

# Bitcoin e a Revolução Blockchain



# Apresentação

Um pouco sobre mim

# Alisson Solitto, 24 anos



Técnico em Informática  
Técnico em JAVA/WR



**UNIVEM**  
Centro Universitário Eurípides de Marília

Ciência da Computação  
MBA em Gestão de TI



Mestrando em  
Ciência da Computação



+7 anos de experiência com o  
desenvolvimento de software

**Blog:** <https://solitto.com.br>

**GitHub:** <https://github.com/alissonsolitto>

**Linkedin:** <https://www.linkedin.com/in/solitto>

**Lattes:** <http://lattes.cnpq.br/7754813473705418>

**Simplechain:** <https://simplechain.com.br>

**IzyMobile:** <http://izymobile.com>

# Agenda



- 1. História**
- 2. O que é**
- 3. Como funciona**
- 4. Cases**

# História do Blockchain e Bitcoin

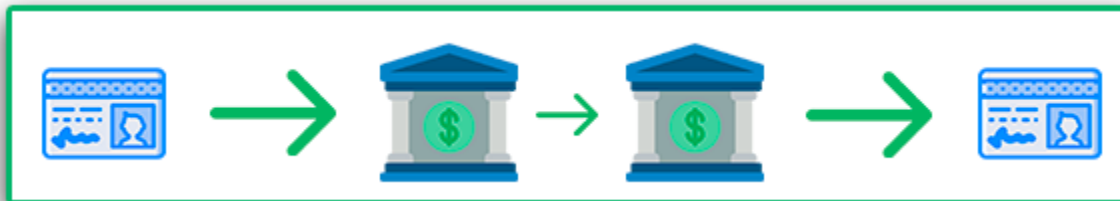
# História

- White Paper Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
- Ano: 2008 – Crise dos EUA

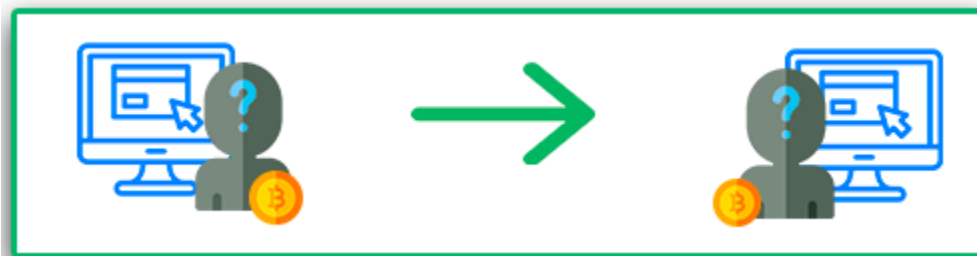




- Sistema Bancário



- Sistema Blockchain





# Blockchain

# Bitcoin







Bitcoin



Ethereum



Bitcoin Cash



Ripple



Litecoin



Ardor



Monero



Ethereum Classic



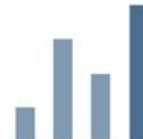
NEO



OmiseGO



Hshare



Iconomi



Qtum



Stratis



Tether



Zcash



Ark



Nexus



## Bitcoin

bitcoin / bitcoin

Watch 3.1k

Code Issues 748 Pull requests 293 Projects 8 Security Insights

Bitcoin Core integration/staging tree <https://bitcoincore.org/en/download>

bitcoin c-plus-plus p2p cryptocurrency cryptography

21,957 commits 7 branches 226 releases 672 contributors

Branch: master New pull request

Create new file Upload

MarcoFalke Merge #17288: Added TestShell class for interactive Python environments. ...	
.github	github: Add warning for bug reports
.tx	gui: Update transifex slug for 0.19
build-aux/m4	Merge #16110: depends: Add Android NDK support
build_msvc	doc: update MSVC instructions to remove Qt configuration
ci	Merge #17233: travis: Run unit and functional tests on native arm
contrib	doc: Fix some misspellings
depends	Merge #16110: depends: Add Android NDK support
doc	doc: Fix some misspellings
share	nsis: Write to correct filename in first place
src	Merge #17366: test: Reset global args between test suites
test	Merge #17288: Added TestShell class for interactive Python environment
.appveyor.yml	Added libbitcoin_qt and bitcoin-qt to the msbuild configuration.
.cirrus.yml	ci: Remove ccache requirement on the host
.gitattributes	Separate protocol versioning from clientversion



## Litecoin

litecoin-project / litecoin

forked from bitcoin/bitcoin

Watch 538

Star 3.4k

Fork 24.5k

Code Issues 28 Pull requests 8 Projects 0 Wiki Security Insights

Litecoin source tree <http://www.litecoin.org>

litecoin cryptocurrency

18,124 commits 8 branches 215 releases 571 contributors MIT
















Branch: master New pull request

Create new file Upload files Find file Clone or download

This branch is 160 commits ahead, 3993 commits behind bitcoin:master. Pull request Compare

wangxinxi Merge pull request #590 from thrasher-/0.17 ...		Latest commit 1b6c480 on 8 Apr
.github	Litecoin: Branding	11 months ago
.tx	tx: Update transifex slug 016x--017x	last year
build-aux/m4	Litecoin: Branding	11 months ago
contrib	Litecoin: Bump copyright year range	9 months ago
depends	Update zmq to 4.3.1	9 months ago
doc	Litecoin: Update man pages	7 months ago
share	Litecoin: Update Litecoin icons and images	9 months ago
src	Litecoin: Adjust splashscreen padding	7 months ago
test	Litecoin: Bump copyright year range	9 months ago
.gitattributes	Separate protocol versioning from clientversion	5 years ago
.gitignore	Litecoin: Branding	11 months ago
.travis.yml	Litecoin: Add script support to Travis	11 months ago
CONTRIBUTING.md	Litecoin: Branding	11 months ago

## Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾		Exchanges ▾	Watchlist	USD ▾		Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 <b>Bitcoin</b>	\$170.138.348.061	\$9.436,48	\$27.215.746.639	18.029.862 BTC	2,44%	 ...
2	 <b>Ethereum</b>	\$20.246.134.675	\$186,72	\$10.759.631.339	108.428.292 ETH	2,35%	 ...
3	 <b>XRP</b>	\$13.100.853.499	\$0,302923	\$1.827.469.284	43.248.091.671 XRP *	3,54%	 ...
4	 <b>Bitcoin Cash</b>	\$5.290.278.355	\$292,36	\$2.467.615.505	18.095.350 BCH	0,89%	 ...
5	 <b>Tether</b>	\$4.130.983.773	\$1,01	\$31.909.275.852	4.108.044.456 USDT *	-0,02%	 ...
6	 <b>Litecoin</b>	\$3.983.331.863	\$62,62	\$4.458.393.183	63.609.833 LTC	6,81%	 ...
7	 <b>Binance Coin</b>	\$3.241.598.207	\$20,84	\$271.319.192	155.536.713 BNB *	1,24%	 ...
8	<b>EOS</b>	\$3.239.570.008	\$3,45	\$2.696.205.671	938.821.495 EOS *	5,18%	 ...

# O que é?

## Blockchain e Bitcoin

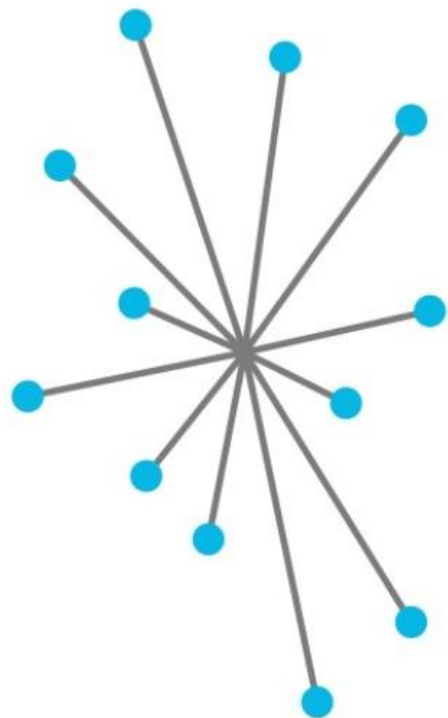


# Blockchain

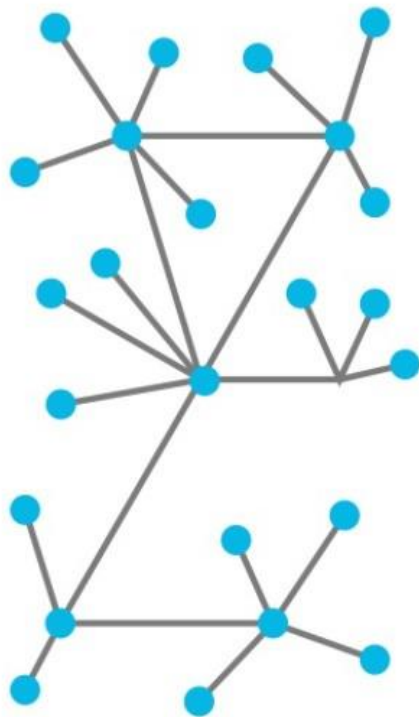
- O blockchain é uma rede de computadores **distribuída** (P2P).
- Rede de banco de dados distribuída
  - Cada participante possui uma cópia exata da base de dados
  - **Não há um servidor central** responsável pela confiança e segurança da informação
  - **Sistema de consenso**



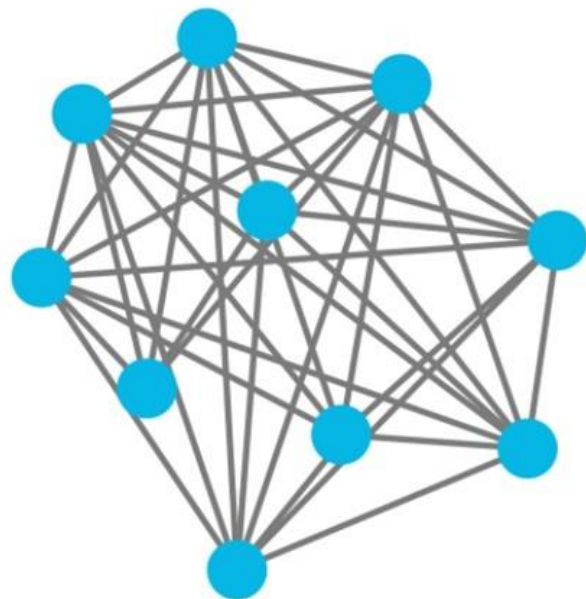
**Bitcoin** → **Descentralizado**  
**Blockchain** → **Distribuído**



Centralized



Decentralized



Distributed

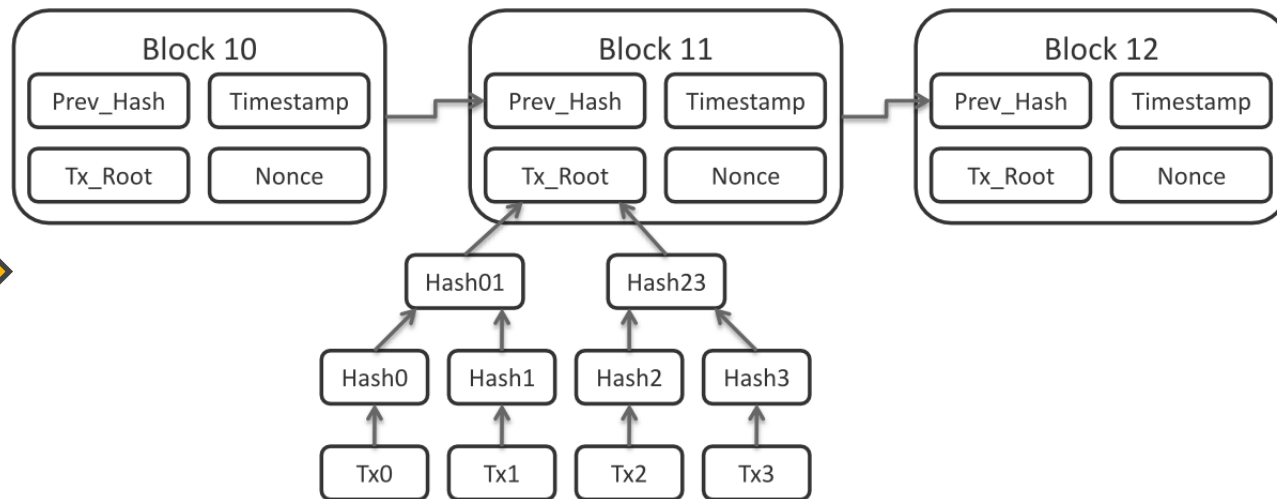
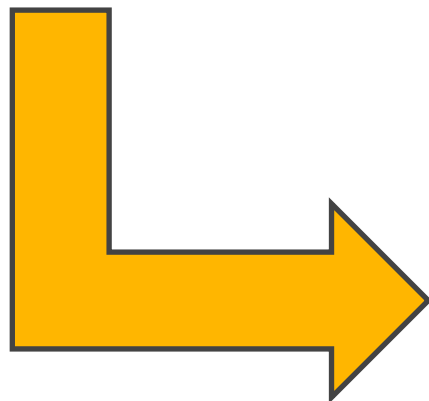
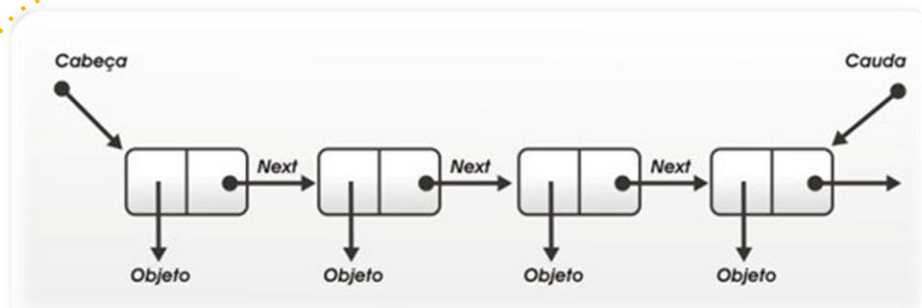


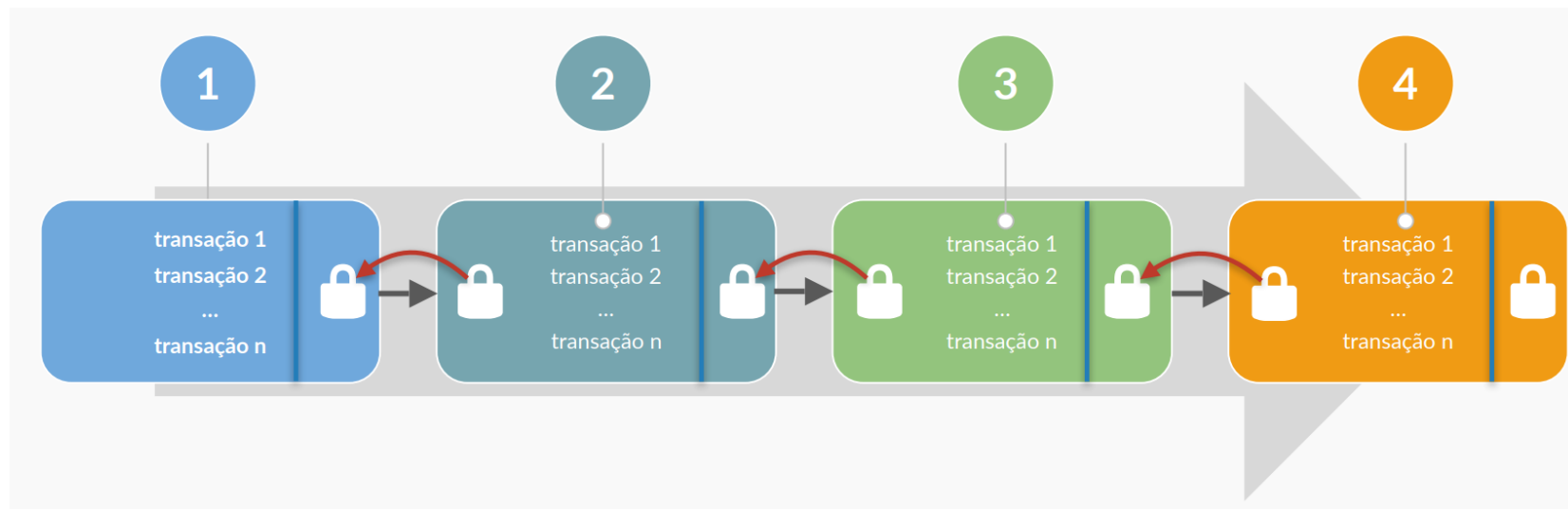
## Pública

## Privada

<p>Faz uso de criptomoedas</p> <p>Não permissionado</p> <p>Descentralizado</p> <p>Mudanças são mais lentas</p>	<b>BLOCKCHAIN</b>	<p>Dispensa o uso de criptomoedas</p> <p>Permissionado</p> <p>Centralizado</p> <p>Mudanças são mais rápidas</p>
----------------------------------------------------------------------------------------------------------------	-------------------	-----------------------------------------------------------------------------------------------------------------







3

**Como  
funciona?**

**Blockchain**

# Chaves e Endereços



**ALICE**

Large Random  
Number

Key Generation  
Program



# Anonimato



**Bitcoin Address:**

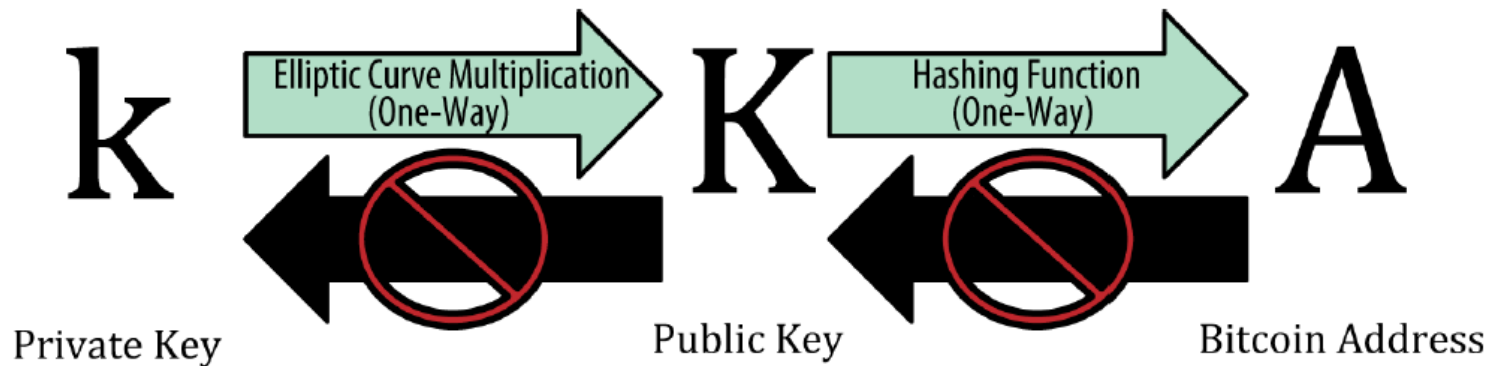
1MBx2wJzkqKavVbJscw92ktP8FTscV2ukV

**Private Key (Wallet Import Format):**

5KYxpFuYKfub671YUCFc2vf8XECRonBue3h3388dDsAp78AYscM

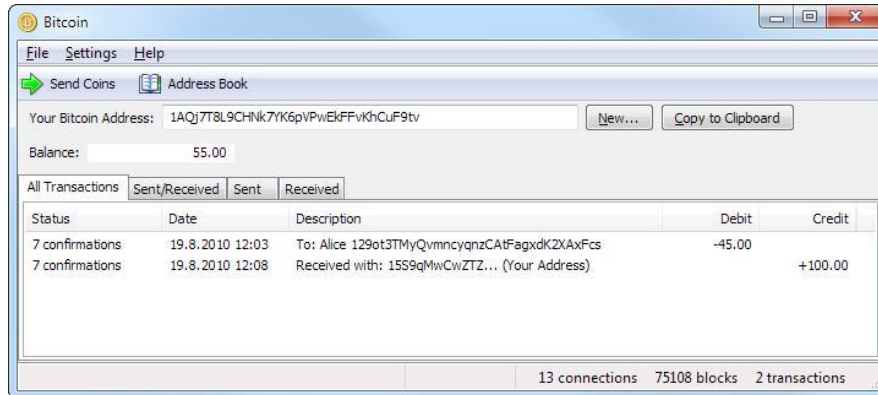


# Chaves e Endereços



# Wallets

- Hardware
- Software
- Paper



# Transações



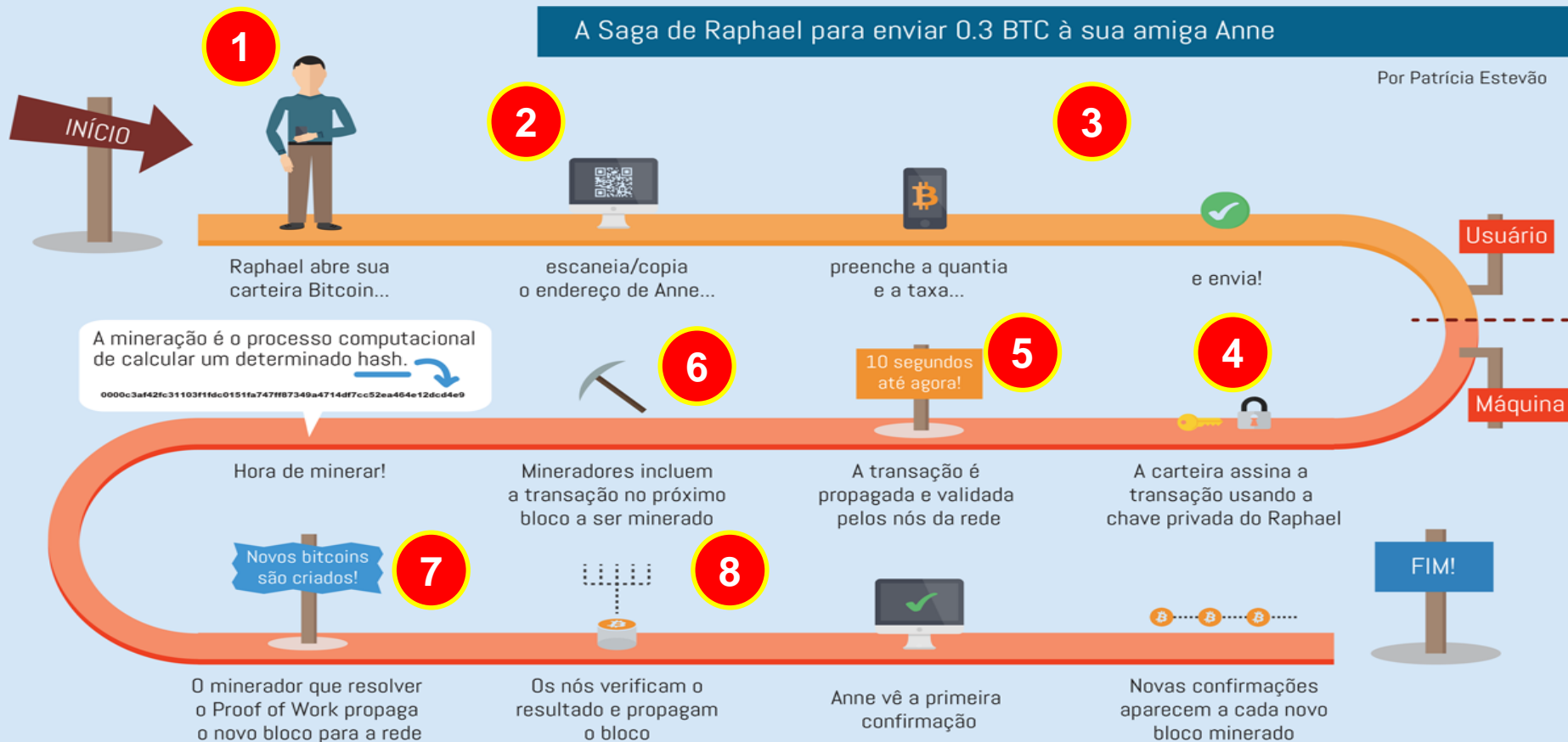
- Principal funcionalidade do Blockchain
- É uma transferência de dados entre usuários da rede que são:
  - Propagadas para os nós do blockchain
  - Validadas
  - Inseridas em um novo bloco da cadeia
- *Uma vez que as transações são incluídas em um bloco e este tem confirmações suficientes na cadeia, a transação pode ser considerada irreversível.*



# O CICLO DE VIDA DE UMA TRANSAÇÃO BITCOIN

A Saga de Raphael para enviar 0.3 BTC à sua amiga Anne

Por Patrícia Estevão





# Mineração

- O grande modelo que sustenta a rede descentralizada e publica do Blockchain do Bitcoin e o sistema de incentivo, esse sistema é conhecido como mineração.
- O processo de mineração tem duas funções essenciais
  - Proteger a rede Bitcoin contra possíveis transações fraudulentas
  - Gerar novas unidades do ativo Bitcoin como recompensa



## BLOCO 29

NONCE 4250

DADO:

R\$ 40 De: Paula > Camila

R\$ 60 De: Joana > Mario

R\$80 De: Pedro > Daniel

HASH: 00009642ba13e

HASH 0000652f3252e  
anterior:

0 = 1312af178c253f84028d480a6adc1e25e81caa44...  
1 = e9afc424b79e4f6ab42d99c81156d3a17228d6e1...  
2 = ae37343a357a8297591625e7134cbea22f5928be...

4248 = 6e110d98b388e77e9c6f042ac6b497cec466...  
4249 = c004190b822f1669cac8dc37e761cb73652...  
4250 = 0000c3af42fc31103f1fdc0151fa747ff8...



Hash:

**1Z8F**

Previous hash: **0000**

Hash:

**6BQ1**

Previous hash: **1Z8F**

Hash:

**3H4Q**

Previous hash: **6BQ1**

# Ataque



# Vamos Minerar \$\$





# Mineração

- Existem duas maneiras de minerar na rede blockchain do Bitcoin:
  - **Mineração solo:** nesta modalidade o no minerador faz todo o processamento de um novo bloco de maneira individual.
  - **Pool de mineração:** os nos mineradores se agrupam para compartilhar os recursos computacionais e fazer o processamento de um novo bloco.

# Mineração









A **Bitmain Technologies Ltd.**, ou **Bitmain**, é uma empresa privada com sede em **Pequim**, na **China**, que projeta chips de circuitos integrados específicos para a mineração de bitcoin.





SPOT ORDER

Receive \$150 coupon after delivery

Antminer T17-40TH/s

Shipping in 7 working days after fully paid

\$1252.00



FUTURES ORDER

Antminer S17e - 64TH/s

Shipping date: 21-31, Dec. 2019

\$2083.00



PRE-ORDER

Antminer S17e - 64TH/s

Shipping in January, 2020

\$2003.00



SPOT ORDER

Antminer S9k-14TH/s

Shipping in 7 working days after fully paid

\$138.00

Hash Rate Unit	Hash	Hashes Per Second
1 GH/s	1,000,000,000	One Billion
1 TH/s	1,000,000,000,000	One Trillion
1 PH/s	1,000,000,000,000,000	One Quadrillion

## Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.

Source: blockchain.com



**Hashrate** é o número de *hashes* que pode ser executado por um minerador bitcoin em um determinado período de tempo (geralmente um segundo).

# Cases e Aplicações

## Tecnologia Blockchain

# Benefícios



- Imutabilidade
- Transparência
- Confiabilidade
- Disponibilidade
- Descentralizado
- Distribuído

# Cases



- Registro de Documentos
- Sistema de Votação
- Identidade Digital
- Medicina
- BNDSToken
- Mercado Financeiro

# Innovation: Same day mobile international payments in “3 clicks & 40 seconds” for our retail customers using distributed ledger technology



➔ **Digital wallet**

➔ **Personal Finance Manager**

➔ **Same day international Payments**

➔ **P2P payments**

Going live in 4 countries  
1Q'2018



Full transparency on fees  
and FX upfront

We expect to be one of the  
**first global banks** to roll  
out Distributed Ledger  
Technology based  
payments for individuals

**€10Bn target market for international  
retail payments<sup>1</sup>**

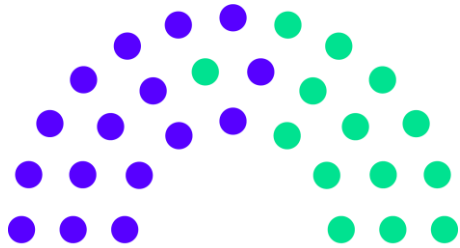


Initial investment in  
September 2015

(1) International retail payments volume (ex-interbank) in Santander's natural markets (Western Europe, Latam, North America and Eastern Europe)



# Tecnologias



Quorum  
J.P.Morgan



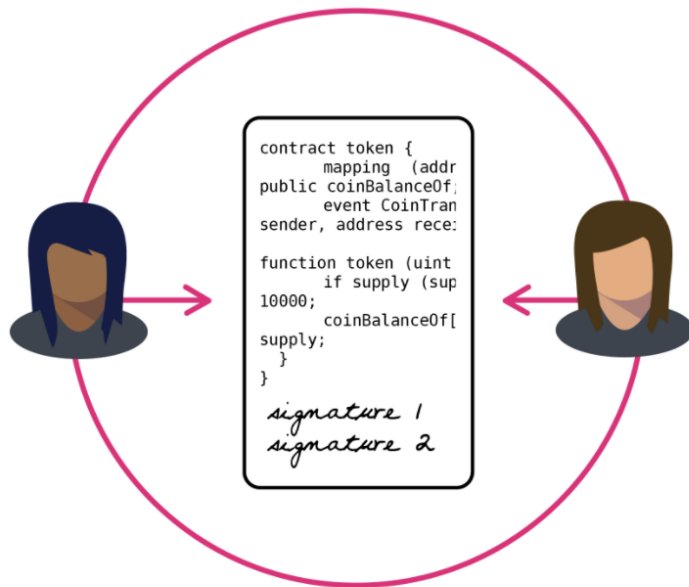
ethereum

# Tecnologias



**HYPERLEDGER**

# Smart Contracts





```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

    /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```





**Muito  
Obrigado!**

**Fim...**