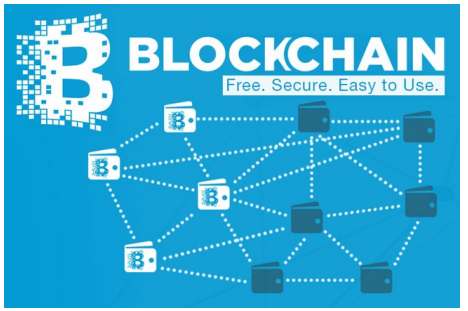
Blockchain, Bitcoin etcetera: separando a realidade do exagero

Jeroen (Jerom) van de Graaf
Departamento de Ciência da Computação

INSCRYPT

UFMG

Programa hoje



- Blockchain
- Bitcoin
- Bitcoin é dinheiro?
- Aplicações de blockchain
- Ethereum, dapps, smart contracts
- ICOs

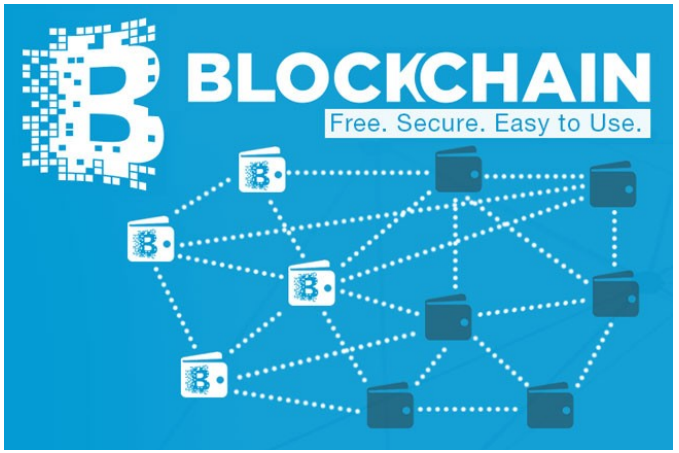
bitcoin

Satoshi Nakamoto fez duas invenções

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



bitcoin

Explicando o blockchain: cartório convencional

Carimbo de tempo em documentos

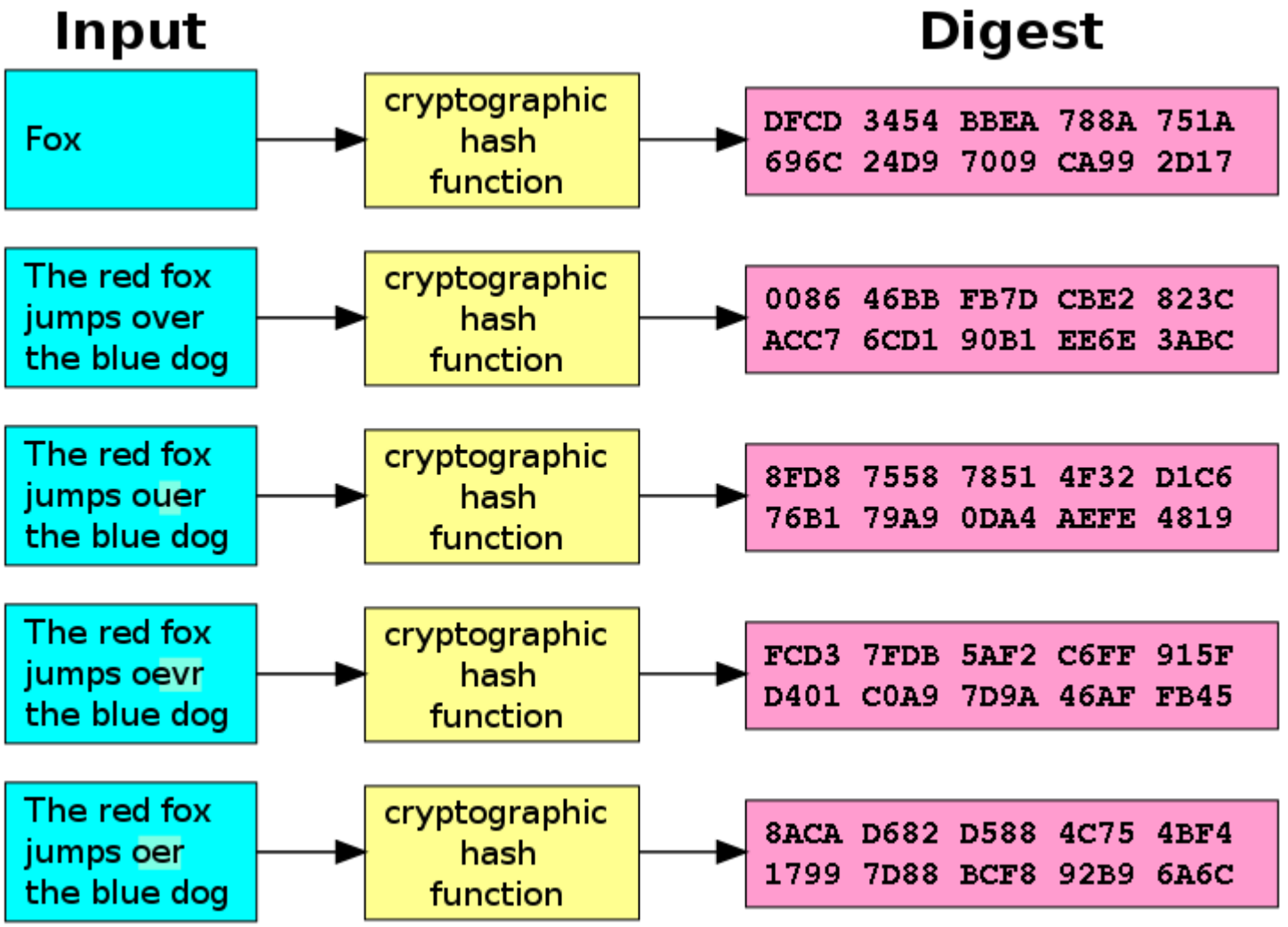
- Data e hora
- Assinatura

Ingredientes para um cartório online

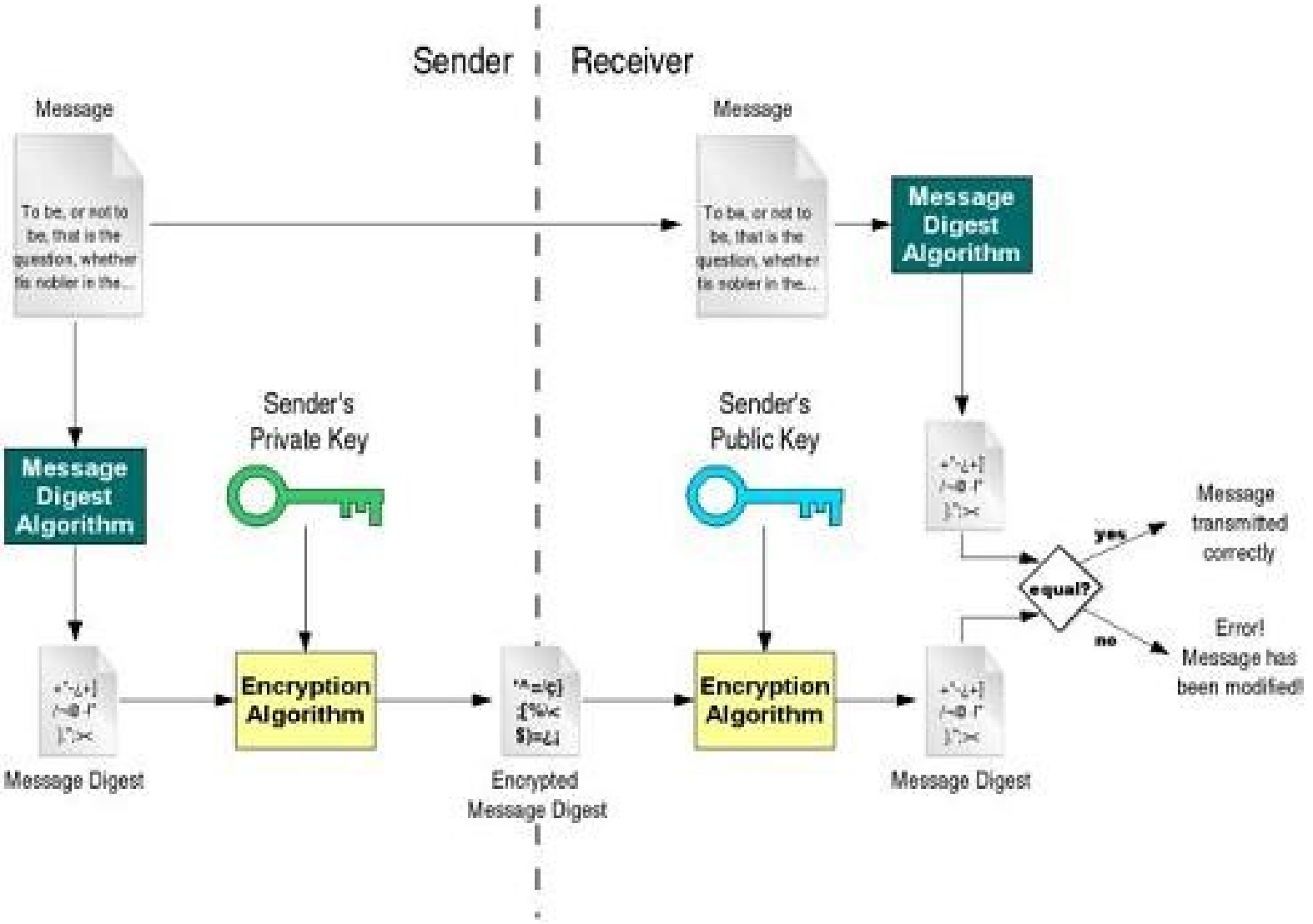
Carimbo de tempo em documentos

- Data e hora
  - Em breve
- Assinatura
  - Função de hash criptográfica
  - Criptografia com chave pública

Função de hash criptográfico *(MD5=RIP, SHA1)*



Criptografia com chave pública e assinatura digital

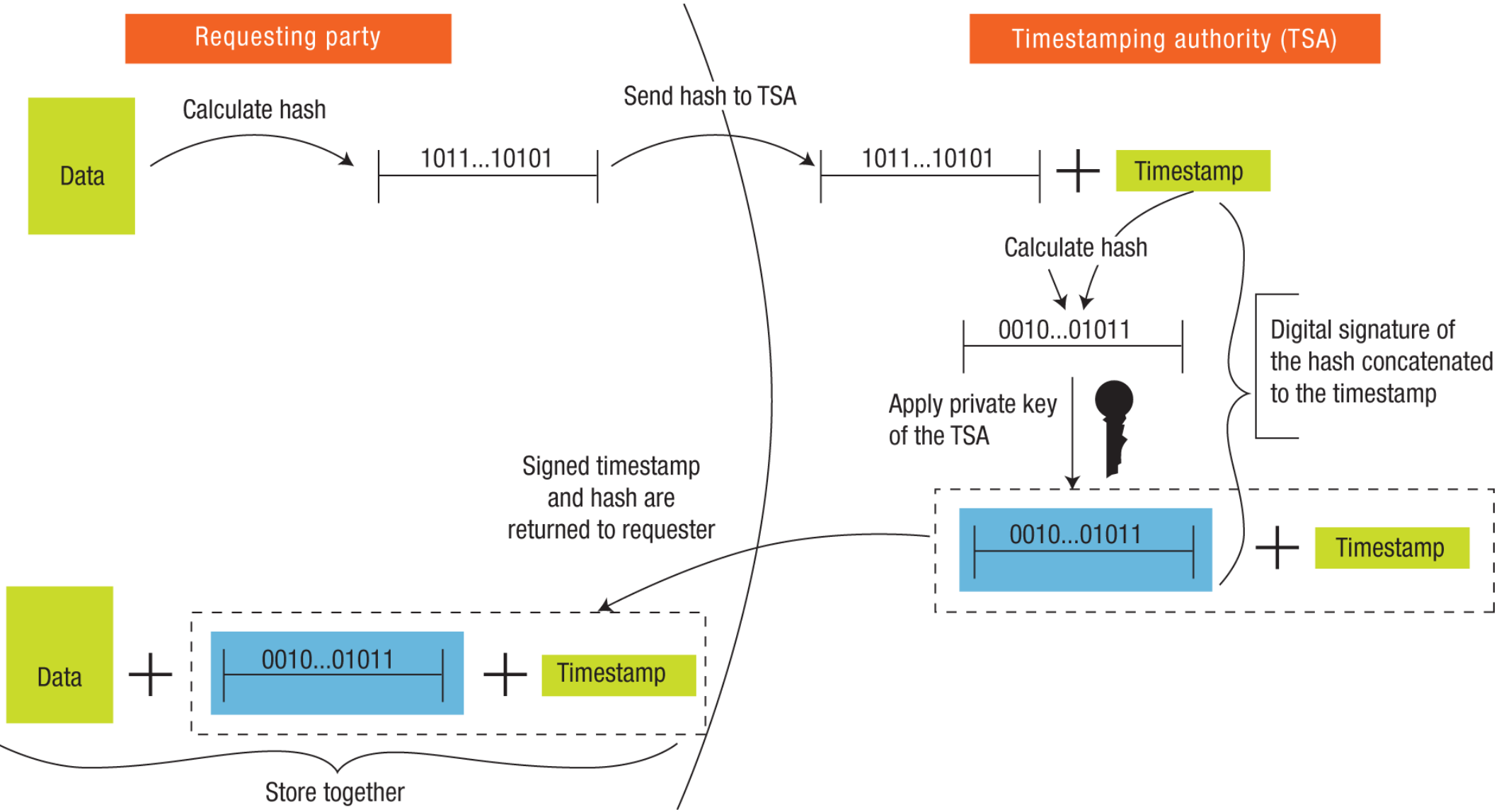


Ingredientes para um log seguro

Carimbo de tempo em documentos

- Data e hora : de onde?
  - Log seguro = tempo sequencial
  - Próprio computador? Não é confiável
  - Autoridade de Carimbo de Tempo
- Assinatura digital

Autoridade de Carimbo de Tempo



Registro seguro com uma cadeia de hash

→ O registro é protegido usando uma função hash H

$$\underbrace{entrada[n-1] + hash[n-2]}$$

$$\underbrace{entrada[n] + hash[n-1]}$$

$$\underbrace{entrada[n+1] + hash[n]}$$

→ Qualquer modificação do log será detectada

O log seguro distribuido

- Imagine um serviço de log seguro
  - Na internet
  - Peer-to-peer
  - Distribuido
  - Completamente transparente

→ **BLOCK CHAIN**

Blockchain

Um blockchain é um serviço de log seguro

– distribuido --- não tem dono

– transparente --- cada entrada é rastreável

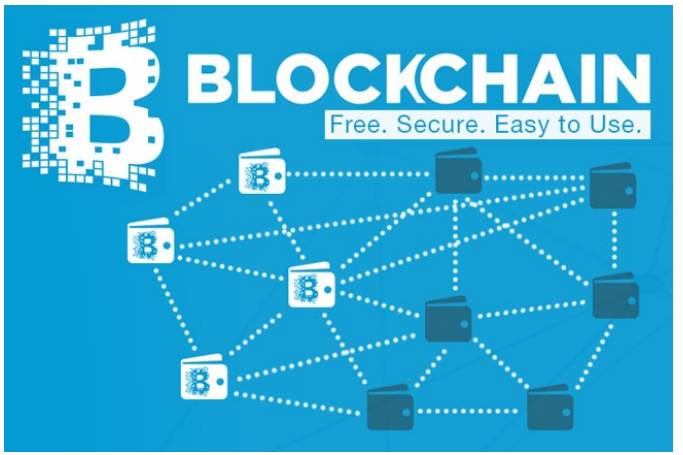
– confiável --- 24x7

Exemplos

– Bitcoin

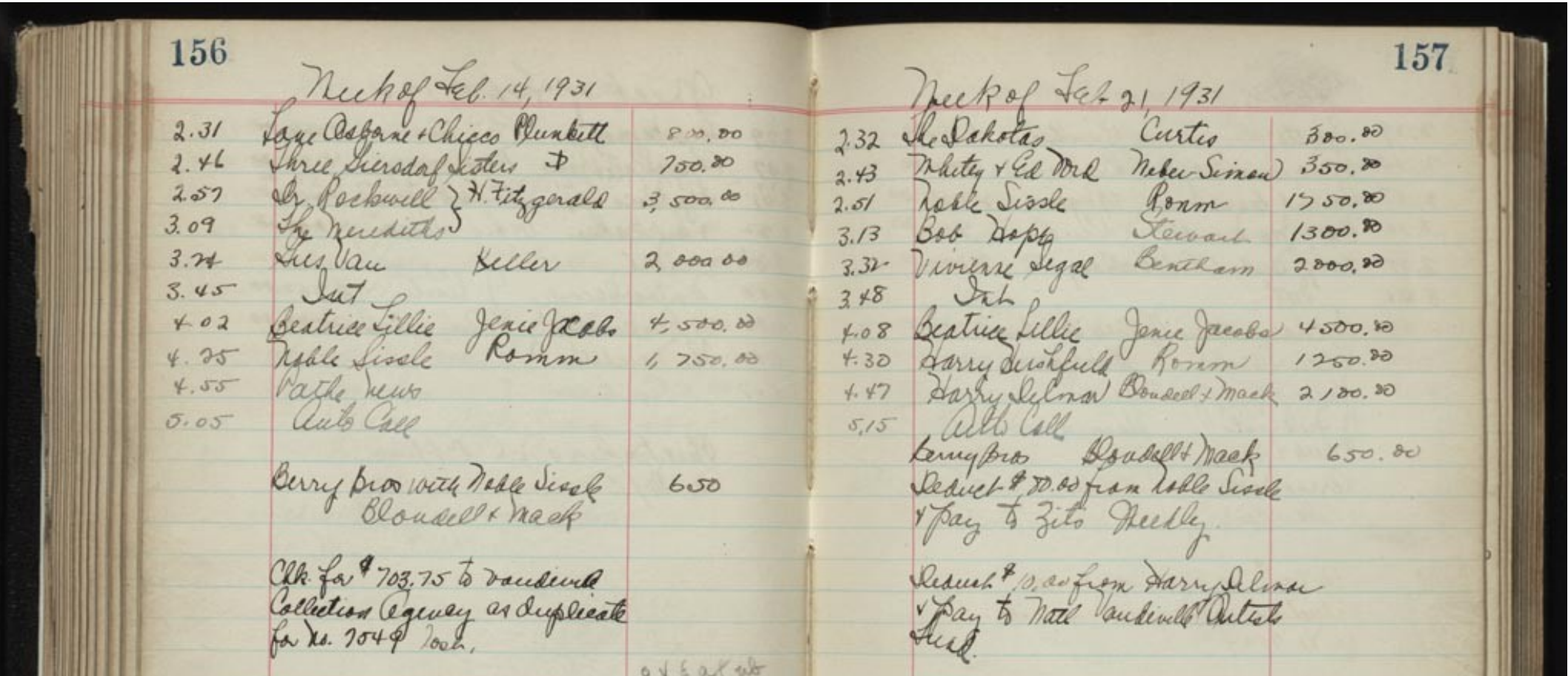
– Ethereum

– Hyperledger



Blockchain = *virtual ledger*

Para manter eventos, documentos, transações temos artefatos como registros, cadastros, cadernos, livros-caixa, diários de bordo, jornais, logs, **livros-razão** = *ledger* → *Distributed Ledger Technology*



Aplicações do blockchain

* Rastreamento de documentos (cartório)
* Rastreamento de transações (cartório)
* Rastreamento de bens (logística, diamantes, madeira amazônica)

Aplicações do blockchain

* Rastreamento de documentos (cartório)
* Rastreamento de transações (cartório)
* Rastreamento de bens (logística, diamantes)
* *Rastreamento de transferências financeiras*

    → *Bitcoin, Ethereum e outras cripto-moedas*

O que é bitcoin???

não é: como funciona bitcoin

Passei parte das minhas férias jogando poker com um colega e nossos filhos

O que é bitcoin???

Usamos feijões para apostar

Podríamos ter usado outros objetos: fósforos, contas, pedrinhas, ….

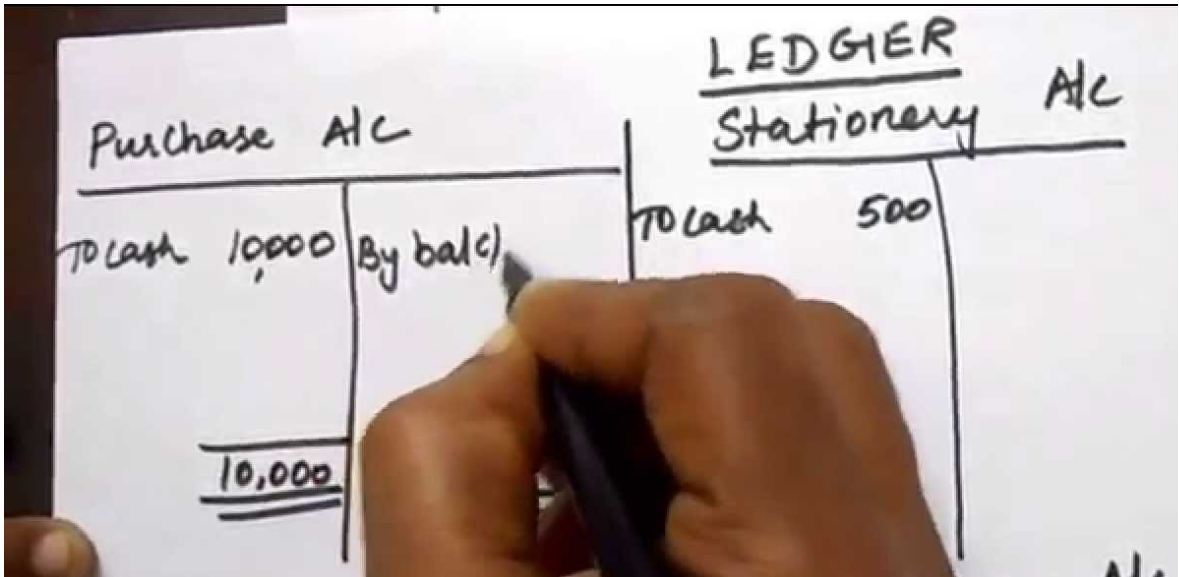
(fichas têm denominação diferentes)

O Livro-feijão

ENTRA A TECNOLOGIA DA INFORMAÇÃO

(1) ao em vez de trocar os feijões fisicamente, anotamos num caderno quem paga quanto feijões a quem

Um livro-caixa de feijões – um Livro-Feijão.



O Feijão Virtual

ENTRA A TECNOLOGIA DA INFORMAÇÃO

(2) Vamos implementar esse Livro-Feijão em software, desenvolvido e mantido por uma autoridade central de confiança, chamada o **Central de Transações de Feijões**.

Agora podemos dividir um Feijão em miliFeijões, microFeijões e nanoFeijões (modestamente batizado de "Jeroen" :-).

Assim criamos o **Feijão Virtual**.

Eliminar a central confiável

ENTRA A CRIPTOGRAFIA

(3) Agora queremos eliminar aquela Central de Transações de Feijões, em que toda parte precisa confiar e portanto o ponto fraco do sistema.

–- Teremos um exército de centenas de Mini-Validadores de Transações de Feijões,

–- trabalhando de forma distribuída numa rede *peer-to-peer*.

Propriedades do crypto-feijão

A CRIPTOGRAFIA GARANTE

-- a integridade das transações no Livro-Feijão;

-- a autenticidade das transações provenientes das partes (através de assinaturas digitais);

-- o controle sobre a quantidade total dos CryptoFeijões;

-- a pseudonimidade das participantes;

-- o consenso entre os Mini-Validores;

-- um pagamento (taxa) para os Mini-Validadores para o trabalho de validação (os Mini-Validadores são chamados de mineradores).

O crypto-feijão versus o bitcoin

-- conceitualmente Bitcoin e Crypto-Feijão são idênticos

-- Bitcoin não tem valor intrínseco;

-- Bitcoin ganhou valor no mercado Silk Road, fechado pelo FBI em 2013;

-- Bitcoin não é dinheiro mas um objeto de troca

– Na Holanda, bitcoin é tratado como um metal precioso

Blockchain : questões

* Quem mantém o serviço no ar?
  - Voluntários
  - Partes interessadas
    - Blockchain federado
    - Blockchain proprietário
  - Indivíduos que ganham com isso
* Como chegar a um consenso num ambiente distribuido?
  - Será respondido em breve

Um banco mantém um livro-caixa

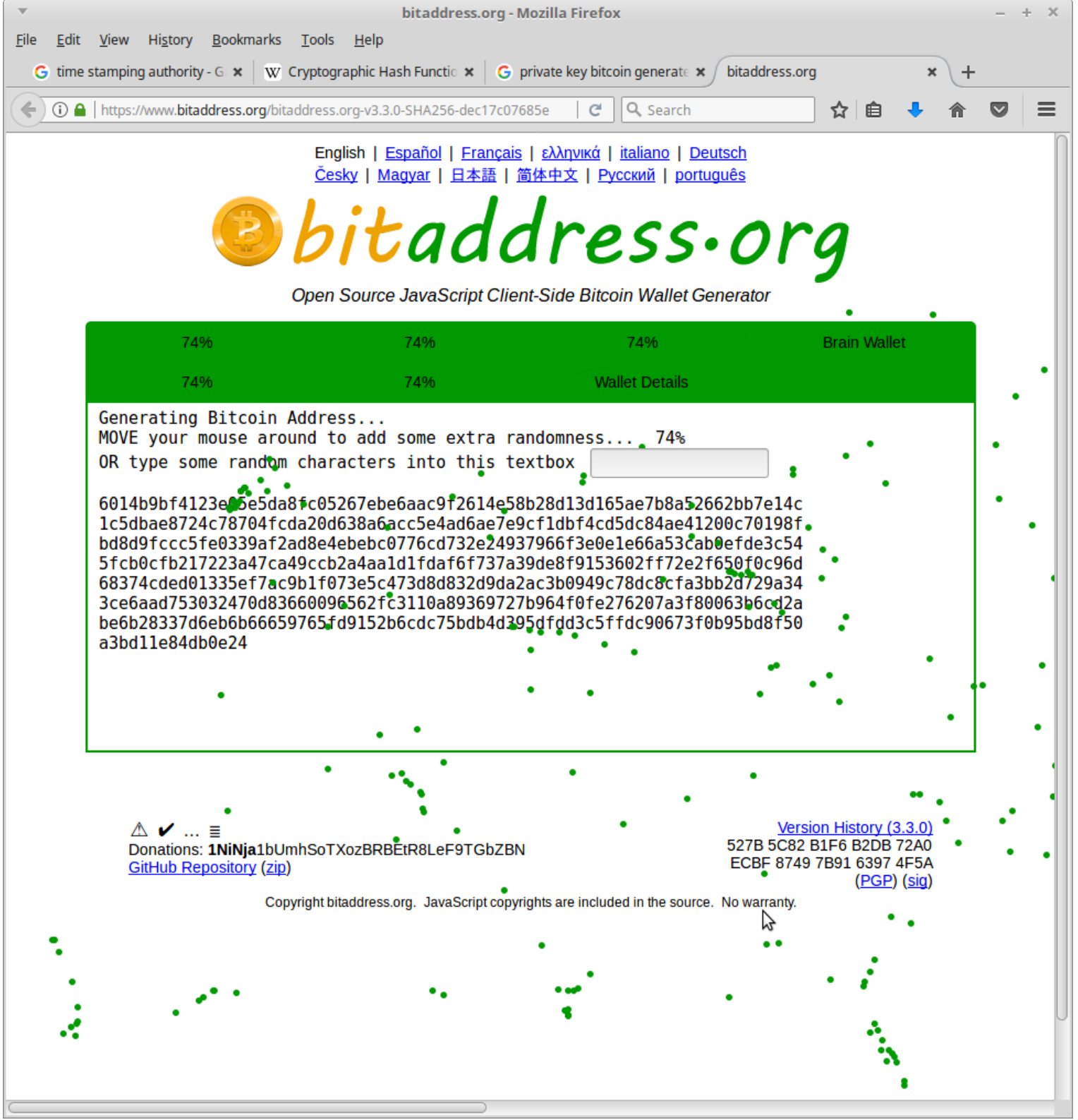
- Número de conta
- Valor associado a cada conta
- Transferências entre contas:
  - Subtrai 51 créditos de conta #1
  - Adiciona 50 créditos a conta #2
  - O custo da desta transação é 1 crédito

Bitcoin implementa um banco virtual, substituindo o banco por um blockchain

Bitcoin

Número de conta = bitcoin address = chave pública

- Na verdade, é o hash da chave pública


bitaddress.org - Mozilla Firefox
File Edit View History Bookmarks Tools Help
time stamping authority - G
Cryptographic Hash Functic
private key bitcoin generate
bitaddress.org
https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e
Search
English | Español | Français | ελληνικά | italiano | Deutsch
Česky | Magyar | 日本語 | 简体中文 | Русский | português
bitaddress.org
Open Source JavaScript Client-Side Bitcoin Wallet Generator
74% 74% 74% Brain Wallet
74% 74% Wallet Details
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness... 74%
OR type some random characters into this textbox
6014b9bf4123e[illegible]5e5da8fc05267ebe6aac9f2614e58b28d13d165ae7b8a52662bb7e14c
1c5dbae8724c78704fcda20d638a6acc5e4ad6ae7e9cf1dbf4cd5dc84ae41200c70198f
bd8d9fccc5fe0339af2ad8e4ebebc0776cd732e24937966f3e0e1e66a53cab0efde3c54
5fcb0cfb217223a47ca49ccb2a4aa1d1fdaf6f737a39de8f9153602ff72e2f650f0c96d
68374cded01335ef7ac9b1f073e5c473d8d832d9da2ac3b0949c78dc8cfa3bb2d729a34
3ce6aad753032470d83660096562fc3110a89369727b964f0fe276207a3f80063b6cd2a
be6b28337d6eb6b66659765fd9152b6cdc75bdb4d395dfdd3c5ffdc90673f0b95bd8f50
a3bd11e84db0e24
Donations: 1NiNja1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)
Version History (3.3.0)
527B 5C82 B1F6 B2DB 72A0
ECBF 8749 7B91 6397 4F5A
(PGP) (sig)
Copyright bitaddress.org. JavaScript copyrights are included in the source. No warranty.

English | Español | Français | ελληνικά | italiano | Deutsch
Česky | Magyar | 日本語 | 简体中文 | Русский | português

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet
Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address | **Private Key**

SHARE

1JjXK4UiPYxvVQ62sDt7KVqpMQ9AYbTtdu

SECRET

KyBKgcPgojvyreFAuMvFekQemUQ8SrKFNQH9zdDxrg9sjW6YPTD2

A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you are familiar with PGP you can download this all-in-one HTML page and check that you have an authentic version from the author of this site by matching the SHA256 hash of this HTML with the SHA256 hash available in the signed version history document linked on the footer of this site. If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will not be retrievable. Your Bitcoin private key should be kept a secret. Whomever you share the private key with has access to spend all the bitcoins associated with that address. If you print your wallet then store it in a zip lock bag to keep it safe from water. Treat a paper wallet like cash.

Add funds to this wallet by instructing others to send bitcoins to your Bitcoin address.

Check your balance by going to blockchain.info or blockexplorer.com and entering your Bitcoin address.

Spend your bitcoins by going to blockchain.info and sweep the full balance of your private key into your account at their website. You can also spend your funds by downloading one of the popular bitcoin p2p clients and importing your private key to the p2p client wallet. Keep in mind when you import your single key to a bitcoin p2p client and spend funds your key will be bundled with other private keys in the p2p client wallet. When you perform a transaction your change will be sent to another bitcoin address within the p2p client wallet. You must then backup the p2p client wallet and keep it safe as your remaining bitcoins will be stored there. Satoshi advised that one should never delete a wallet

Bitcoin

Número de conta = bitcoin address = chave pública

- Na verdade, é o hash da chave pública

Valor associado a cada conta:

- Ninguem está mantendo o saldo das contas,
- O saldo é deduzido do histórico de todas transações

Transferências entre contas:

- Conta #1 recebeu 75 bitcoins
- Destes, repassa 50 bitcoin para conta #2
- O troco, 25 bitcoins, volta para conta 1
- O custo da desta transação é 0
- Assinada com a chave privada da conta #1

Como se mantém consenso na rede P2P?

– As partes que mantém o blockchain devam resolve um desafio para a versão dela prevalecer

– Os blocos *b[1]…b[n]* a serem incorporados são concatenados com um valor aleatório *R*

– O desafio é: encontrar um valor de R tal que

***SHA256 (b[1]…b[n] | R)* começa com 70 zeros**

– Quem encontrar este *R* primeiro envia ele para todas as outras partes

– As outras abondonam suas tentativas e aceitam esta nova extensão do block chain como verdadeiro.

– Quem ganhou pode se pagar uma pequena taxa →

mineiração de bitcoin

Bitcoin: vantagens

Não tem banco, não tem governo

- Redução de custos
- Impossibilita qualquer politicagem por governos

Altamente acessível:

- Qq pessoa com um smart phone pode entrar e usar
- É somente criar um par de chave pública—chave privada

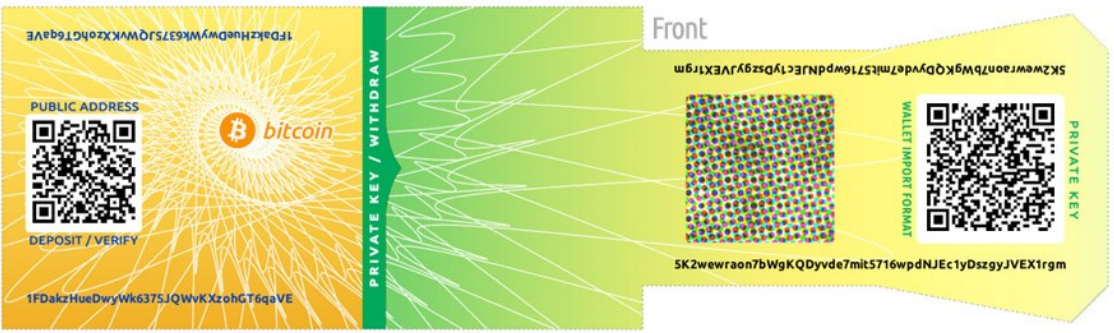
Transferências entre contas são de graça:

- Isso permite pagamentos com valores muito baixo

Bitcoin: desvantagens

Não tem banco, não tem governo

- Não tem regras, não tem proteção
- O próprio usuário é responsável por sua própria segurança
  - Se você perde sua chave privada, você perde (o acesso a) seu dinheiro
  - Existem corretores para cuidar disso
  - Um destes, MountGox, foi hackeado em 2014, causando um prejuizo de US$ 470.000.000 a seus clientes. Quebrou.



Bitcoin: mais desvantagens

- Não tem tanta anonimidade que se pensa
- É meio lerdo
  - 10 minutos
  - Esperar 6 transações ~uma hora

O bitcoin é dinheiro?

Nassif: “Bitcoin é crime contra a economia popular”

Bitcoin é bolha, mas não é pirâmide, por Jeroen van de Graaf

O MUNDO DAS CRIPTOMOEDAS

QUI, 01/02/2018 - 17:28

Bitcoin é bolha, mas não é pirâmide

por Jeroen van de Graaf

Resposta a "As criptomoedas e os crimes contra a economia popular e Salve se das criptomoedas enquanto é tempo por Luis Nassif"

Caro Nassif,

O bitcoin é dinheiro?

A importância de dinheiro é que representa um valor de troca universal.

A humanidade usou vários objetos como dinheiro:

- Metais
- Joias
- Conchas
- Pedras → Yap
- Papel

O bitcoin é dinheiro?

Antes da primeira guerra:

- dinheiro era uma promessa de ouro
- Reserva de ouro = **lastro**

Depois da primeira guerra: **hiper-inflação** em Alemanhã

Padrão de ouro (Bretton-Woods – 1944)

- Todas as moedas ficam dentro de uma margem relativo a o dólar
- O dólar está fixado ao ouro
- Criação do IMF

O bitcoin é dinheiro?

Fiat money

- 1971 – Nixon: desvalorização do dolar
- “Lastro” é a riqueza e o PIB de um país
- “Fiat” = ordem, “que assim seja”

Bitcoin não é dinheiro

- muito volátil
- na Holando bitcoin é um metal precioso
- Quem determina o valor do bitcoin é o mercado

Website
Website 2
Explorer
Explorer 2
Explorer 3
Message Board
Message Board 2
Source Code
Rank 1
Coin Mineable

Market Cap	Volume (24h)	Circulating Supply	Max Supply
$137,134,558,962 USD 16,920,625 BTC	$7,615,790,000 USD 948,979 BTC	16,920,625 BTC	21,000,000 BTC

Charts | Markets | Social | Tools | Historical Data

Bitcoin Charts

Como começou Bitcoin?

– Satoshi Nakamoto foi autor do white paper propondo Bitcoin

– Desenvolveu software para Bitcoin

– Numa primeira transação genesis criou 50 bitcoin em janeiro 2009

– Fez mineiração no valor de

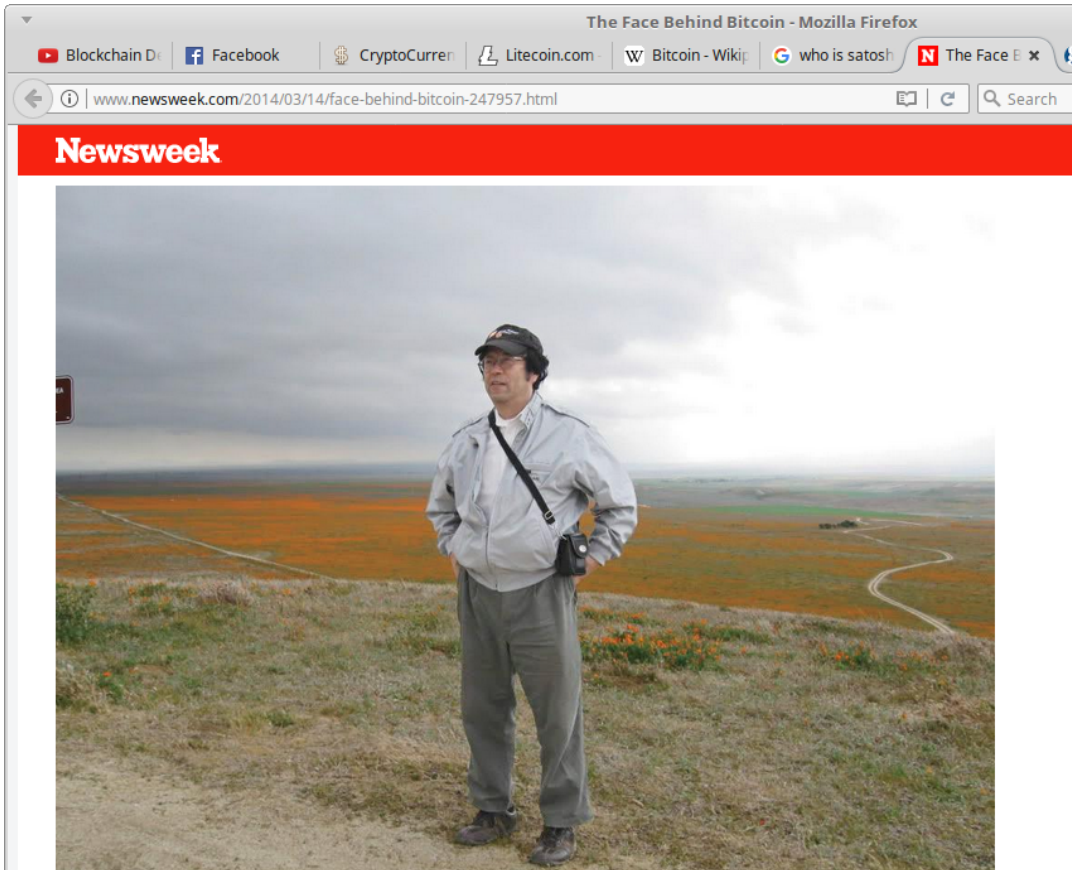
~1.000.000 bitcoin

– Desapareceu!

– Pode sacar o dinheiro?

– É Nick Szabo?

(Banking on Bitcoin – Netflix)



Aplicações do blockchain

* Rastreamento de documentos (cartório)
* Rastreamento de transações (cartório)
* Rastreamento de bens (logística, diamantes)
* Rastreamento de transferências financeiras

    → Bitcoin, Ethereum e outras cripto-moedas

Aplicações do blockchain

* Rastreamento de documentos (cartório)
* Rastreamento de transações (cartório)
* Rastreamento de bens (logística, diamantes)
* Rastreamento de transferências financeiras

    → Bitcoin, Ethereum e outras cripto-moedas

* *Blockchain com inteligência:*

    – *registro confiável*

    – *computação confiável (mas lerdo)*

    – *tempo confiável*

    – *dinheiro confiável*

Scripts e transferência de dinheiro

→ Bitcoin permite coisas de tipo: este pagamento é autorizado se for assinado por no mínimo 2 destas 3 contas

→ Bitcoin permite scripts, mas a linguagem é limitada

Blockchain+ scripts + tempo+cripto-moeda

--Dapps (distributed apps) – Smart contracts

– Tokens; moedas

ethereum

Exemplo de um smart contract

Três partes:

– Concessionário

– Detran

– Comprador

Smart contract:

– *Se pagamento_comprador == 40000 mil reais*:

  – *Transfere dinheiro (bitcoin, ...)*

  – *Transfere propriedade*

  – *Crie nova placa e emite documentos do carro*

ethereum

Como se evite que um programa entra em loop?

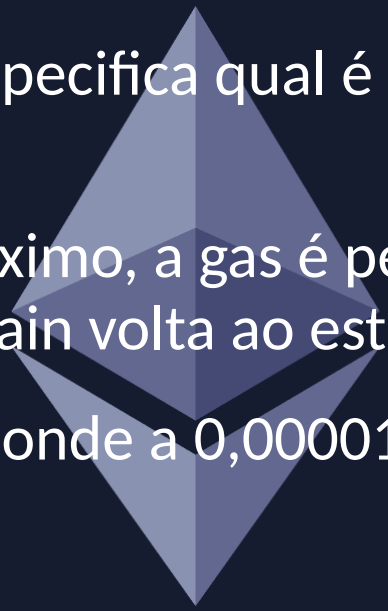
A *Ethereum Vitual Machine* tem conjunto de operações básicas

Cada operação básica custa uma quantidade de gas(olina)

Cada progama submetido especifica qual é o máximo de unidades gas que ele pode custar

Se um programa estoura máximo, a gas é perdida mas as operações serão desfeitas (o blockchain volta ao estado anterior)

Uma unidade de gas corresponde a 0,00001 ETH



ethereum

O que se pode fazer com isso?

→ Implementar as regras para formar em Computação

→ Implementar processos de negocios

- – banco
- – seguros
- – ...

→ Implementar processos de governo

→ Apostar na internet / lotarias

ethereum

O que se pode fazer com isso?

→ Transferir valores entre países

→ Juros altos no Brasil x Juros baixos na Holanda

→ usar Bitcoin para transferir valores

→ Swapy.network:

- – creditores, debitores
- – avaliadores de risco
- – baseado no Ethereum

ethereum

O que se pode fazer com isso?

→ cara/coroa distribuída entre N partes

→ 1a rodada: cada parte *i*

- – escolhe x_i de 256 bits
- – escolhe r_i de 256 bits
- – publica $SHA256(r_i, x_i)$

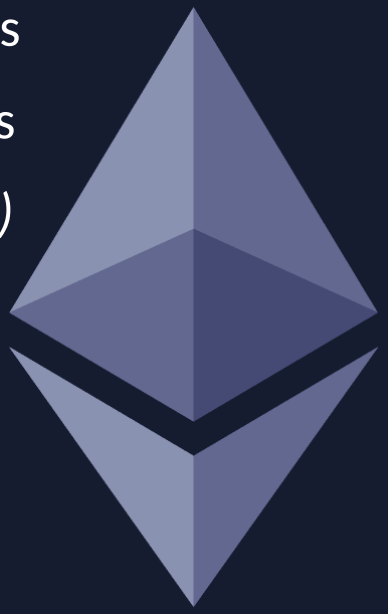
→ 2a rodada: cada parte *i*

- – publica x_i, r_i

→ Resultado: $R = r_1 + r_2 + ... + r_N$

→

→



ethereum

O que se pode fazer com isso?

→ cara/coroa distribuída entre N partes

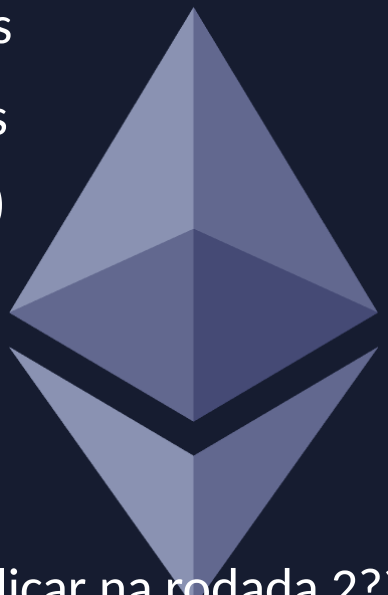
→ 1a rodada: cada parte *i*

- – escolhe x_i de 256 bits
- – escolhe r_i de 256 bits
- – publica $SHA256(r_i, x_i)$

→ 2a rodada: cada parte *i*

- – publica x_i, r_i

→ Resultado: $R = r_1 + r_2 + ... + r_N$



→ E se uma parte se recusa a publicar na rodada 2??

→ Solução: exige um depósito antes de começar, e devolve apenas a quem publica

ethereum

Ethereum é um computador nas nuvens

Ethereum is an **open-source, public, blockchain-based distributed computing platform** featuring **smart contract (scripting) functionality**.

It provides a decentralized **Turing-complete** virtual machine, the **Ethereum Virtual Machine (EVM)**, which can execute scripts using an international network of public nodes.

Ethereum also provides a cryptocurrency token called **"ether"**, which can be transferred between accounts and used to compensate participant nodes for computations performed.

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed **without any possibility of downtime, censorship, fraud or third party interference**.

Como começou Ethereum

- Iniciativa de Vitalik Buterin
- Financiado através de *crowdfunding*
- Dinheiro usado para desenvolver a plataforma
- Começou 30 de julho de 2015.
- Os investidores foram pagos em Ether

The DAO

- ONG / fundo de investimento
- Distributed Autonomous Organization
- Completamente virtual
- Inscrição via crowd funding
- DAO Tokens dão direito de votar nas propostas
    - Como ações de uma empresa
- Todas as regras foram implementadas em cima de Ethereum como programas/scripts

“The code is the contract”

Objetivo: eliminar advogados

O código é o contrato portanto escrever
código se tornou algo importante

No caso do DAO em junho de 2016, um hacker
encontrou um erro na linguagem SOLIDITY e desviou 70 miliões de doláres

Racha na comunidade:

- Temos que corrigir o código e desfazer esta transação

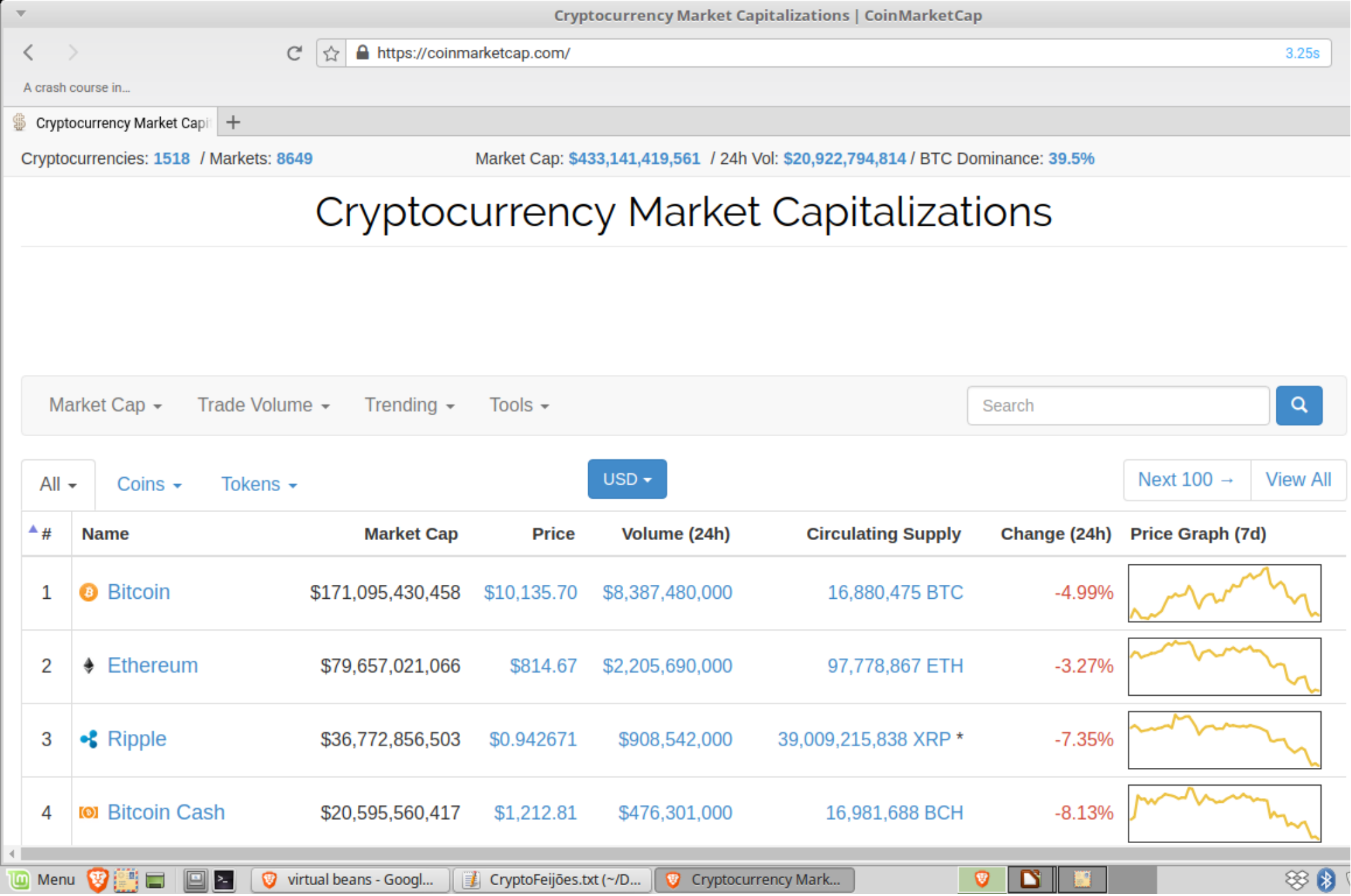
  → Ethereum

- Não, o código é a lei. Este hack faz parte do jogo

  → Ethereum Classic

Crowdfunding com cripto-moedas está na moda

- ICO = Initial Coin Offering
- Houve 863 ICOs em 2017; US$ 6 bilhões
- Não é sem risco:
  - Muito scams
  - Em julho um ICO foi hackeado



Existem hoje (868) 1518 criptomoedas

Impacto do blockchain

- A sociedade moderna sempre funcionou com autoridades – *trusted third parties* – mantendo registros:
  - Cartórios
  - Bancos
  - Entidades de administração pública
  - Etc etc
- O blockchain oferece uma alternativa **transparente e confiável** a estes registros
- Um blockchain proprietário sem inteligência e sem moeda não é muito novidade; melhor usar um banco de dados com log seguro

Impacto do blockchain

- Tecnologias como Ethereum possibilitam
  - execução de scripts em cima do seu block chain
  - (des)incentivar comportamento (in)desejável usando multas/prêmios em ether
- Assim surgiu uma nova disciplina: a cripto-economia
  - criptografia
  - teoria de jogos

Riscos do blockchain

- A tecnologia é complexa e não é madura ainda
- Cuidado com a rigidez dos programas//smart contracts
- Não subestime o papel positivo das autoridades
- Resistência cultural


criptografia transparente

Criptografia transparente

Ajudar as organizações a mostrar que eles são transparentes, justa, idônias.

Exemplos

- Block chain
- Eleições online com verificabilidade total
- Leilões, licitações e sorteios justas e transparentes
- Mineração de dados mantendo privacidade
- Processamentos de dados no cloud

vera vote

Perguntas?

jvdg@ufmg.br

INSCRYPT

DCC
DEPARTAMENTO DE
CIÊNCIA DA COMPUTAÇÃO

zeta
transparent
cryptography

EMBRAPII
UE - DCC/UFMG
SOFTWARE PARA SISTEMAS
CIBER-FÍSICOS

Meu livro sobre a insegurança da urna

www.mitourna.info

Arraes Editores vai publicar