaces gráficas (web, Android, iOS, etc.)
- ✓ Implementar um repositório de módulos (como Play Store, App Store)
- ✓ Adicionar Stellar como lastro
- ✓ Intercâmbio de valores sem lastro

PRÓXIMOS PASSOS

- ✓ Interfaces gráficas (web, Android, iOS, etc.)
- ✓ Implementar um repositório de módulos (como Play Store, App Store)
- ✓ Adicionar Stellar como lastro
- ✓ Intercâmbio de valores sem lastro

STELLAR

Não é baseado em proof-of-work, mas em consenso.

https://www.stellar.org/

USOS

- ✓ Gerenciador de contas em jogos e aplicações
- ✓ Criação de economias temporárias em eventos, cursos, comunidades, etc.
- ✓ Realização de micropagamentos locais
- ✓ Gerenciamento de dinheiro coletivo (grupos, turmas, famílias, etc.)

DÚVIDAS?
TRAUMAS?
QUESTIONAMENTOS?

Não hesite em perguntar.

SIGA O PATACA
NO TWITTER
@gopataca

apoio

MERCADO BITCOIN.NET