

Simplificando o Bitcoin

por Fernando Paladini

Sobre mim



- Faz ciência da computação na UFSC, 4º semestre.
- É desenvolvedor web (Ruby on Rails e Java, um pouco de NodeJS, Python e C++, , etc.).
- Teve projetos relacionados ao Bitcoin e também a ciência.
- Adora novas tecnologias.
- Ama a ciência.

Instituto Bitcoin



Pilares do Instituto Bitcoin:

- Promover
- Proteger
- Padronizar

Tanto Bitcoin, como criptomoedas.

Bitcoin Brasil Desenvolvedores



Incentivo e criação de projetos
relacionados ao Bitcoin.

Todos os projetos:

- Open-source
- Sem fins lucrativos

www.github.com/btcbrdev/



O que nós já sabemos sobre o Bitcoin

Bitcoin



Open Source

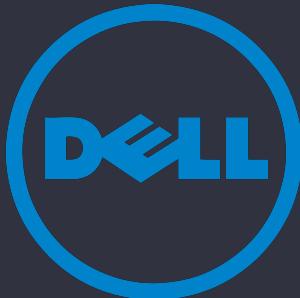


Descentralizado



Gratis

O que é possível fazer com o Bitcoin?



Compras!



Doações!

Wikimedia

LibreOffice

GIMP

VideoLan

Sea Shepard

Archive.org

Wikileaks

Mozilla

GNOME

Guardar!

Guardar e proteger o seu dinheiro da inflação.

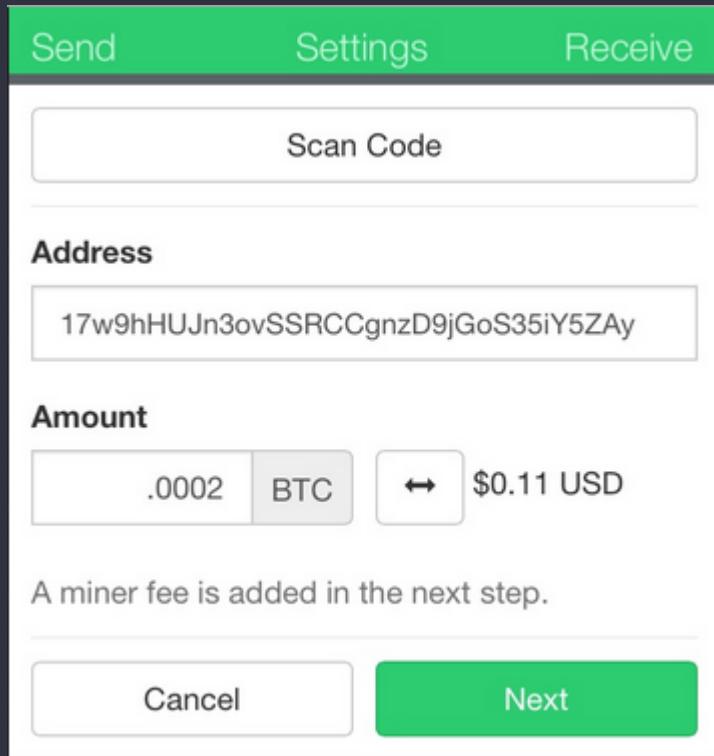
Investir!

É possível emprestar bitcoins a taxas de juros.

Remessas internacionais!
Enviar dinheiro para o outro lado do mundo em minutos.

Como usar o Bitcoin?

1. Baixar uma carteira Bitcoin.
 2. Obter bitcoins de alguma maneira.
- Enviar bitcoins: digitar endereço e quantidade.
- Receber bitcoins: passar o seu endereço bitcoin ao interessado.



Como usar o Bitcoin?

O Bitcoin é um protocolo e por isso pode ser implementado em praticamente qualquer dispositivo. Existem carteiras bitcoin em:



Desktop



Web

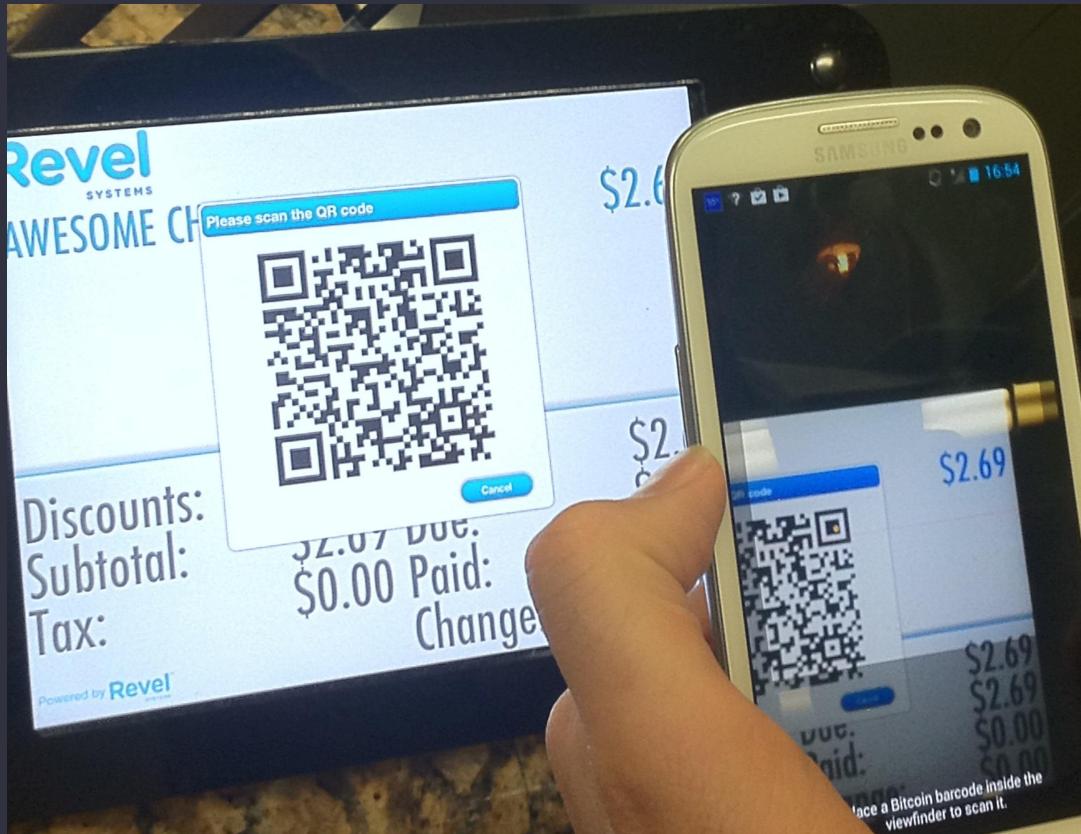


Mobile



Papel

Como usar o Bitcoin?





O que nós **NÃO** sabemos sobre o Bitcoin

Ao invés de explicar o que é Bitcoin, vamos criar algo parecido com o que o Bitcoin faz

Sim, iremos [reinventar](#) o Bitcoin

Vamos imaginar que estamos jogando
Banco Imobiliário



Nele temos algumas propriedades (casas e hotéis):





Mas temos um problema!
“Alguém” perdeu o dinheiro do jogo

Temos que criar algo que nos permita comprar propriedades e pagar taxas (aluguéis, "Revés"). Precisamos de algo que todos nós concordamos que tem valor

Em outras palavras, precisamos de uma moeda

Precisamos de uma moeda facilmente comerciável e que
não possa ser falsificada, por isso vamos evitar o
dinheiro em espécie (papel)

A solução é especificar um saldo para todos os jogadores no começo do jogo, anotá-lo em um caderno e ir atualizando-o com o tempo

Ana 100 moedas

Gabriel 100 moedas

Lucas 100 moedas

Josikwylkson 100 moedas

Chamamos essa lista de saldos de **livro-razão** ou
apenas **registro**. O termo original é *ledger*.

O Registro é a “Lei”. Uma conta tem o saldo que o Registro diz que ela tem. Sem choro.

Se tivermos um jogo com 20 ou 30 pessoas, quem será o responsável por controlar o Registro?

Essa pessoa tem que ser confiável.

Essa pessoa pode ser eu. Você deixa?

Se eu ficar responsável pelo Registro, posso roubar e dizer que tenho 20 moedas a mais.

Centralizar o Registro ou a economia do nosso jogo em
uma pessoa ou entidade **não é uma boa ideia.**

Então que tal dar para todo mundo um caderno com uma cópia do Registro? Quando uma alteração for feita, ela deve ser propagada entre todos as cópias do Registro.

Registro da Ana

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Gabriel

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Josik

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Lucas

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Parece bom.
Agora vamos começar o jogo...

A Ana compra uma casa do Lucas por 5 unidades e
atualiza o Registro dela.

Registro da Ana

| | |
|--------------|------------|
| Ana | 95 moedas |
| Gabriel | 100 moedas |
| Lucas | 105 moedas |
| Josikwylkson | 100 moedas |

Registro do Gabriel

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Josik

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Lucas

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Então ela diz:

“Ei seus usuários de Windows, atualizem essa merda”

A problem has been detected and Windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, Datestamp 3d6dd67c

Registro da Ana

| | |
|--------------|------------|
| Ana | 95 moedas |
| Gabriel | 100 moedas |
| Lucas | 105 moedas |
| Josikwylkson | 100 moedas |

Registro do Gabriel

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Josik

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |

Registro do Lucas

| | |
|--------------|------------|
| Ana | 100 moedas |
| Gabriel | 100 moedas |
| Lucas | 100 moedas |
| Josikwylkson | 100 moedas |



Registro da Ana

| | |
|--------------|------------|
| Ana | 95 moedas |
| Gabriel | 100 moedas |
| Lucas | 105 moedas |
| Josikwylkson | 100 moedas |

Registro do Gabriel

| | |
|--------------|------------|
| Ana | 95 moedas |
| Gabriel | 100 moedas |
| Lucas | 105 moedas |
| Josikwylkson | 100 moedas |



Registro do Josik

| | |
|--------------|------------|
| Ana | 95 moedas |
| Gabriel | 100 moedas |
| Lucas | 105 moedas |
| Josikwylkson | 100 moedas |



Registro do Lucas

| | |
|--------------|------------|
| Ana | 95 moedas |
| Gabriel | 100 moedas |
| Lucas | 105 moedas |
| Josikwylkson | 100 moedas |

Agora todo mundo tem o Registro atualizado.

Mas espere, temos problemas!

A Ana comprou uma casa do Lucas por 5 unidades.

Ana e Lucas tem o registro atualizado.

Gabriel e Josik não tem o registro atualizado.

Se o Lucas caminhar até o Gabriel para mostrar a
atualização **a ser feita no Registro dele**, como o Gabriel vai
saber se a Ana realmente autorizou essa transação?

Registro da Ana

Ana 95 moedas
Gabriel 100 moedas
Lucas 105 moedas
Josikwylkson 100 moedas



| De | Para | Quantidade | Assinatura | Data |
|-----|-------|------------|--------------|----------------------|
| Ana | Lucas | 5 moedas | Ana Fagundes | 25/05/2014 13:22:30s |

Então o problema foi resolvido, mas temos
mais um problema a ser resolvido.

E se o jogo tivesse 30 ou 40 pessoas, como poderíamos
atualizar o Registro de **todas** essas pessoas sempre
que uma transação fosse realizada?

Como poderíamos sincronizar esses Registros de papel?

Não poderíamos. E aí que a computação entra.

Podemos mover os saldos para um Registro digital, utilizar um software para sincronizar esses dados entre todo mundo do jogo. Podemos utilizar também uma matemática que garanta que só eu possa gastar o meu dinheiro e que as assinaturas digitais de cada transação não sejam esquecidas.



E bem, é isso que o [Protocolo Bitcoin](#) (basicamente) faz.

No Bitcoin, ao invés de identificar uma conta pelo número ou pelo nome do dono, as contas são identificadas por um identificador alfanumérico.

Por exemplo:

1KCFS9Td2c8PVF31h9N5r2zz6AVgTX9GRq

Isso torna o Bitcoin “anônimo”.

Cada conta é chamada de **endereço**.
O número de endereços possíveis é limitado.

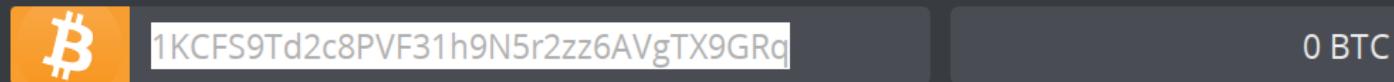
Existem 2^{160} endereços Bitcoin possíveis.

$$2^{160} = 1,461,501,637,330,902,918,203,684,
832,716,283,019,655,932,542,976$$

Isso é maior que o número de estrelas no Universo.
É, você pode ter quantos endereços Bitcoin você quiser.

No Bitcoin, cada movimentação de saldo é registrada e chamada de [transação](#). Todas as transações ficam disponíveis publicamente no [Blockchain](#).

BITCOIN ADDRESS



Overview Transactions 4 Mentions 0 Export ▾

| 1 |
|---|
|---|

| | | |
|--|---------------|--------------------|
| 0.27050811 BTC | > 4 addresses | 4.1K CONFIRMATIONS |
| 2555e3f3123ed6ec8a367be9eac137c8e8979b6f73a5ef23410364be9421bdcf | | |
| Tuesday, February 3rd 2015, 6:31:18 • 27 days 4 hours ago • 6 inputs • 4 outputs • 4 spent | | |

| | | |
|--|--------------------------------------|--------------------|
| 0.27050811 BTC | < 12RZE3EXnzjcydQkhHX3pLriLxSEH9xpM6 | 4.1K CONFIRMATIONS |
| 857bf07d9f10446e5342051fd4e7e7920a3c463f70af071ba14083d7d299accc | | |
| Tuesday, February 3rd 2015, 3:39:32 • 27 days 7 hours ago • 1 inputs • 2 outputs • 2 spent | | |

| | | |
|--|---------------|--------------------|
| 0.88569643 BTC | > 5 addresses | 6.7K CONFIRMATIONS |
| 96db8a9a749b63052a8b507faf48d3c27814d411295c839bc33c0aa30f1f2f1c | | |
| Thursday, January 15th 2015, 17:10:48 • 1 month 15 days ago • 4 inputs • 5 outputs • 5 spent | | |

Isso caracteriza o Bitcoin como um sistema de pagamentos.

Em suma, o melhor sistema de pagamentos do mundo.
A forma perfeita de dinheiro, segundo (alguns) economistas.

Transferência Internacional (Brasil p/ China)

R\$10.000

Moeda FIAT (Dólar, Real):

- Entre 2 e 4 dias.
- Taxas que variam de 5% a 10%.
- Dar todos os seus dados para um intermediário.

O que chegou (melhor cenário):

R\$9.500,00

Bitcoin:

- 10 minutos.
- Taxa de R\$0,04 (0,0001 btc).
- Transação direta e “anônima”.

O que chegou (todos os cenários):

R\$9.999,96

O Bitcoin é quase pureza com paçoca, é fenomenal.

Cada endereço Bitcoin possui um saldo. Esse saldo existe através de moedas chamadas bitcoins e que possuem um valor. Logo, o Bitcoin também é uma moeda.

Assim como o ouro, o Bitcoin é global, de forma que ele pode ser comprado e vendido em qualquer país do mundo.

Existirão ao todo 21 milhões de bitcoins que são liberados de forma previsível em um processo chamado mineração. O último bitcoin será minerado em 2140.

Resumindo o *bitcoinês*:

Bitcoin = o sistema Bitcoin como um todo (protocolo, tecnologia).

bitcoin = unidade de moeda (ex: 1 bitcoin, 2.543 bitcoins).

endereço bitcoin = uma conta

transação = uma transferência de bitcoins entre contas.

Blockchain = um registro público com todas as transações da história.

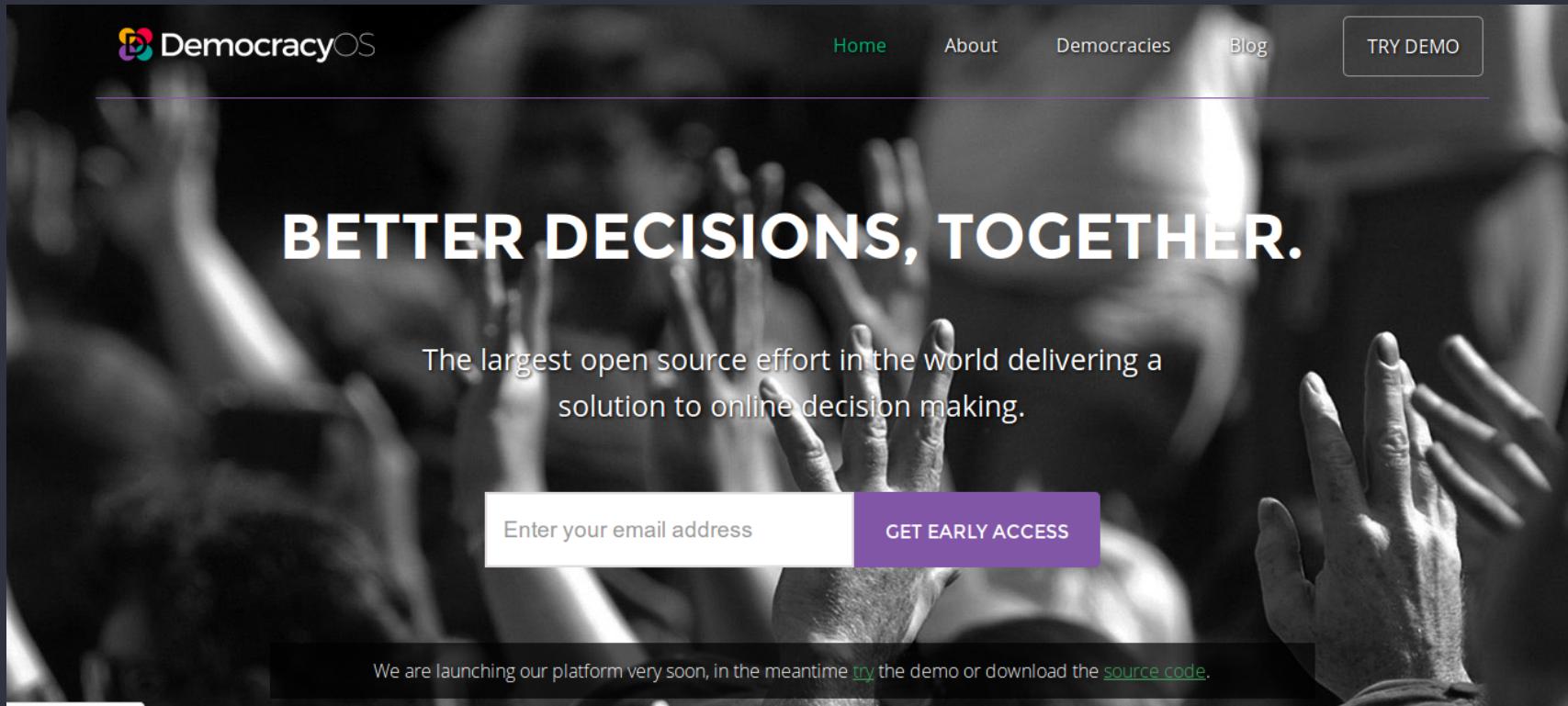
mineração = processo que vai liberando mais bitcoins na rede a uma taxa previsível. É uma recompensa da Rede Bitcoin por deixar o computador processando informações importantes para o sistema.



Por que o Bitcoin pode impulsionar o open-source e
consequentemente o software-livre?

O Bitcoin solucionou vários problemas e permitiu, pela primeira vez, a reprodução de bens escassos no meio digital de forma descentralizada.

DemocracyOS: Democracia real e verificável



The DemocracyOS website features a dark background with a central image of numerous hands reaching upwards, symbolizing participation and democracy. The logo "DemocracyOS" is in the top left corner, with "Democracy" in blue and "OS" in green. The top navigation bar includes "Home" (highlighted in green), "About", "Democracies", "Blog", and a "TRY DEMO" button.

BETTER DECISIONS, TOGETHER.

The largest open source effort in the world delivering a solution to online decision making.

Enter your email address [GET EARLY ACCESS](#)

We are launching our platform very soon, in the meantime [try](#) the demo or download the [source code](#).

Storj.io: Cloud descentralizada

[APPS](#)[BLOG](#)[FORUM](#)[FAQ](#)[EARLY ACCESS](#)

Decentralized Cloud Storage

Storj is based on blockchain technology and peer-to-peer protocols to provide the most secure, private, and encrypted cloud storage.

[GET UPDATES](#)

*We will never share, rent, or sell your email address to anyone, ever.

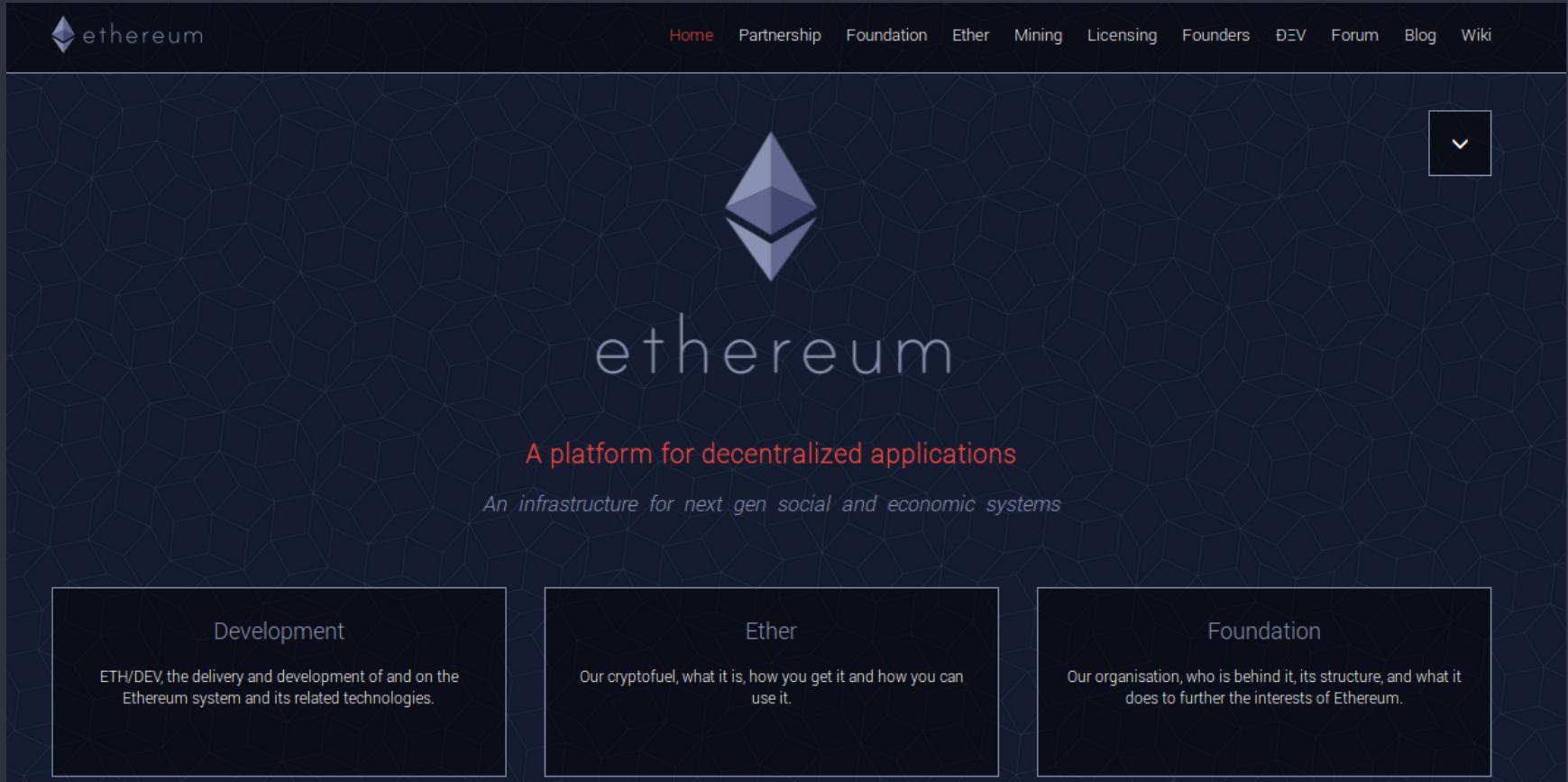


BitNation: governança descentralizada

ABOUT • SERVICES • INVEST • FAQ • CONTACT • TEAM • COMMUNITY • AMBASSADOR NETWORK

BITNATION
GOVERNANCE 2.0

Ethereum: apps descentralizados



The image shows the Ethereum homepage. At the top left is the Ethereum logo. A navigation bar at the top right includes links for Home, Partnership, Foundation, Ether, Mining, Licensing, Founders, DEV, Forum, Blog, and Wiki. The central feature is the Ethereum logo (a purple hexagon with a white triangle) and the word "ethereum" in lowercase. Below this is a subtext: "A platform for decentralized applications" and "An infrastructure for next gen social and economic systems". Three callout boxes at the bottom provide links to "Development", "Ether", and "Foundation".

Development
ETH/DEV, the delivery and development of and on the Ethereum system and its related technologies.

Ether
Our cryptofuel, what it is, how you get it and how you can use it.

Foundation
Our organisation, who is behind it, its structure, and what it does to further the interests of Ethereum.

“Eu penso que o Bitcoin é o primeiro [dinheiro encriptado] que tem o potencial de fazer alguma coisa como mudar o mundo.”

(Peter Thiel, fundador do Paypal)

Slides licenciados sob:



Mais informações? Ficou interessado? Tem alguma dúvida?



github.com/paladini
facebook.com/nandopaladini
fernando.paladini@institutobitcoin.org